Privacy and Participation: Personal Information and Public Sector Regulation in the United States

*Paul M. Schwartz**

---

* © Paul M. Schwartz, 1995. Professor of Law, The University of Arkansas (Fayetteville). I presented this Article at a conference held at the Annenberg Center for Communication Policy Studies in Washington, D.C. Criticisms on this occasion proved highly useful. I wish to thank Fred Cate for the opportunity to address this conference.

For their comments on previous drafts, I wish to thank Jutta Körbel, Spiros Simitis, David Dow, David Flaherty, Robert Gellman, Joel R. Reidenberg, Don Judges, Joseph Goldstein, Martin Flaherty, William Treanor, and John Applegate. Anne Arendt and David Gay provided excellent bibliographic assistance, and Terri Yeakley provided superb administrative help. Finally, I am grateful to the staff of the Iowa Law Review for its assistance and its patience.

In a world of international data transmissions, where global information sharing takes place involving a tremendous amount of personal data referring to individuals, the protection of individual privacy presents a critical regulatory challenge.[1] In Europe, where this issue has received the most concerted attention in the world, strong protections for personal data have been created.[2] The efficacy of these measures would be limited, however, if their reach ended at the borders of Europe. As a result, many European nations have extended their national laws to regulate extra-territorial activities involving the personal data of their citizens. These laws sometimes permit a blockage of international transfers of personal information.[3] At the transnational level, both the Council of Europe and the Commission of the European Union have created legal instruments that permit the blockage of data transfers to countries with inadequate protections.[4]

These national and trans-European measures pose a significant challenge to the free flow of data to the United States. The decision to permit a specific transfer of personal information to the United States requires Europeans to evaluate the nature and the extent of data protection law in the United States. This evaluation requires a relatively narrow examination of the specific context of the planned transfer, the nature of the concerned data, and the specific legal protections in the United States for these data.[5] Nevertheless, broader analysis can also be of significant utility. This Article will discuss the extent to which European and American data protection law share similar objectives and the extent of the convergence in these different legal systems.[6]

---

1. For a discussion of this regulatory challenge with an emphasis on European developments, see Spiros Simitis, From the Market to the Polis: the EU Directive on the Protection of Personal Data, 80 Iowa L. Rev. 445 (1995); Paul M. Schwartz, European Data Protection Law and Restrictions on International Data Flows, 80 Iowa L. Rev. 471 (1995).

2. *See generally* Colin J. Bennett, Regulating Privacy: Data Protection and Public Policy in Europe and the United States (1992); David H. Flaherty, Protecting Privacy in Surveillance Societies (1989).

3. *See* Schwartz, supra note 1, at 488-92.

4. Id. at 478-79, 483-89.

5. Id. at 485.

6. For a skillful comparative analysis concerning the extent of convergence in the law of

This Article begins by exploring possible objectives of data protection law. Part I discusses the limitations of a focus on privacy as "informational seclusion," which prohibits the state or private organizations from collecting or applying certain kinds of personal data. Part I advocates a shift in paradigms away from this "right to be let alone." It argues that data protection law must develop a notion of privacy as it relates to and is protective of participation. This "privacy as participation" model recognizes that in many instances the processing of personal information will take place. In light of this recognition, it uses the law to create a structure within which personal data may be utilized while an individual's capacity for decisionmaking is respected and encouraged. Decisionmaking in two areas is found to be essential: (1) deliberative autonomy, and (2) deliberative democracy. Evidence from the Federal Republic of Germany indicates how one nation has accepted this objective.

Having set forth the participatory approach to data protection, Part I further discusses the legal structure that embodies such a participatory model. The data protection model requires attention to four important elements: (1) the creation of a statutory fabric that defines obligations with respect to the use of personal information; (2) the maintenance of transparent processing systems; (3) the assignment of limited procedural and substantive rights to the data subject; and (4) the establishment of effective government oversight of data use. Strong evidence exists indicating European-wide acceptance of this model. Perhaps the best evidence of this acceptance lies in the European Union's Directive on Data Protection Law,[7] which elevates the elements of the data protection model to the status of European law.

Part II compares this European approach to American legal developments concerning data protection in the public sector. It examines selected norms of constitutional, federal, and state law. This analysis centers on the public sector for two reasons. First, such a focus allows this study to be both fairly comprehensive in scope and reasonably manageable in length. Second, the best case for data protection law in the United States is likely to be found in the public sector. The state usually requires less justification when governing itself than when regulating private activities. Weaknesses in data protection within the public sector can be

---

sexual harrassment, see Anita Bernstein, Law, Culture and Harrassment, 142 U. Pa. L. Rev. 1227 (1994).

7. Common Position (EC) No. /95 With a View to Adopting Directive 94/ /EC of the European Parliament and of the Council on the Protection of Individuals With Regard to the Processing of Personal Data and on the Free Movement of Such Data, 1995 O.J. (C 93, April 13, 1995) [hereinafter Data Protection Directive]. The text of the Directive is reprinted at 80 Iowa L. Rev. 697 (1995).

The Data Protection Directive has not yet been officially adopted. It has, however, been formally approved by the Union's Member States and is now before the European Parliament. James Pressley, EU Approves New Measure to Protect Personal Data, Wall St. J. Eur., Feb. 21, 1995, at 2.

expected to be accompanied by even greater shortcomings in data protection within the private sector.

Part II finds that American data protection law, like its European counterpart, recognizes the value of privacy as participation. Therefore, the high stakes debate about international data transfers is not complicated by different foundational legal concepts in Europe and the United States. The thesis of this Article is, however, that American data protection law currently does not coherently and completely reflect the paradigm of privacy as participation.

On the level of constitutional law, data protection in the United States is most successful when it is allied with the concept of deliberative democracy. This term refers to the process by which citizens make decisions about the justice of basic political institutions and social policies.[8] Although American constitutional law pays careful attention to governmental data application when areas of deliberative democracy such as "associational privacy" and the electoral franchise[9] are involved, informational privacy also should be protected when it is not directly linked to political activities. It deserves this broader protection because an underlying capacity for decisionmaking forms the basis not only for participation in political life, but for sharing in intimate behavior or communal activities. The critical criterion justifying the expanded protection is the concept of deliberative autonomy, which concerns the underlying capacity of individuals to form and act on notions of the good when deciding how to live their lives.[10]

Constitutional attention to informational privacy must move beyond simply protecting personal data associated with deliberative democracy; rather, it should also offer safeguards when an individual's underlying capacity for decisionmaking is threatened. Yet, the Supreme Court's Fourth Amendment jurisprudence protects only informational seclusion.[11] The Supreme Court's decision in *Whalen v. Roe*[12] offers another example of how the notion of privacy sometimes fares poorly when it is not associated with political process values. In the interpretation of some lower courts, the *Whalen* right of informational privacy sometimes merely protects a right to be let alone.[13] Other lower courts, however, have applied *Whalen* in a fashion that protects the individual's participation in society.[14]

---

8. James E. Fleming, Constructing the Substantive Constitution, 72 Tex. L. Rev. 211, 253-55 (1993).

9. *See* infra parts II.A.1-2.

10. John Rawls has described the fundamental societal importance of individuals with "the capacity for a conception of the good." John Rawls, Political Liberalism 332 (1993). This capacity is to guide "our conduct over a complete life." Id. at 335. For a brilliant centering of this interest within the American legal tradition, see Fleming, supra note 8, at 253.

11. *See* infra part II.A.3.

12. 429 U.S. 589 (1977).

13. *See* infra part II.A.4.

14. *See* id.

On the statutory level in the public sector, American federal data protection law has neglected to update existing laws, overemphasized the value of individual enforcement rights, and failed to institute adequate independent governmental oversight of personal information processing.[15] On the state level, American public sector data protection law suffers from even greater weaknesses.[16] Unlike federal law, state data protection law usually does not employ an omnibus law that sets fair information practices for governmental entities. As a result, data protection only exists in a state if separate statutes protect certain types of personal information. This kind of patchwork approach leaves many types of data unprotected.

Despite the undeniable merit of particular regulations, American data protection law in the public sector generally has not been successful. Its weaknesses are particularly significant due to the many European legal measures, both national and transnational, permitting a blockage of data transfers to nations with insufficient protections. This Article concludes by attempting to explain the American difference in data protection.[17] It argues that although the role of government is similar in the United States and Europe, Americans exhibit considerable defensiveness, if not hostility, toward state activism. This ambivalence undercuts American attempts to create data protection law, which requires the state to make difficult regulatory decisions about structuring the application of personal information.

I. THE GOALS OF DATA PROTECTION LAW

Although not in widespread use in the United States, the term "data protection," in the rest of the world, refers to a system of legal rules that structure the application of personal data.[18] The first section of this Part argues that data protection law cannot orient itself according to an idea of information seclusion. Such a simple right to be "let alone" is of limited utility in the computer age. Instead, data protection law must focus on a notion of privacy as participation. Such participation relates to two areas: (1) deliberative autonomy and (2) deliberative democracy. Privacy as participation should form the critical theoretical orientation of data protection law. Examples from German law will illustrate that at least one European legal system has acknowledged the necessity of such a paradigm

15. *See* infra part II.B.

16. *See* infra part II.C.

17. *See* infra part III.

18. *See* Bennett, supra note 2, at 3-6 (describing international development of data protection law); Flaherty, supra note 2, at 11-17 (describing the role of data protection oversight agencies which seek to enforce data protection rules that promote accountability and fair information practices); *see also* Paul M. Schwartz, Data Processing and Government Administration, 43 Hastings L.J. 1321, 1374-84 (1992) (discussing the role of law in structuring governmental data use); Spiros Simitis, Reviewing Privacy in an Information Society, 135 U. Pa. L. Rev. 707, 737-46 (1987) (discussing essential components of efficient data protection regulations).

shift.

In its second section, this Part will develop a legal structure for the realization of the participatory model of data protection. This structure consists of four essential elements: (1) the creation of a statutory fabric that defines obligations with respect to the use of personal information; (2) the maintenance of transparent processing systems; (3) the assignment of limited procedural and substantive rights to the data subject; and (4) the establishment of effective governmental oversight of data use. In explaining these four elements, Part I.B will trace their expression in an important European-wide norm, the European Union's Directive on Data Protection.

A. Participation and Individual Self-Determination

Privacy can refer to many things; privacy might, for example, simply indicate a legal concern for keeping information confidential.[19] This Article will call this notion "informational seclusion." A model of data protection that is concerned with informational seclusion generally proceeds by forbidding the state or private organizations from collecting or using certain kinds of personal information. This approach to privacy attempts, in the immortal words of Brandeis and Warren, to protect the right to be "let alone."[20]

Yet, privacy as the right to be let alone serves as an incomplete paradigm in the computer age. The activist state and service economy depend on an increased and intensified knowledge of the citizen in such roles as taxpayer, employee, consumer, or recipient of the state's benefits.[21] This knowledge is employed to control administration and to shape human behavior.[22] In this age, privacy as a right to be let alone presents a number of shortcomings. To begin with, information seclusion is rarely achievable; when gathering personal information is the objective, good, perhaps even excellent, reasons will often exist *not* to leave someone alone.

For example, consider the processing of personal information in the realm of medicine. Hospitals, doctors, and pharmacies in both Europe and the United States must process and share often highly sensitive personal information.[23] Such data processing is carried out because of a desire to

---

19. One expression of this notion is found in tort law's protection against public disclosure of embarrassing private facts. *See* Restatement (Second) of Torts § 652D (1977) (imposing liability on anyone publicizing information that would be highly offensive to a reasonable person or does not legitimately concern the public).

20. Samuel D. Warren & Louis D. Brandeis, The Right to Privacy, 4 Harv. L. Rev. 193, 193-97 (1890).

21. Schwartz, supra note 18, at 1329-33.

22. Id.; *see* Jerry L. Mashaw, Bureaucratic Justice 26 (1983) ("The general decisional technique [of bureaucratic rationality] is information retrieval and processing.").

23. Paul M. Schwartz, The Protection of Privacy in Health Care Reform, 48 Vand. L. Rev. 295, 300-06, 326-27 (1995).

limit expenditures; to increase the effectiveness of treatments; to prevent the choice of bad treatments or overprescription of medicine; and to control potentially fatal drug interactions.[24] The state, seeking access to this information, promulgates regulations to facilitate its collection by the public and private sectors. This state interest is grounded in both the state's general police power (expressed in Europe and the United States alike through the licensing and regulation of doctors, hospitals, and pharmacies) and specific regulatory powers relating to the provision of medical insurance.[25]

The widespread collection and processing of medical data exemplifies the problematic nature of an attempt to protect information seclusion — this idea can be applied only to a limited number of situations. Privacy as information seclusion tends to collapse in the face of the weighty reasons provided in support of seeking personal information.[26] Put another way, this approach to privacy is a false paradigm for data protection law because it applies to the exception and not the rule. Only the collection of certain kinds of sensitive information might be restricted by this approach, and even such data will often be in demand for justifiable reasons.[27]

A second shortcoming of privacy as information seclusion is that its utility ceases at the moment personal data are surrendered. Yet, in the computer age, the critical issue is no longer limited to *whether* personal data should be collected and processed, but *how* these data should be used. Significantly more personal data are collected and used as a result of the increasing use of computer technology. Indeed, by reducing personal information to a fluid digital form, the computer encourages the sharing of data within different organizations.[28] Data protection law should respond by countering the computer's omniscience with a compromise between the concealment and exposure of personal information. A right to be let alone does not help address the question of how this compromise should be struck.

Data protection law requires a different approach. Privacy conceived as relating to the human capacity for participation is more helpful than the concept of informational seclusion in structuring data protection law. The

---

24. Id. at 300-06.

25. Id. at 303-06, 324-27. European governments currently may take a more comprehensive role regarding the provision of medical insurance than the United States government. Yet, through Medicaid and Medicare, the American government is already in the business of financing and overseeing health care services. *See* id. at 300-03.

26. *See* Whalen v. Roe, 429 U.S. 589, 602 (1977) ("Disclosures of private medical information to doctors, to hospital personnel, to insurance companies, and to public health agencies are often an essential part of modern medical practice even when the disclosure may reflect unfavorably on the character of the patient.").

27. *See, e.g.*, Planned Parenthood v. Casey, 112 S.Ct. 2791, 2932-33 (1992) (upholding state requirements of record keeping and reporting for facilities at which abortions are performed).

28. I have referred to this tendency as an ability which allows the computer to make the information that it processes "multifuctional." Schwartz, supra note 18, at 1339.

privacy as participation approach finds that limitations on the processing of personal information are necessary because individual decisionmaking in a democratic society takes place *without* and *within* the life of the community.[29] Indeed, the health of such a society depends on the functioning of each person's individual capacity for decisionmaking. As Ronald Dworkin has argued, "each citizen [is] responsible for imagining what his society's public commitments to principle are, and what these commitments require in new circumstances."[30] Such important acts of individual creative imagination require that citizens be able both to retreat from and to participate in social life. As one European professor of law expresses this idea, "privacy is a characteristic of relations with others."[31]

At the same time that a free society depends upon individual self-determination, the processing of personal information can have a destructive effect on this capacity. In today's information society, extensive collections of data relating to identifiable persons are typically organized in extensive computer data banks. This kind of data processing creates a potential for suppressing a capacity for free choice: the more that is known about an individual, the easier it is to force his obedience. Through the use of their data banks, the state and private organizations can transform themselves into omnipotent parents and the rest of society into helpless children. Indeed, totalitarian regimes in Eastern Europe relied on information gathering and data storage to weaken the individual capacity for critical reflection and to repress any social movements outside their control. Even without computers, these regimes demonstrated the fragility of the human capacity for self-determination in the face of widespread spying and data collection.[32] The state must organize the processing of personal information in a way that will preserve and encourage the individual's capacity for free decision making.

Specifically, data protection law must concern itself with decision making relating to two critical areas. The first can be called "deliberative autonomy"; the second, "deliberative democracy." Deliberative autonomy refers to the underlying capacity of individuals to form and act on their notions of the good when deciding how to live their lives.[33] A limitless sharing of information about such topics as one's medical history, sexual

---

29. *Cf.* Stanley Ingber, Judging Without Judgment: Constitutional Irrelevancies and the Demise of Dialogue, 46 Rutgers L. Rev. 1473, 1553 (1994) ("[I]ndividualism provides an unrealistic account of our moral existence; individuals are not separate from the community in which they reside.").

30. Ronald Dworkin, Law's Empire 413 (1986).

31. Adalbert Podlech, Das Recht auf Privatheit, *in* Grundrechte als Fundament der Demokratie 50, 51 (Joachim Perels ed., 1979); *see* Jed Rubenfeld, The Right of Privacy, 102 Harv. L. Rev. 737, 753 (1989) (discussing how a state proscription, by taking over or occupying the totality of a citizen's life, can destroy individual autonomy).

32. For a discussion of these tendencies within the German Democratic Republic, see Paul M. Schwartz, Constitutional Change and Constitutional Legitimation: The Example of German Unification, 31 Hous. L. Rev. 1027, 1052-53 (1994).

33. Fleming, supra note 8, at 253; Rawls, supra note 10, at 214-35.

behavior, or financial affairs raises a threat to this first interest in self-determination. Data protection law must offer safeguards to preserve the underlying capacity for decision making.

In contrast, deliberative democracy refers to the decisional process by which individuals make choices about the merits of political institutions and social policies.[34] Interference with the right to vote and with political associations, for example, restricts individual choice, blocks the channels of political change and, eventually, dooms democracy. In the words of John Hart Ely, interference with participation in the political process creates "stoppages in the democratic process."[35] Deliberative democracy requires that citizens be permitted to apply their deliberative capacities to the consideration of the justice of basic institutions and social processes. As in the area of deliberative autonomy, data protection law plays a critical role in deliberative democracy; the law must structure the use of personal information so that individuals will be free from state or community intimidation that would destroy their involvement in the democratic life of the community.

Deliberative autonomy and deliberative democracy provide a critical normative expression of goals for data protection law. Before supplementing these somewhat abstract notions with a more specific programmatic scheme, it should be noted that some evidence exists that European data protection has oriented itself around this notion of privacy as participation. This orientation has been expressed particularly clearly in the Federal Republic of Germany.

In Germany, the legal doctrine underlying data protection law is "the right of personality."[36] Although the right of personality has a distinguished lineage and is of venerable age, its full acceptance by German law occurred relatively recently.[37] The post-war German constitution, the Basic Law (*Grundgesetz*), enacted in 1949, provides the most important textual basis of this right: Article 1 protects human worth, and Article 2, human personality.[38] Taken together, these two provisions create the right of personality.[39]

The right of personality protects more than the mere right to be let

---

34. Fleming, supra note 8, at 254.

35. John Hart Ely, Democracy and Distrust 117 (1980).

36. For an introduction to this doctrine, see Heinrich Hubmann, Das Persönlichkeitsrecht 268-332 (1967).

37. For a clear and concise introduction to this development, see David Currie, The Constitution of the Federal Republic of Germany 316-21 (1994).

38. Article 1(1) provides: "The dignity of man shall be inviolable. To respect and protect it shall be the duty of all state authority." Grundgesetz [Constitution] [GG] art. 1 & 2 (F.R.G.), *reprinted in* Currie, supra note 37, at 343 app. Article 2(1) states: "Everyone shall have the right to free development of his personality in so far as he does not violate the rights of others or offend against the constitutional order or the moral code." Id.

39. For a sampling of the critical case law of the German Consitutional Court developing this right, see 54 Entscheidungen des Bundesverfassungsgerichts [BVerfGE] 148, 155 (Eppler) (1980); 34 BVerfGE 269, 281 (Soraya) (1973); 27 BVerfGE 1, 6-7 (Mikrozensus) (1969).

alone. In the words of the German Constitutional Court, the right of personality provides a place in the "center of the constitutional order [for] the worth and dignity of the individual, who functions in free self-determination as a member of a free society."[40] As the Court has indicated, the right of personality safeguards individual capacities that secure the basis for a certain kind of communal life.[41] Self-determination matters because it ensures the existence of a free society.

German law has moved beyond the notion of a right of personality that protects merely an "inner domain" or "an autonomous domain of private life promotion."[42] German law has accepted an idea of privacy as related to and promotive of participation. To do so, it developed a new aspect of the right of personality: the right of informational self-determination. In its pathbreaking *Census* decision of 1983, the Constitutional Court carried out a decisive step in German law's acceptance of the model of privacy as participation.[43]

Rather than seeking to identify secret or sensitive information that the state could not collect, the Constitutional Court discussed the social nature of most personal information and called for legal provisions to structure the treatment of personal data.[44] These provisions must allow the person affected to know who will use his personal data and the purposes to which this information will be put.[45] The Court declared:

> The person who cannot oversee with sufficient certainty which of the information about him is known in distinct domains of his social environment, and who is unable to evaluate the knowledge of a possible communication partner, can be greatly inhibited in his freedom to decide or plan in personal self-determination. . . . This would have not only a negative effect on the individual's chances of development, but would also harm the common good because self-determination is an elementary functional condition of a free democratic community based on its citizens' capacity to act and participate.[46]

This language explains why participation in social life requires legal attention to a myriad of constellations of data use and transmission. Such

---

40. 65 BVerfGE 1, 41 (Volkszählungsgesetz) (1983).

41. Id.

42. For these earlier decisions, see 35 BVerfGE 202, 220 (Lebach) (1973); 32 BVerfGE 373, 379 (Krankenblätter) (1972); 27 BVerfGE 344, 350-51 (Ehescheidungsakten) (1970); 6 BVerfGE 32, 41 (Ausreisefreiheit) (1956).

43. 65 BVerfGE 1, 41 (Volkszählungsgesetz) (1983). For a discussion of this case, see Paul M. Schwartz, The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination, 37 Am. J. Comp. L. 675, 686-94 (1989). An English translation of excerpts from this opinion with excellent commentary is found in Donald P. Kommers, The Constitutional Jurisprudence of the Federal Republic of Germany 332-36 (1989). For later cases applying this important right, see Neue Juristische Wochenschrift [NJW] 707 (1989), NJW 2805 (1987).

44. 65 BVerfGE at 43-45.

45. Id.

46. Id. at 42-43.

attention benefits the individual and the community, which depends on the self-determination of its members for healthy functioning.

B. The Participatory Model of Data Protection Law

The participatory model of data protection requires a certain normative orientation: The law must organize the social application of personal information to preserve and encourage individual self-determination. This general normative orientation is best realized within a certain programmatic structure. The required approach not only must grant individual interests to the citizen herself, but also must assign different roles to the legislature, judiciary, and governmental oversight agencies.

Four elements are crucial for the structuring of a legal system that embodies the value of privacy as participation: (1) the creation of a statutory fabric that defines obligations with respect to the uses of personal information; (2) the maintenance of transparent processing systems; (3) the assignment of limited procedural and substantive rights to the data subject; and (4) the establishment of effective governmental oversight of data use. In the following discussion of these elements, this Part explores their presence in an important transnational document, the Commission of the European Union's Directive on Data Protection.[47] The Directive represents proof both of European agreement about the essential elements of data protection law and of an intention to harmonize domestic European law at a high level that reflects these elements.[48]

The first element of this model of data protection law is the creation of a statutory fabric that defines obligations with respect to the processing of personal information.[49] Different risks will arise depending on the area of life subject to administration or surveillance through data processing. Legislation, therefore, must not only take the form of a general data protection law, providing a safety net in an age of rapid technological developments, but must also consist of specific laws directed at discrete sectors of data application. This form of legislative structuring is particularly important because any assignment of rights to individuals can only be limited in scope; thus, broader statutory limits on the processing of

---

47. Data Protection Directive, supra note 7, arts. 2-24.

48. Each country in the Union expresses data protection law in a different fashion. These differences reflect the unique social, political, and historical background of the country in question. *See generally* Flaherty, supra note 2, at 21-29, 93-103, 165-72. Yet, when domestic data protection law falls short of the requirements of the Directive, this transnational document will have direct effect within the European country. Although a directive of the European Union generally relies on domestic legal institutions for its transformation into law, direct reliance by Member Nations on the Directive is possible if it is not implemented into domestic law correctly, completely, or punctually. Schwartz, supra note 1 at 481-82.

49. *See* Privacy Protection Study Commission, Personal Privacy in an Information Society 14-15 (1977) [hereinafter Personal Privacy] (finding that privacy protection depends on legislation and other forms of regulation that "create and define obligations with respect to the uses and disclosures that will be made of recorded information about an individual").

personal data must be created.

The Data Protection Directive of the European Union recognizes this need for defined statutory obligations with respect to the processing of personal data. It lists the statutory provisions required in Member States and obliges these nations to "provide that processing of personal data is lawful only if carried out in accordance" with these rules.[50] Agreement also exists in Europe as to the necessary kinds of substantive protections. As the Directive and the laws of numerous European countries indicate, a statute authorizing the collection of personal information must generally specify the purposes of data collection, place limitations on the period of information storage, and provide measures of data security.[51] It must also create special protection for certain kinds of sensitive data.[52]

The second element necessary in the model of data protection law is the maintenance of transparent processing systems. This essential norm requires that the application of personal information be structured in an open manner which is understandable to individuals. When the establishment of secret files can serve to coerce the individual, comprehension of the application of information can encourage participation in the spheres of social and political life. In this sense, the Directive provides the concise general rule that "a person is entitled, on request, to know of the existence of a processing operation."[53] It also requires that "a data subject from whom data are collected" generally be told of the purposes of the intended processing and whether disclosures of the information to a third party are planned.[54]

The third element of the model of data protection law is the assignment of limited procedural and substantive rights to the data subject. In addition to substantive rights, some of the necessary individual rights are procedural: An individual should be informed of whether the supplying of personal information is mandatory and of the type of mechanism available for inspection and correction of these data. Such notice also serves to further the second element of data protection law, the transparency of information processing. The Union's Directive generally allows an individual rights both to object to the processing of her personal data and to be free from decisions "based solely on automatic processing of data intended to evaluate certain personal aspects."[55] An important, additional part of any assignment of rights to the individual is the shaping of effective remedies. Chapter III of the Directive requires Member Nations

50. Data Protection Directive, supra note 7, art. 5.

51. Id. arts. 6, 17. For the presence of these elements in a domestic European data protection law, namely that of France, see, e.g., Act 78-17 on Data Processing, Data Files, and Individual Liberties §§ 28-29 (Fr.), *in* Data Protection in the European Union: The Statutory Provisions (Spiros Simitis et al. eds., 1994) [hereinafter Data Protection Statutes].

52. Data Protective Directive, supra note 7, art. 8.

53. Id. art. 10. The Directive also provides for exceptions to this rule. Id. art. 14.

54. Id. arts. 11-12.

55. Id. art. 15.

to make available a variety of judicial remedies to the individual.[56] These remedies are to include damages and penalties for the violation of personal rights.[57]

Finally, independent monitoring of information processing is necessary. Such an institution of data protection oversight plays three critical roles. To begin with, in an area of rapid technological change, this body provides expertise which is to be placed at the service of the government, business, and citizens. Second, the data protection commission helps in the development and oversight of international measures that effect global data transfers. Finally, this agency serves as a focal point for societal discussion about the utilization of information processing technology.[58]

Most Western European nations already have established such organizations. Even outside Europe, independent data protection agencies have been created in Australia and Canada.[59] As for the Directive, it requires its Member States to "designate an independent public authority to supervise the protection of personal data."[60] This authority is to monitor the development and application of national data protection law and to fulfill specified functions that the Directive sets out.

The data protection model described in this Article requires legal limits on governmental and societal demands for personal information. The preceding comparisons to the Directive indicate that Europe has adopted this approach. This Article now makes use of this paradigm as a yardstick for comparisons with American law.

II. AMERICAN DATA PROTECTION LAW IN THE PUBLIC SECTOR

The privacy as participation model of data protection is not unknown to American law. Looking only in the public sector, one finds elements of this model present in both constitutional law and federal and state legislative measures. These legal provisions recognize the relation between limits on information flows and the individual's ability to participate in political and social life.[61] Yet, entirely successful forms of data protection have not been created in the United States.

At the constitututional level, this Article considers the extent to which

---

56. Id. arts. 22-24.

57. Data Protection Directive, supra note 7, arts. 23-24.

58. For a description of how data protection commissioners in France and Germany carry out this task, see Evangelia Mitrou, Die Entwicklung der institutionellen Kontrolle des Datenschutzes 273-79 (1993). For a further analysis of these three roles of data protection agencies, see Schwartz, supra note 1, at 493-94.

59. For analysis of the Canadian approach, see Flaherty, supra note 2, at 243-303. Another international example is Hong Kong, where a Law Reform Commission has called for the creation of a Privacy Commissioner. Hong Kong Law Reform Commission, Privacy: the Protection of Personal Information (1993).

60. Data Protection Directive, supra note 7, art. 30.

61. *See* infra parts II.A.4, II.B.1.

protections exist for both deliberative democracy and deliberative autonomy. In the United States, the greatest successes in data protection have occurred when the government's data collection impinges on a constitutional right concerning democratic process values. When the state's data processing chills "associational rights" or the "right to vote," courts have taken effective action.[62] In contrast, judicial attention to an American right of decision autonomy has not led to adequate levels of protection.[63]

Federal legislation concerning data protection also incorporates participatory values. The Privacy Act represents a particularly important example of such an effort.[64] This law outlines important fair information practices for federal agencies to follow in processing personal information. Yet, the Privacy Act contains numerous shortcomings that undercut its value.

The weaknesses of the Privacy Act are accompanied by significant problems on the state level. Most states lack laws, similar to the Privacy Act, that regulate the governmental use of personal information.[65] Rather, the approach by states is to establish protections in a patchwork fashion. Thus, while the treatment of library records is regulated in all states, more sensitive information is often ignored. In addition, all states have freedom of information laws.[66] While the federal Freedom of Information Act contains strong provisions for privacy protection, many state laws do not. This shortcoming creates a powerful pressure for the release of personal information held by state governments.

A. Constitutional Law: Deliberative Democracy and Deliberative Autonomy

The United States Constitution establishes a framework for a debate among citizens about the nation's institutional relationships and fundamental values.[67] One way this document does so is by providing critical controls on the State; its provisions carefully establish the government's structure and limit its behavior.[68] The Constitution also contains provisions that indicate concern for individual self-determination. Its Bill of Rights and Civil War Amendments contain the most important language in this regard.[69] These provisions prevent the state not only

62. *See* infra parts II.A.1-2.

63. *See* infra parts II.A.3-4.

64. 5 U.S.C. § 522a (1977 & Supp. 1994).

65. *See* infra part II.C.

66. Id.

67. For academic discussion of this idea, see Bruce Ackerman, We the People: Foundations 22 (1991); Stanley Ingber, supra note 29, at 1473-79.

68. For a comparative analysis of the way in which two constitutions, those of the United States and the Federal Republic of Germany, carry out these functions, see Schwartz, supra note 32, at 1086-1101.

69. *See* infra part II.A.1-4.

from interfering in the exercise of certain activities, but also from carrying out certain kinds of collection and utilization of personal information.

Despite these protections of higher law, the constitutional requirements for informational privacy cannot be expected to enumerate programmatic detail. The Constitution sets forth a structure for national dialogue by reserving only the most important principles to higher law; it relegates most issues to the give-and-take of normal politics.[70] The four elements of the data protection model developed in this Article raise issues ordinarily reserved to normal politics in the United States.[71] If these elements are present at all, we can expect them to be the result of statutory law. This section concerns itself with higher law's attention to deliberative democracy and deliberative autonomy.

1. Associational Privacy

The First Amendment to the United States Constitution protects the individual's associational rights.[72] In a series of important decisions in the 1950s and 1960s, the Supreme Court prevented the state from collecting information that would unconstitutionally compel a disclosure of group affiliation.[73] These decisions provide important protection for the constitutional interest in group or associational privacy.

NAACP v. Alabama is the leading group privacy case.[74] In the 1950s,

---

70. Ackerman, supra note 67, 243-69. For a critical, comparative discussion of this approach, see Schwartz, supra note 32, at 1091-1101.

71. Only the most important rules for shared social life are placed on the higher, constitutional law-making track; on this track, there are many institutional barriers challenging constitutional change. Ackerman, supra note 67, at 243-51.

72. The First Amendment's guarantee of the freedom of association is applicable to the states through the Fourteenth Amendment's Due Process Clause. *See* NAACP v. Alabama, 357 U.S. 449, 460 (1958) ("It is beyond debate that freedom to engage in association for the advancement of beliefs and ideas is an inseparable aspect of the 'liberty' assured by the Due Process Clause of the Fourteenth Amendment, which embraces freedom of speech.").

73. *See generally* Gibson v. Florida Legislative Investigative Comm., 372 U.S. 539 (1963) (reversing conviction of contempt for not disclosing information contained in organization's membership list); Bates v. Little Rock, 361 U.S. 516 (1960) (reversing convictions for the violation of a municipal occupational license tax compelling disclosure and publication of membership lists); NAACP v. Alabama, 357 U.S. at 449 (reversing judgement of contempt for refusing to disclose membership lists). All these cases involved the NAACP, a civil rights organization.

During this same period, the members of the American Communist Party's claims of freedom of association generally fared considerably less well before the Supreme Court. *See* Communist Party of the U.S. v. Subversive Activities Control Bd., 367 U.S. 1, 89 (1961) (holding that registration of a communist group and its members under § 7 of the Subversive Activities Control Act of 1950 did not violate freedom of association under the First Amendment); Scales v. United States, 367 U.S. 203, 230 (1961) (stating that the membership clause of the Smith Act does not infringe on freedom of association under the First Amendment). *But see* DeGregory v. Attorney General, 383 U.S. 825, 828-30 (1966) (holding that the need to safeguard against subversion did not justify compelled disclosure of individual's political and associational past without a compelling state interest).

74. 357 U.S. 449 (1958) (holding the state's interest insufficient to override appellant's

Alabama sought to prevent the National Association for the Advancement of Colored People (NAACP) from conducting activities within its boundaries. It did so by enforcing a law that required out-of-state corporations to meet certain licensing qualifications. Relying on this statute, the Attorney General of Alabama sought production of a large number of the NAACP's records, including lists of "all Alabama 'members' and 'agents' of the Association."[75]

The Supreme Court's decision in this case began by noting that the NAACP was engaged in a collective effort with lawful goals. As the Court observed, the NAACP's goal was to "foster beliefs" it had "the right to advocate."[76] Disclosure of the NAACP's membership list to the state would, however, adversely affect the organization's ability to carry out its mission. The Association "made an uncontroverted showing that on past occasions revelation of the identity of its rank-and-file members had exposed these members to economic reprisals, loss of employment, threat of physical coercion, and other manifestations of public hostility."[77] The Court declared that the right to associate for expressive activity could be limited only if (1) the restriction served a compelling governmental interest unrelated to the supression of ideas and (2) more narrowly tailored means were unavailable to further this state interest.[78] The absence of such a showing by Alabama and the presence of proof of a pattern of past coercion and threats of such future activity led the Supreme Court to find that Alabama's data collection scheme represented an unconstitutional infringement of the right of association of the NAACP's members.[79]

The Supreme Court's protection of associational privacy reveals that American law does not always view privacy as merely synonymous with isolation. In *NAACP v. Alabama* and its other group privacy decisions, the Court recognized that disclosure of membership information can have highly negative consequences for individuals.[80] Indeed, the threat of this

---

First Amendment right to political and associational privacy).

75. Id. at 453.

76. Id. at 463.

77. Id. at 462. For an astonishing example of a state spying on such civil rights organizations, see American Civil Liberties Union of Miss. v. Mississippi, 911 F.2d 1066 (5th Cir. 1990). This case concerned the records of the Mississippi State Sovereignity Commission, a governmental organization created in 1956 that "was the state's secret intelligence arm, committed and devoted to the perpetuation of racial segregation in Mississippi." Id. at 1068. This organization's "intrusive reach into people's private lives was often not only surreptitious but also marked by dire consequences." Id. at 1068, n.1. For a journalist's recent account of the activities of the Mississippi State Sovereignty Commission, see Calvin Trillin, A Reporter at Large: State Secrets, The New Yorker, May 29, 1995, at 54.

78. NAACP v. Alabama, 357 U.S. at 463-65.

79. Id. at 464-65.

80. *See, e.g.*, Gibson v. Florida Legislative Investigative Comm., 372 U.S. 539, 557 (1963) (alluding to a "chilling" effect on the free exercise of constitutionally enshrined rights of free speech, expression, and association which could result if the Court failed to protect the privacy of organization's membership lists); Bates v. Little Rock, 361 U.S. 516, 524 (1960)

intimidation comes not only from the state, but also from private parties.[81] These cases show that "disclosure [by the state] may become a sanction in a hostile community."[82] Group status forms a part of and helps safeguard individual status; as a result, the Court in the *NAACP* case found "group privacy" important as a condition for individual participation in the political process. Constitutional limits on the state's collection and application of personal information relating to group membership protect participation in political self-government.[83]

2. *The Right to Vote*

The health of a democratic system requires not only protection of information regarding group political activity, but also judicial attention to the impact of data processing on the right to exercise the electoral franchise. This scrutiny is necessary because certain kinds of uses of information can impinge on the right to vote and thereby interfere directly with the individual's participation in political self-governance.[84] A state statute involving data collection or processing that interferes with the right to vote should be subject to searching judicial scrutiny.[85] In such cases, the critical constitutional provisions implicated by such information use are the Equal Protection Clause, the Fourteenth Amendment, and the First Amendment.[86]

(observing that identification of NAACP members resulted in "harassment and threats of bodily harm"); NAACP v. Alabama, 357 U.S. at 462 (noting that membership disclosure leads to "economic reprisal, loss of employment, threat of physical coercion, and other manifesting of public hostility").

81. Harry Kalven, The Negro and the First Amendment 93 (1965).

82. Id. at 120.

83. For an excellent example of a lower court applying the notion of group privacy to protect informational privacy, see Paton v. La Prade, 469 F.Supp. 773, 776-77 (D.N.J. 1978).

84. The Supreme Court has given a clear and concise explanation for its finding that the right to vote is no less than a "fundamental" constitutional interest. In *Reynolds v. Sims*, 377 U.S. 533, 561-62 (1964) the Court stated,

> [The] right to suffrage is a fundamental matter in a free and democratic society. Especially since the right to exercise the franchise in a free and unimpaired manner is preservative of other basic civil and political rights, any alleged infringement of the right of citizens to vote must be carefully and meticulously scrutinized.

85. In the words of the Supreme Court, "[n]o right is more precious in a free country than that of having a voice in the election of those who make the laws under which, as good citizens, we live. Other rights, even the most basic, are illusory if the right to vote is undermined." Wesberry v. Sanders, 376 U.S. 1, 17 (1976). Before the state can interfere with the right to vote, it must meet the "strict scrutiny" test. This kind of judicial scrutiny requires the state to show it has a "compelling" interest in a contested regulation that is "narrowly tailored" to minimize the interference with the fundamental interest. Hill v. Stone, 421 U.S. 289, 297 (1975); Kramer v. Union Free School Dist. No. 15, 395 U.S. 621 (1969); Harper v. Virginia Bd. of Elections, 383 U.S. 663 (1966).

86. In addition to the important protections offered the electoral process by the Fifteenth, Nineteenth, Twenty-fourth, and Twenty-sixth Amendments, the Supreme Court has read the Fourteenth Amendment, the Equal Protection Clause, and the First Amendment as placing restrictions on the power of the states to qualify the exercise of the franchise. *See*

A recent decision of the Fourth Circuit provides a good example of such judicial scrutiny. In *Greidinger v. Davis*,[87] the Fourth Circuit relied upon the Constitution's protection of voting rights to bar a state's data collection practices. The Virginia voter registration scheme required that all citizens otherwise qualified for the electoral franchise possess a Social Security Number (SSN) and provide this number on their application.[88] In Virginia, virtually anyone could obtain statewide voter registration lists containing the SSNs of voters.[89]

The Fourth Circuit found that the state's registration procedure conditioned the right to vote on disclosure of a SSN to the public.[90] Indeed, such public disclosure of SSNs imposed a "substantial burden" on the right to vote because of an individual's justifiable concern for confidentiality of her SSN.[91] The *Greidinger* court observed, "Succinctly stated, the harm that can be inflicted from the disclosure of a SSN to an unscrupulous individual is alarming and potentially financially ruinous."[92] By conditioning the electoral franchise on public dissemination of SSNs, Virginia had created an intolerable burden on the right to vote.[93] The Fourth Circuit ordered the state to "cure this constitutional infirmity by either deleting the requirement that a registrant disclose his SSN or eliminating the use of SSNs" in voter registrations lists and other records

---

Storer v. Brown, 415 U.S. 724, 729 (1974) ("[S]ubstantial burdens on the right to vote or associate for political purposes are constitutionally suspect and invalid under the Equal Protection Clause unless essential to serve a compelling state interest.").

87. 988 F.2d 1344 (4th Cir. 1993).

88. Id. at 1345. "The SSN is a nine-digit account number assigned by the Secretary Department of Health and Human Services for the purpose of administering the Social Security laws." Id. at 1352. It is also used for identification purposes in numerous other governmental programs and within the private sector. Id. at 1352-53. For a further discussion of the SSN, see Schwartz, supra note 18, at 1355-56 nn.164-65.

89. *Greidinger*, 988 F.2d at 1345. With some restrictions, the law in question permitted disclosure to: (1) any registered voter, (2) candidates in certain elections, (3) political party committees, (4) incumbent office holders, and (5) nonprofit organizations which promote voter participation and registration. Id.

90. Id. at 1352.

91. Id. at 1354.

92. Id. The court noted, "For example, armed with one's SSN, an unscrupulous individual could obtain a person's welfare benefits or Social Security benefits, order new checks at a new address on that person's checking account, obtain credit cards, or even obtain the person's paycheck." Id. at 1353. In addition, the *Greidinger* court observed, "Other uses [of the SSN] include unlocking the door to another's financial records, investment portfolios, school records, financial aid records, and medical records." Id. at 1354 n.9.

93. Virginia's legislation scheme compelled "a would-be voter . . . to consent to the possibility of a profound invasion of privacy when exercising the fundamental right to vote." Id. at 1354. Virginia could have defended the burden on voting only if it first advanced a compelling state interest that justified the disclosure and dissemination of SSNs and then indicated that it had narrowly tailored its treatment of the SSNs to minimize the burden on voters. Id.

The *Greidinger* court found that Virginia had a compelling interest in preventing voter fraud and encouraging voter participation. The furthering of these interests, however, did not require the state to disclose SSNs to private individuals. Id. at 1354-55.

open to the public and various organizations.[94]

Similar to the protection of associational privacy in *NAACP v. Alabama*,[95] this voting rights case attempts to limit disclosure of data in order to protect deliberative democracy. Such judicial activity reflects a belief that informational privacy is an integral part of the political process. To keep the channels of political change open, constitutional restrictions must be placed on the state's treatment of information regarding both group affiliation and the electoral franchise. Yet, constitutional attention must also be paid to deliberative autonomy. Beyond participation in political activities, constitutional protection must extend to deliberations about how to live one's life. Even in the absence of a connection with group privacy or voting rights, deliberative autonomy is worthy of its own constitutional protection. This Article will consider attempts at protecting deliberative autonomy through the Fourth Amendment and the right of informational privacy announced by the Supreme Court in *Whalen v. Roe*.[96]

3. The Fourth Amendment

The Fourth Amendment to the United States Constitution protects individuals from unreasonable searches and seizures. Its text establishes "[t]he right of the people to be secure in their persons, houses, papers and effects, against unreasonable searches and seizures."[97] This amendment should provide an important basis for protection of personal information from unreasonable government action. Yet, judicial application of the Fourth Amendment leaves it capable of protecting little more than informational seclusion. Isolated in her home, or within the confines of her residence's curtilage, the individual has, at least in some circumstances, an expectation of privacy that the Constitution does safeguard.[98] Outside of this limited space, however, the Fourth Amendment provides far less protection.

The Fourth Amendment's weakness in this context is due to the Supreme Court's established methodology for deciding when searches or seizures are protected by this constitutional provision. In evaluating

---

94. *Greidinger*, 988 F.2d at 1355.

95. 357 U.S. 449 (1958). For further discussion concerning NAACP v. Alabama, see supra notes 74-83 and accompanying text.

96. 429 U.S. 589 (1977) (unanimous decision).

97. U.S. Const. amend. IV.

98. *See* Minnesota v. Olson, 495 U.S. 91, 96-97 (1990) (holding that an overnight guest has Fourth Amendment privacy interest during stay in host's home); Florida v. Riley, 488 U.S. 445, 449-52 (1989) (discussing Fourth Amendment's protection of area within the curtilage of home and shielded from view by a fence); Oliver v. United States, 466 U.S. 170, 177-82 (1984) (discussing lack of Fourth Amendment protection for marijuana grown in open field). *See also* United States v. Karo, 468 U.S. 705, 713-715 (1984) (concluding that monitoring of a beeper placed in a container is permissible when a car moves along the public highways, but not when container is placed within private residence which is "a location not open to visual inspection").

whether governmental conduct impinges upon the Fourth Amendment, the Supreme Court looks at the expectations of individuals and of society. Governmental action will be limited by the Fourth Amendment only if the object of the search has at stake an actual, subjective expectation of privacy, and society is prepared to recognize this expectation as reasonable.[99] As a result, the Supreme Court's test for the application of the Fourth Amendment looks at both the individual's personal expectation regarding the activity in question and the social verdict regarding her expectation of privacy.[100] This approach to the Fourth Amendment has two critical shortcomings.

First, the Supreme Court has found that reasonable expectations of privacy attach neither to activities that take place in "public" nor to objects controlled by a third party. If the State can see the activity, whether with the naked eye of its officials or with the enhancement of technology, or can find evidence of it elsewhere, the Fourth Amendment offers no shield for the individual.[101] As a result of this approach, the Court has found this Amendment to be inapplicable to documents in the control of one's accountant or financial records at one's bank.[102] Yet, much of the

---

99. Smith v. Maryland, 442 U.S. 735, 740 (1979) (quoting Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring)).

100. Id. For example, Justice White described the personal expectation of privacy of an individual who stays as a guest in someone's home: "From the overnight guest's perspective, he seeks shelter in another's home precisely because it provides him with privacy, a place where he and his possessions will not be disturbed by anyone but his host and those his host allows inside." *Olson*, 495 U.S. at 98-99.

The Supreme Court has often split, however, on the basic question of when an expectation of privacy exists. In Florida v. Bostick, the majority claimed to have considered all the circumstances in deciding whether police sweeps of buses in interstate or intrastate travel implicated the Fourth Amendment. *Bostick*, 501 U.S. 429, 435 (1991). However, the dissenting judges stated that suspicionless police sweeps of buses bear all the indicia of an unjustified intrusion and violate core values of the Fourth Amendment. Id. at 450. The Court also has wrestled with assessing the expectation of privacy in one's luggage or in a closed container placed in one's vehicle, California v. Acevedo, 500 U.S. 565, 573-76 (1991); United States v. Chadwick, 433 U.S. 1, 13 (1977), or in one's moving vehicle itself, Chambers v. Maroney, 399 U.S. 42, 48-52 (1970).

101. *Riley*, 488 U.S. at 449-52 (White, J., plurality opinion) (upholding helicopter surveillance of marijuana growing in a greenhouse on an individual's property); *Oliver*, 466 U.S. at 177-82 (discussing lack of Fourth Amendment protection for marijuana grown in open field); *Smith*, 442 U.S. at 741-46 (holding that the Fourth Amendment does not prevent police from installing pen register at telephone company's office to record numbers dialed from telephone at individual's home).

The Supreme Court generally has a positive reaction to the application of technology to enhance the state's ability to monitor activities. *See, e.g.*, United States v. Knotts, 460 U.S. 276, 282 (1983) (addressing the constitutionality of using a "beeper" device to monitor a closed container's location and concluding that "nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case").

102. United States v. Miller, 425 U.S. 435, 442-43 (1976); Couch v. United States, 409 U.S. 322, 335-36 (1973).

In a similar fashion, lower courts have held the Fourth Amendment to be inapplicable

government's use of personal data involves information that is outside an individual's control. The Fourth Amendment provides little protection for personal information already controlled by third parties or the government itself.

Second, the Supreme Court's search for reasonable expectations of privacy is tautological. The Fourth Amendment is held to be applicable in those circumstances in which people reasonably expect it to be applicable.[103] Thus, when a desire for privacy is incommensurate with the general social view of reasonable privacy (or, more accurately, the Supreme Court's estimation of this view), Fourth Amendment protection does not exist. This amendment applies only when society already awaits it. In the context of data protection, this circular approach ignores the silent ability of technology to erode our expectations of privacy. Technology is developed, installed, and applied in a complex social process which tends to have, at best, a secondary concern for privacy. Yet, post facto, the Supreme Court accepts as a given the apparently lowered expectations of privacy resulting from new technology.

As one example of judicial acceptance of such post facto, lowered privacy expectations, the Supreme Court has found that electronic surveillance by third parties wearing a hidden audio bug is not subject to the Fourth Amendment's protection.[104] According to the Court, we all know, after all, that anyone we talk with might wear such a device; thus,

---

to governmental observation of one's listing of her return address on an envelope—after all, this information is visible to any number of postal workers, United States v. Choate, 576 F.2d 165, 174-77 (9th Cir.), *cert. denied*, 439 U.S. 953 (1978); United States v. Bianco, 534 F.2d 501, 507-08 (2d Cir. 1976).

103. *See Riley*, 488 U.S. at 451-52 (White, J., plurality opinion) ("[T]here is nothing in the record or before us to suggest that helicopters flying at 400 feet are sufficiently rare in this country to lend substance to respondent's claim that he reasonably anticipated that his greenhouse would not be subject to observation from that altitude."); California v. Ciraolo, 476 U.S. 207, 215 (1986) ("In an age where private and commercial flight in the private airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.").

Sometimes, however, the Court has explained why a certain expectation of privacy matters to the individual and society. Justice White discussed the privacy interest implicated when one stays as an overnight guest in someone's home in terms of social values and the needs of the individual:

> Staying overnight in another's home is a longstanding social custom that serves functions valuable by society. We stay in others homes when we travel to a strange city for business or pleasure, when we visit our parents, children, or more distant relatives out of town, when we are in between jobs or homes, or when we house-sit for a friend. We will all be hosts and we will all be guests many times in our lives. . . .
>
> . . . . We are our most vulnerable when we are asleep because we cannot monitor our own safety or the security of our belongings.

Olson, 459 U.S. at 98-99.

104. United States v. White, 401 U.S. 745, 753 (1971) (plurality opinion); Lopez v. United States, 373 U.S. 427, 440 (1963).

there can be no reasonable expectation of privacy in such conversations.[105] To give another example, in deciding the Fourth Amendment's applicability to government snooping from fixed winged aircraft or helicopters, the Supreme Court has placed significant weight on federal safety regulations concerning an apparently unrelated topic: the heights at which such aircraft may be operated.[106] For the Court, however, such safety regulations demonstrate the presence of aircraft at a given height, and the resulting absence of any reasonable expectation of privacy from observation by these planes and helicopters. Absent from such an approach is a sense that some searches are unreasonable because of their negative impact on a free society.[107]

The "reasonable expectation of privacy" approach is a threshold test that keeps the Fourth Amendment from being applied in many contexts of informational privacy. As an initial matter then, the Fourth Amendment is often inapplicable. When the Fourth Amendment *is* applied, or rather, when a reasonable expectation of privacy is present, the Supreme Court still allows privacy to be invaded provided warrants based on probable cause are issued. Judges and magistrates have signed warrants authorizing audio bugs to be placed in a target's home and even in her bedroom.[108] Here, the test is usually not the reasonableness of the search, but the existence of probable cause to carry out a search. The Fourth Amendment simply requires that a court issue a search warrant based on a good probability of finding sought-after items or information. If the state can demonstrate probable cause, even the individual's seclusion within a zone of spatial privacy can be invaded. [109]

4. Informational Privacy

In its important decision in *Whalen v. Roe*,[110] the Supreme Court began the process of identifying the elements of an American constitution-

---

105. *White*, 401 U.S. at 752.

106. *Riley*, 488 U.S. at 451-52; *Ciraolo*, 476 U.S. at 215.

107. *See Riley*, 488 U.S. at 457 (Brennan, J., dissenting) (noting that the Court should consider whether police activity is consistent with the "'aims of a free and open society'" (citing Anthony G. Amsterdam, Perspectives on the Fourth Amendment, 58 Minn. L. Rev. 349, 403 (1974)); *see also* Jerry L. Mashaw, Due Process in the Administrative State 169 (1985) ("The question is not what rights are natural to persons, but what rights persons must have to maintain a particular liberal-democratic polity."); Silas J. Wasserstrom & Louis M. Seidman, The Fourth Amendment as Constitutional Theory, 77 Geo. L.J. 19, 30-34 (1988) (discussing the paucity of Supreme Court efforts in deciding what makes an unreasonable search).

108. *See* Akhil R. Amar, Fourth Amendment First Principles, 107 Harv. L. Rev. 757, 802-03 (1994) ("In love with the warrant, the Court has blessed hidden audio and video bugs—apparently even ones that must be installed by secret physical trespass—so long as these bugs are approved in advance by judicial warrant.") (citations omitted).

109. Professor Amar has made an ambitious attempt to re-orient the Fourth Amendment. Id. at 800-19. He emphasizes the Fourth Amendment's textual emphasis that "all searches and seizures be reasonable," id. at 759, and argues that judges and juries need to play a new, critical role in evaluating constitutional reasonableness. Id. at 800-19.

110. 429 U.S. 589 (1976) (unanimous decision).

al right of informational privacy. This case concerned a New York law that created a centralized state computer file of the names and addresses of all persons who obtained certain drugs pursuant to a doctor's prescription.[111] While upholding the state's exercise of power, the Supreme Court found this governmental gathering of information to affect two interests. One was an "individual interest in avoiding disclosure of personal matters"; the other, "the interest in independence in making certain kinds of important decisions."[112]

The first *Whalen* interest has led to the development of an American right of informational privacy focused on an individual's capacity for participation. Some lower courts applying this concept of a nondisclosure interest consider the impact on deliberative autonomy of the state's collection of personal information. At the same time, other lower courts read *Whalen* as establishing only a limited right to informational seclusion, which, as might be expected, generally has been found *not* to merit protection. *Whalen* and its progeny reveal an American constitutional right of informational privacy that is suspended between privacy paradigms of participation and seclusion.

a. "[A]voiding disclosure of personal matters"

The first privacy interest that the Supreme Court identified in *Whalen* was in "avoiding disclosure of personal matters."[113] To check whether the interest in nondisclosure was protected, the Court first discussed the possibility that health department employees would fail to maintain proper security.[114] At the very start of its opinion, the Court examined the security measures that the State of New York had created.[115] These standards required that the original prescription forms be stored in a vault in a room surrounded by a wire fence and guarded with an alarm system, and that all prescription forms ultimately be destroyed.[116] The Court found that these actions were well designed to ensure that the personal information would be kept safe from public disclosure.[117]

In addition to expressing this concern for data security, the *Whalen* Court engaged in analysis of the government's plans for the data. In particular, it discussed the possibility that the health department would offer the stored data as evidence in court proceedings.[118] The Court also reprinted the relevant statutes governing the collection and application of

111. Id. at 592-93.
112. Id. at 599-600.
113. Id. at 599.
114. Id. at 600.
115. Whalen, 429 U.S. at 593-94 (discussing the district court's findings and opinion).
116. Id.
117. Id. at 601-02.
118. Id. at 600.

the personal information in a footnote to its opinion.[119] The *Whalen* Court found that the applicable statutory safeguards adequately protected the interest in avoiding public disclosure of personal matters. There was no "proper ground for attacking the statute as invalid on its face."[120]

One potential weakness of the first *Whalen* interest is its seemingly exclusive concern with the government's "public" disclosure. The *Whalen* opinion might appear to hold that so long as access to the data remains limited to the government, no privacy interest is implicated. Thus, protection of the first part of the constitutional right to informational privacy would seem to require the estimation of the likelihood that the public will gain access to personal data collected by the government. Yet, attention to a notion of privacy as participation additionally requires the analysis of the impact of *governmental* knowledge and application of personal data — not merely the consideration of the result of *public* knowledge when the government releases such information.

Later decisions of lower courts have found, although not uniformly, that *Whalen*'s nondisclosure interest applies not only to the government's plans to disclose information in its control, but also to the government's initial request for the information.[121] Such a reading represents an important development in the American constitutional right of informational privacy. As a result, the interest in nondisclosure has been held to apply to the government's request for information regardless of whether the public will ever gain access to the personal data. The identification of a plan for data collection that affects this interest does not, however, end a court's task.

Whalen establishes that the right of individuals to control access to their information is not absolute. The better-reasoned of the lower court decisions following *Whalen* develop a contextual analysis for weighing the impact of governmental data collection on privacy as participation. Courts have looked at a number of factors in evaluating contested practices and statutes concerning data processing. Most importantly, courts have considered: the nature of the statutory mandate requiring information collection; the potential for harm through future disclosures, including the damage that such disclosure will cause to the relationship in which the information was generated; the degree of the state's need for access to the information; and the adequacy of the safeguards to prevent unauthorized

---

119. Id. at 594 n.12.

120. Whalen, 429 U.S. at 601.

121. For a sampling of these cases, see Doe v. Attorney Gen., 941 F.2d 780, 795-97 (9th Cir. 1991); Thorne v. City of El Segundo, 726 F.2d 459, 468-69 (9th Cir. 1983); Fadjo v. Coon, 633 F.2d 1172, 1175-77 (5th Cir. 1981); United States v. Westinghouse, 638 F.2d 570, 575-78 (3d Cir. 1980); Hodge v. Carroll County Dept. of Social Servs., 812 F.Supp. 593, 600-02 (D. Md. 1992); Soucie v. County of Monroe, 736 F.Supp. 33, 35-36 (W.D.N.Y. 1990). *But see* General Motors Corp. v. Nat'l Inst. for Occupational Safety and Health, 636 F.2d 163, 166 (6th Cir. 1980), *cert. denied*, 454 U.S. 877 (1981).

disclosures.[122]

This approach was carried out by a federal district court in *Doe v. Borough of Barrington*.[123] In this case, local law enforcement officers' had disclosed the plaintiff's positive HIV test result to his neighbor.[124] Following this disclosure, the neighbor in question quickly contacted the local media and parents in the school where the plaintiff's children were enrolled.[125] According to the *Barrington* court, a panic in the school followed, parents removed their children from this institution, and members of the family of the individual with HIV felt "shunned by the community."[126]

In applying *Whalen*, the *Barrington* court initially noted "the stigma and harrassment that comes with public knowledge of one's affliction with AIDS."[127] This knowledge can lead an "entire family to be ostracized."[128] Although under some circumstances the government might choose to release such information, in this case the state's interest did not justify such action.[129] In the district court's words, the police officer's disclosure to the neighbor served no state interest "because there was no threat of transmission [of AIDS] present."[130] The *Barrington* court found that the municipality in question was liable not only for the disclosure, but also for its failure to train its police "to keep confidential one's infection with the AIDS virus."[131]

As *Barrington* indicates, the federal judiciary can play a significant role in hearing objections to the state's data processing laws and its practices regarding the application of personal information. In this way, *Whalen* and some of its progeny have created a significant constitutional component to the law of data protection in the United States. These decisions have carefully evaluated the impact of the state's application of personal information on individual self-determination. Unfortunately, other courts have read the first *Whalen* interest more restrictedly. According to these courts, the right of informational privacy applies only when the underlying information concerns fundamental constitutional rights. In this view, *Whalen* protects only a limited range of information: data about activities to which the Supreme Court has already extended the protections of substantive due process privacy.[132]

---

122. *Doe*, 941 F.2d at 795-97; *Thorne*, 726 F.2d at 468-69; *Westinghouse*, 638 F.2d at 575.
123. 729 F.Supp. 376 (D.N.J. 1990).
124. Id. at 378.
125. Id. at 379.
126. Id.
127. Id. at 384.
128. *Barrington*, 729 F. Supp. at 385.
129. Id.
130. Id.
131. Id. at 389.
132. *See, e.g.*, Ramie v. City of Hedwig Village, 765 F.2d 490, 492 (5th Cir. 1985) (holding that police did not violate plaintiff's right to privacy by questioning plaintiff about her religious beliefs and gender); Plante v. Gonzales, 575 F.2d 1534, 1539 (5th Cir. 1978), *cert.*

In its established jurisprudence, the Supreme Court's application of substantive due process privacy requires "strict scrutiny" review of governmental measures that affect certain protected areas and activities.[133] The Court currently engages in such review only when the state impinges upon fundamental activities or decisions that are so important that "neither liberty nor justice would exist if [they] were sacrificed."[134] In carrying out such scrutiny, the Court applies the test of whether an activity is "implicit in the concept of ordered liberty."[135] Once this test is passed, judicial evaluation of a challenged regulation of the activity entails a search for a heightened justification for the state's measure.[136]

The Supreme Court's application of substantive due process has protected the individual from state interference in certain aspects of child-rearing or in decisions regarding the procreative consequences of sexual activities.[137] This constitutional doctrine also insulates individuals who engage in certain other activities from collective political action.[138] Under the influence of these decisions, some courts have viewed *Whalen*'s nondisclosure interest as placing limits only on the state's processing of personal data relating to activities already protected by substantive due

---

denied, 434 U.S. 1129 (1979) (holding that mandatory financial disclosure for elected officials is constitutional).

133. *See, e.g.*, Roe v. Wade, 410 U.S. 113 (1973) (finding that pregnant women have a fundamental right of privacy); Griswold v. Connecticut, 381 U.S. 479, 481-86 (1965) (finding a fundamental right of marital privacy); Pierce v. Society of Sisters, 268 U.S. 510, 534-35 (1925) (holding compulsory public school attendance a violation of parental right to direct the educational upbringing of their children).

134. Bowers v. Hardwick, 478 U.S. 186, 191-92 (1986) (alteration in original) (quoting Palko v. Connecticut, 302 U.S. 318, 326 (1937)); *see* Moore v. City of East Cleveland, 431 U.S. 494, 503 (1977).

135. *Palko*, 302 U.S. at 325-326.

136. *Compare* Kelley v. Johnson, 425 U.S. 238, 247-48 (1976) (finding that governmental grooming requirements for members of police force impinge upon no "fundamental" interest and therefore must only be "rational" to be upheld) *with* Roe v. Wade, 410 U.S. at 152-55 (finding the right of privacy of pregnant woman is "fundamental" and therefore, can be impinged upon only when state has a "compelling" interest).

In the context of abortion, the Court has, however, found that a middle range of state measures, those that place no "undue burden" on the fundamental right in question, are subject to less intense judicial scrutiny. *See* Planned Parenthood v. Casey, 112 S.Ct. 2791 (1992) (plurality opinion) (arguing that the state may regulate abortion in numerous ways, but it may not place an "undue burden" on a woman's ability to decide whether to terminate her pregnancy).

137. For cases dealing with child rearing and the family, see Prince v. Massachusetts, 321 U.S. 510 (1925); Meyer v. Nebraska, 262 U.S. 390 (1923). For cases dealing with procreation, see Carey v. Population Servs., 431 U.S. 678 (1977); Eisenstadt v. Baird, 405 U.S. 438 (1972). For an argument that these cases now protect only the individual as such, rather than the individual as a member of a family unit, see Janet L. Dolgin, The Family in Transition From Griswold to Eisenstadt and Beyond, 82 Geo. L.J. 1519 (1994).

138. *See, e.g.*, Moore v. City of East Cleveland, 431 U.S. 494 (1977) (plurality opinion) (finding the tradition of extended family sharing a household to be deserving of constitutional protection).

process.[139] This interpretation attempts to preserve the individual's informational seclusion; it seeks to isolate from the state's grasp information trails left by certain important behavior.[140]

In developing a model of data protection, this Article has argued for the necessity of a retreat from this paradigm of information seclusion.[141] When conceived of as a right to be let alone, the value of privacy tends to collapse in light of the significant reasons for seeking personal information. Yet, judicial restriction of the *Whalen* nondisclosure interest only to fundamental rights creates just such a limited right to information seclusion. The Fourth Circuit's decision in *Walls v. City of Petersburg* provides a superb illustration of the limited utility of this interest.[142] Indeed, an ironic juxtaposition is possible between *Walls* and *Greidinger v. Davis*,[143] another Fourth Circuit decision. Although it protected deliberative democracy in *Greidinger*,[144] a voting rights case, the Fourth Circuit was far less sensitive to the issue of deliberative autonomy in *Walls*.

Walls concerned a city employee who lost her job after refusing to answer an official questionnaire.[145] The questionnaire's most objectionable inquiry was "Question 40," which asked, "Have you ever had sexual relations with a person of the same sex?"[146] For the Fourth Circuit, although "[t]he relevance of this question to Walls' employment is uncertain, . . . Question 40 does not ask for information that Walls has a right to keep private."[147] No right to keep this information from the state existed because the Supreme Court in *Bowers v. Hardwick* had explicitly rejected "'the proposition that any kind of private sexual conduct between consenting adults is constitutionally insulated from state proscription.'"[148] The Fourth Circuit reasoned that the absence of a constitutional right to engage in sexual relations with members of the same sex permitted the state to require its employees to reveal whether they engaged in such behavior.[149]

Those courts that read *Whalen* as concerned only with fundamental rights find that only a limited dimension of privacy is to be protected. These courts focus on privacy as it relates to the information trails of a narrow group of fundamental activities. If no such activity is at stake, no constitutional right of informational privacy is implicated.[150] Yet, even

---

139. Ramie v. City of Hedwig Village, 765 F.2d 490 (5th Cir. 1985); J.P. v. DeSanti, 653 F.2d 1080 (6th Cir. 1981); Plante v. Gonzalez, 575 F.2d 1119 (5th Cir. 1978).

140. *Cf. Ramie*, 765 F.2d at 492 (stating that the "Constitution is violated only by invasions of privacy involving the most intimate aspects of human affairs").

141. *See* supra part I.A.

142. 895 F.2d 188 (4th Cir. 1990).

143. 988 F.2d 1344 (4th Cir. 1993).

144. Id.

145. *Walls*, 895 F.2d at 190.

146. Id.

147. Id. at 193.

148. Id. (citing Bowers v. Hardwick, 478 U.S. 186, 191 (1986)).

149. Id.

150. For examples of cases holding that information in various kinds of records did not

when fundamental activities are at stake, courts rarely will place any meaningful constitutional limitations on the state's collection of personal information. The degree of information removable from collective political decisions will not be great. *Walls* illustrates not only a restrictive application of *Whalen* to information seclusion, but also the relative ineffectiveness of the approach when it is finally utilized.

In *Walls*, part of the contested questionnaire required city employees to supply detailed information concerning marriages, divorces, and the birth of children.[151] In light of the Supreme Court's established case law, this inquiry would appear to touch an area of substantive due process privacy. Yet, the *Walls* court decided not to apply "strict scrutiny" analysis, which usually accompanies substantive due process review, and, instead, used a different baseline test.[152] In deciding whether to protect information about "fundamental" activities, the *Walls* court considered the critical question to be whether such information was "freely available in public records."[153] Only to the extent that such "details [were] not part of the public record" could they be "private and thus protected."[154]

This approach is flawed in that it neglects to assign supremacy to the requirements of constitutional law.[155] To be sure, the Fourth Circuit's logic is reminiscent of the Supreme Court's attempt, in the context of the Fourth Amendment, to discover reasonable expectations of privacy through the presence or absence of statutes or regulations.[156] Nevertheless, the amount of *constitutional* protection due should not depend on the extent to which personal data collected by the state is already protected by statute or regulation. A second flaw with this approach is that it confuses the state's justification in collecting personal information for one purpose with constitutional permission for the *unlimited* application of it.[157] The state can justify the collection of virtually any personal data, no matter how intimate or, for that matter, how closely it is tied to constitutionally

---

implicate a fundamental right protected by the Constitution, see Gutierrez v. Lynch, 826 F.2d 1534, 1539 (6th Cir. 1987); J.P. v. DeSanti, 653 F.2d 1080, 1087-91 (6th Cir. 1981). *See also* Plante v. Gonzalez, 575 F.2d 1119, 1228-32 (5th Cir. 1978) (holding that financial privacy was not a fundamental right protected by the Constitution).

151. *Walls*, 895 F.2d at 193-94.

152. Id.

153. Id. at 193.

154. Id.

155. *See* U.S. Const., art. VI ("This Constitution, and the Laws of the United States which shall be made in Pursuance thereof . . . shall be the supreme Law of the Land. . . . ").

156. *See* supra part II.A.3.

157. In contrast to the approach of the Fourth Circuit in *Walls*, the Ninth Circuit has developed a far more careful approach to evaluating requests of the state for personal information. *See* Thorne v. City of El Seguendo, 726 F.2d 459, 469 (9th Cir. 1983), where the court observed:

> [T]he City must show that its inquiry into appellant's sex life was justified by the legitimate interests of the police department, that the inquiry was narrowly tailored to meet those legitimate interests, and that the department's use of the information it obtained about appellant's sexual history was proper in light of the state's interests.

protected behavior. The critical issue is whether the state's particular interest in a discrete application of personal information comports with constitutional standards.

The first *Whalen* interest, that in nondisclosure, has led to divergent approaches to data protection. Some courts have searched only for areas of already existing substantive due process protections. Their attention has been restricted to protecting privacy as information seclusion. Other courts, such as the district court in *Doe v. Barrington*, however, have examined how the collection and application of personal information by the government will affect the individual's self-determination. These courts have protected privacy as participation.

b. "[I]ndependence in decisionmaking"

The second *Whalen* interest consists of an individual's "independence in making certain kinds of important decisions."[158] According to the Supreme Court, the important decision at stake in *Whalen* was whether needed medicine could be acquired and utilized.[159] In contrast to the first *Whalen* right, this interest is clearly allied with substantive due process privacy's concerns for the protection of certain activities. Indeed, the *Whalen* Court immediately follows its initial enunciation of this branch of the right of informational privacy with a citation to such classic substantive due process decisions as *Roe v. Wade*,[160] *Griswold v. Connecticut*,[161] and *Pierce v. Society of Sisters*.[162] Yet, the Supreme Court leaves open the extent to which the second *Whalen* interest, like these cited decisions, is restricted only to fundamental interests.

Although the *Whalen* Court relies on the doctrinal basis provided by substantive due process, it also extends the constitutional protection offered important activities or decisions to *information* that reports activities or decisions. Extending protection this way is necessary because the processing and application of personal data can affect the independence of the activity or decision that generates the information. In *Whalen*, for example, the Court noted that "some patients [were] reluctant to use, and some doctors reluctant to prescribe," drugs that were medically indicated because of a fear that information would become "publicly known" and "adversely affect" their reputation.[163]

Despite this evidence of coercion, the Supreme Court found that the second aspect of the constitutional right of informational privacy was not violated by New York's data processing. Although some use of the drugs in question was discouraged by record-keeping, "the decision to prescribe, or

158. 429 U.S. 589, 599-600 (1977).
159. Id. at 602-04.
160. 410 U.S. 113 (1973).
161. 381 U.S. 479 (1965).
162. 268 U.S. 510 (1925). The citations are found at *Whalen*, 429 U.S. at 600 n.26.
163. *Whalen*, 429 U.S. at 600.

to use" remained with the physician and the patient.[164] The second *Whalen* interest represents a missed opportunity for the Supreme Court. Here, the Court should have built on the first *Whalen* interest and explored how independence in decisionmaking could be protected. The necessary judicial examination should look at the means of processing, the types of data bases to be linked, and the purposes for which the processed information will be utilized. Instead of adopting this approach to gauging the impact on decisionmaking, the *Whalen* Court simply inquired whether the freedom to choose to act was theoretically available. Yet, the abstract availability of a choice is less important than the question of whether the government's collection and processing of information will chill decisionmaking.

In contrast to the first *Whalen* interest, the second *Whalen* interest, that of independence in decisionmaking, has been almost entirely absent from judicial decisions.[165] Courts have applied the first *Whalen* interest, that of nondisclosure of personal information, in a mixed fashion, leaving room, however, in this doctrine for the development of a vigorous protection of a constitutional right of informational privacy as participation. Yet, courts have been reluctant to use the second *Whalen* interest as a bar to the state's information-gathering practices. Indeed, courts usually mention this interest only in passing on the way to their analysis of the first *Whalen* interest.[166]

B. Federal Legislation: The Privacy Act and the Participatory Model

This Article has examined constitutional law through the perspective of two norms: deliberative democracy and deliberative autonomy. Although higher law safeguards both values, it is more successful in addressing deliberative democracy. This Article will now examine statutory law, in which detailed, programmatic elements of data protection should be present. In particular, it will consider the presence in this area of law of the data protection model described in Part I.B. The essential elements of this model are: the creation of a statutory fabric defining obligations with respect to the processing of personal information; the maintenance of transparent processing systems; the assignment of limited procedural and substantive rights to the data subject; and the establishment of effective governmental oversight of data use.

Numerous pieces of federal legislation address the government's collection and application of personal information;[167] this Article will

---

164. Id. at 603.

165. For a brief mention of the second interest, see Mann v. University of Cincinnati, 824 F. Supp. 1190, 1198-99 (S.D. Ohio 1993).

166. Fadjo v. Coon, 633 F.2d 1172, 1174-76 (5th Cir. 1981); Faison v. Parker, 823 F.Supp. 1198, 1201-02 (E.D. Pa. 1993); Hodge v. Carroll County Dept. of Social Servs., 812 F.Supp. 593, 599-600 (D. Md. 1992); Soucie v. City of Monroe, 736 F. Supp. 33, 35-36 (W.D.N.Y. 1990).

167. *See e.g.*, 26 U.S.C. § 6103 (1988) (providing for confidentiality of tax returns and return information, but also permitting certain limited disclosures); 42 U.S.C. § 1305 (1988)

concentrate on the Privacy Act[168] and the Freedom of Information Act (FOIA).[169] The Privacy Act represents the most comprehensive attempt to structure information processing within the public sector.[170] It is an omnibus data protection measure that regulates how federal agencies collect personal information and apply it in decisionmaking. The Freedom of Information Act (FOIA) structures third-party access to federal records, including personal information in the control of federal agencies.[171]

The importance of the Privacy Act and FOIA arises from the key position of federal agencies in the ongoing deliberative process of government. Administrative agencies have a special role in the American state because they "fall between the extremes of the politically over-responsive Congress and the over-insulated courts."[172] Administrative agencies provide a unique forum for stimulating politically informed discourse. In the development of a consensus about the public good, they can foster the necessary kind of public deliberation. Yet, the collection of personal information by governmental agencies risks squelching such public discourse. Data gathering places pressure on individuals to conform to institutional standards of behavior. Even in the United States, a country endowed with a robust democracy, the law must carefully structure the government's collection and processing of information so that federal agencies can fulfill their potential for assisting the democratic order.

1. Creation of a Statutory Fabric of Defined Obligations

The Privacy Act reflects the first element of the data protection model by establishing requirements for agencies in their maintenance of records on individuals. In so doing, it recognizes the relation between privacy and participation. Indeed, the passage of this statute in 1974 reflected congressional awareness of the negative effect that data processing could have on the citizen's ability to join in social life. As the findings to the

---

(authorizing the application of social security disability records). For an analysis of the laws that authorize the collection of information in the program of Aid to Families with Dependent Children, see Schwartz, supra note 18, at 1355-60.

168. 5 U.S.C. § 552a (1988).

169. Id. § 552.

170. At the same time that the Privacy Act is fairly comprehensive by the standards of American data protection law, it is far narrower than the European data protection laws that establish general measures of data protection for government and the private sector. *See, e.g.*, Act 78-17 on Data Processing, Data Files and Individual Liberties § 15 (Fr.) *in* Data Protection Statutes, supra note 51; Act providing rules for the protection of privacy in connection with personal data files §§ 17, 23 (Neth.), *in* Data Protection Statutes, supra note 51.

In contrast to this European approach, the Privacy Act applies only to data in the control of one part of the government, namely federal agencies. 5 U.S.C. § 552a(a)(1) (1988). Moreover, the Privacy Act does not concern release of personal information from private organizations to agencies — only the application of such information by agencies once they have it. Gilbreath v. Guadalupe Hosp. Found. Inc., 5 F.3d 785, 791 (5th Cir. 1993).

171. 5 U.S.C. § 552(f).

172. Mark Seidenfeld, A Civic Republican Justification for the Bureaucratic State, 105 Harv. L. Rev. 1511, 1528 (1992).

Privacy Act declared, "the opportunities for an individual . . . are endangered by the misuse of certain information systems."[173]

The Privacy Act obliges agencies (1) to store only such personal information as is relevant and necessary,[174] (2) to collect information to the greatest extent practicable from the subject individual,[175] (3) to maintain records with accuracy and completeness,[176] and (4) to establish appropriate administrative and technical safeguards to assure the security of records.[177] It also sets in place detailed rules limiting the conditions for disclosure of an individual's records.[178] There are, however, two major weaknesses in the Privacy Act's attempt to define federal agency obligations concerning personal data: its "routine use" exemption and its provisions for computer matching.

a. The Routine Use Exemption

The Privacy Act prohibits the disclosure of records without the written request of "the individual to whom the record pertains."[179] The Act provides, however, no fewer than twelve disclosure exemptions to this prohibition.[180] If information falls within one of the exemptions, it can be disclosed and otherwise shared without the individual's permission. The excessively broad scope of some of these exemptions weakens the Privacy Act's attempt to set obligations for agencies' processing of personal data.

One exemption exists for disclosures to all federal law enforcement agencies.[181] A second disclosure exemption applies to various parts of the federal government, including both Houses of Congress.[182] Perhaps the

---

173. Privacy Act of 1974, Pub. L. No. 93-579, § 2(2), 88 Stat. 1896, 1896 (1974).
174. 5 U.S.C. § 552a(e)(1).
175. Id. § 552a(e)(2).
176. Id. § 552a(e)(5).
177. Id. § 552a(e)(10).
178. Id. § 552a(b).
179. 5 U.S.C. § 552a(b).
180. Id.
181. Id. § 552a(b)(7). *But see* Covett v. Harrington, 876 F.2d 751, 755 (1983) (suggesting that information collected for security clearance purposes would not be compatible with disclosure for criminal investigation).
182. 5 U.S.C. § 552a(b)(9). The congressional exemption concerns disclosure of agency information to Congress or its committees and subcommittees, but does not cover disclosures to individual congressmen. *See* Swenson v. U.S. Postal Serv., 890 F.2d 1075, 1077 (9th Cir. 1989) (stating that the congressional exemption "applies only to a house of congress or a committee or subcommittee, not to individual congressman").

Another disclosure provision establishes a "need to know" exemption. Section (b)(1) allows information to be disclosed without written permission "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). One court has interpreted the "need to know" exception as applying only to transfers of information *within* an agency and not *between* agencies. Britt v. Naval Investigative Servs., 886 F.2d 554, 547 (3d Cir. 1989).

To mention a final disclosure exemption, § 552a(b)(12) allows information to be transferred from the government to one kind of private organization without written

most controversial and frequently exploited exemption to the Privacy Act's limitations on disclosure is the "routine use" provision. The language of this exemption prevents an agency from disclosing records without "a written request by, or without the prior consent of, the individual to whom the record pertains, unless disclosure of the record would be . . . for a routine use."[183] Federal agencies have cited this exemption to justify virtually any disclosure of information without the individual's permission.[184] As currently applied, the routine use exemption undercuts the Privacy Act's attempt to create a statutory definition of obligations regarding personal information.

Although agencies have broadly applied the "routine use" exemption, the Privacy Act places definite statutory limitations on the application of the exemption. These limits require: (1) "*compatibility*" for a routine use;[185] (2) *actual notice* of the routine use to the individual to whom the record applies;[186] and (3) *publication* of all proposed routine uses in the Federal Register.[187] Of these limitations, the compatability requirement in particular makes clear that the exemption was not intended as a means for agencies to evade the Privacy Act's statutory obligations.

The compatibility limitation on the routine use exemption occurs in the definition section of the Privacy Act. Here, the Act declares, "the term 'routine use' means, with respect to the disclosure of a record, the use of such record for a purpose which is *compatible* with the purpose for which it was collected."[188] The principle of compatibility requires a significant degree of convergence and a concrete relationship between the purpose for which the information was gathered and its application.[189] This

---

permission of the data subject. This provision permits disclosure "to a consumer reporting agency." 5 U.S.C. § 552a(b)(12). Statutory limits are, however, placed on this disclosure exemption. *See* 31 U.S.C. § 3711(f)(1988).

183. 5 U.S.C. § 552a(b)(3).

184. Bennett, supra note 2, at 108-09; Todd R. Robert Coles, Does the Privacy Act of 1974 Protect Your Right of Privacy? An Examination of the Routine Use Exemption, 40 Am. U. L. Rev. 978, 985 (1991); Flaherty, supra note 2, at 323-24.

185. 5 U.S.C. § 552a(a)(7).

186. 5 U.S.C. § 552a(e)(3)(C). This statute requires such notice to be made by the agency "on the form which it uses to collect the information or on a separate form that can be retained by the individual." Id. § 552a(e)(3). The Privacy Act does not, however, explicitly require such actual notice before an agency can utilize the "routine use" exemption. The Ninth Circuit has sought to strengthen the publication limitation on the "public use" exemption. Reading the statutory scheme of the Privacy Act as a whole in Covert v. Harrington, 876 F.2d 751 (9th Cir. 1989), the court found that compliance with the requirement of actual notice of routine uses was obliged *before* agency reliance on the routine use exemption. The Ninth Circuit urged agencies "to inform . . . individuals . . . of the routine uses to which that information may be put." Id. at 756. According to the *Covert* court, supplying actual notice at the time that the agency collects information from the individual "is a sound and inexpensive policy." Id.

187. 5 U.S.C. § 552a(e)(4)(D).

188. Id. § 552a(a)(7) (emphasis added).

189. Britt v. Naval Investigative Servs., 886 F.2d 544, 549-50 (3d Cir. 1989); Swenson v. United States Postal Serv., 890 F.2d 1075, 1078 (9th Cir. 1989).

language places an important substantive limitation on the notion of a routine use, which, unfortunately, agencies generally have ignored.

Not only is the "routine use" exemption applied in a fashion that ignores relevant statutory language, such agency practice continues despite prolonged and well-placed criticism of it. As early as 1977, the Privacy Protection Study Commission, a blue-ribbon commission created by Congress at the time of the Privacy Act's enactment, noted its disapproval of overbroad applications of the routine use exemption.[190] In 1983, the House Committee on Government Operations issued a condemnation of such agency practice.[191] Three years later, the Congressional Office of Technology Assessment complained that the routine use exemption had become "a catchall exemption."[192] More recently, David Flaherty, in a pathbreaking comparative study of data protection law, *Protecting Privacy in Surveillance Societies*, called the American routine use exemption "a huge loophole."[193] Despite these comments, agencies continue to justify almost any use of information as a "routine use" of the data.

Such agency practice has not escaped the attention of the federal judiciary, which has placed some limits on the exploitation of the routine use exemption. Although some courts have upheld almost any kind of interagency sharing of data as a "routine use" authorized by the Privacy Act,[194] recently, other courts have taken an active role in enforcing the

---

190. Privacy Protection Study Comm'n, The Privacy Act of 1974: An Assessment 91-93 (1977).

191. House Comm. on Gov't Operations, Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress, H.R. Doc. No. 98-455, 98th Cong., 1st Sess. 41-53 (1983) [hereinafter 1983 House Committee Report].

192. Office of Technology Assessment, Electronic Record Systems and Individual Privacy 105 (1986) [hereinafter Electronic Record Systems].

193. Flaherty, supra note 2, at 323. Some level of Congressional awareness of abuse of the "routine use" exemption is indicated by the Privacy Act Amendments of 1991, H.R. 2443, 102nd Cong., 1st Sess. In this Bill, which was, however, never passed, Representative Robert Wise suggested two promising changes to the Privacy Act that pertain to the routine use exemption. First, the definition of a routine use disclosure would no longer rely on compatibility, but necessity. According to the amendment, a routine use should be for a purpose "which is necessary for the purpose for which [the record] was collected." Id. § 2(d). This language is much narrower than a disclosure for a compatible purpose.

The second proposed change in the Privacy Act prohibited reliance on a Federal Register publication of any routine use disclosure "which is contrary to, or which modifies the application of, any other condition of disclosure established by [the Privacy Act]." Id. § 3(3). This amendment prohibited agencies from creating a routine use notice that circumvents statutory limitations on disclosure. In introducing the Privacy Act Amendment of 1991, Rep. Robert Wise noted, for example, that agencies have exceeded the boundaries of the routine use exemption for disclosures in emergencies by writing notices that do not require notification to the individual. 137 Cong. Rec. H3449, 3451 (daily ed. May 22, 1991) (statement of Rep. Wise).

194. Andrews v. Veterans Admin., 838 F.2d 418 (10th Cir. 1988); Howard v. Marsh, 785 F.2d 645 (8th Cir. 1986), *cert. denied*, 479 U.S. 988 (1986); United States v. Miller, 643 F.2d 713 (10th Cir. 1981); Windsor v. Federal Executive Agency, 614 F.Supp. 1255, (D. Tenn. 1983), *aff'd*, 767 F.2d 923 (6th Cir. 1985); United States v. Collins, 596 F.2d 166 (6th Cir. 1979). *But*

existing statutory limitations on the routine use exemption. In particular, the Third and the Ninth Circuits have handed down important opinions enforcing the Privacy Act's "compatibility" and "notice" requirements.[195]

Unfortunately, these opinions have had minor impact on federal data use. This ineffectiveness is due to the Privacy Act's narrow scheme of remedies. Under the Privacy Act, a federal court cannot order an agency to do anything other than provide the data subject with access to her records, to amend inaccuracies in these documents, and to pay money, under limited circumstances, to injured individuals.[196] Beyond these remedies, it cannot order an agency to change its practices.[197] As a result, isolated judicial decisions have not changed the overall practices of federal agencies. The Privacy Act's limited remedies will be discussed at greater length in the section regarding the Act's assignment of rights to the individual.

b. Computer Matching

Data matching is the electronic comparison of two or more sets of records in order to find individuals included in more than one data base.[198] The federal government now carries out data matching on *billions* of records. One survey of only a small portion of federal matching programs identified data exchanges in one five-year period involving seven billion records.[199] Single matches have been carried out on as many as

---

see Tigerina v. Walters, 821 F.2d 789 (D.C. Cir. 1987).

195. In Britt v. Naval Investigative Servs., 866 F.2d 544 (3d Cir. 1989), the Third Circuit emphasized the importance of the compatibility requirement. It invalidated a claim of "routine use" because the planned application of information was different than the case-specific purpose for originally collecting the data. Id. at 550. The court held that "compatability" required a "concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure." Id. at 549-50.

Another case that stressed the importance of the compatibility requirement is Swenson v. United States Postal Serv., 890 F.2d 1075 (9th Cir. 1989). In this case, the Ninth Circuit found that the Postal Service had stated that its purpose in collecting certain data about its employees concerned equal opportunity issues and the performance of routine personnel functions. Id. at 1078. Therefore, the agency's Federal Register notices could not justify its disclosure to two congressmen of private facts about a mail carrier's employment status. The congressmen had written the Postal Service in reference to an undercounting of rural mail routes, which the mail carrier had brought to their attention. Id. at 1076. Since the Postal Service had not disclosed the personal information about the mail carrier for a purpose compatible with the purpose for which the data had been collected, the Postal Service's disclosure could not be a routine use. Id. at 1078.

196. 5 U.S.C. § 552a(g)(2).

197. Edison v. Department of the Army, 672 F.2d 840, 846 (11th Cir. 1982); Cell Associates v. National Insts. of Health, 579 F.2d 1155, 1161-62 (9th Cir. 1978).

198. Electronic Record Systems, supra note 192, at 38.

199. Senate Comm. on Gov't Affairs, The Computer Matching and Privacy Protection Act of 1987, S. Rep. No. 516, 100th Cong., 2d Sess. 5 (1988).

fifteen million records.[200]

Since passage of the Computer Matching and Privacy Protection Act, a major 1988 amendment to the Privacy Act,[201] the law provides for the regulation of the federal government's data matching. Congress enacted these amendments because the Privacy Act provided little protection to individuals who were subject to data matching.[202] Matches were often considered simply a "routine use" of data.[203] As a result, agencies were able to skirt the Privacy Act's requirement that individuals consent to the use of information for a purpose other than the one initially intended.[204]

The amended Privacy Act now provides for additional procedures, but creates no substantive guidelines to determine when matching is acceptable. It places decisions about computer matching in the hands of individual administrative agencies, which are obliged to follow certain procedures.[205] For example, the amended Privacy Act now prohibits the execution of matches absent a written agreement between the "source agency" and "recepient agency."[206] Moreover, before an agency engages in data matching, it must carry out a cost/benefit analysis.[207] The General Accounting Office (GAO) has found, however, that agency analysis is problematic in nature.[208] Part of the problem is methodological: Standard guidelines do not exist for calculations of costs and benefits.[209] The GAO also discovered many shortcomings in the quality of the agencies' cost/benefit analyses as actually executed.[210] A final procedural requirement of the Computer Matching Act is that Data Integrity Boards be established within each agency before it may participate in matching agreements.[211]

---

200. Electronic Record Systems, supra note 192, at 53.

201. Computer Matching and Privacy Protections Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (1988).

202. *See* Committee on Government Operations, Computer Matching and Privacy Protection Act of 1988, H.R. Rep. No. 100-802, 100th Cong., 2d Sess. 3107, 3114 (1988) (stating that "[f]ederal law in this area [is] disjointed") [hereinafter cited as Legislative History, Computer Matching Act]; Electronic Record Systems, supra note 192, at 57 ("The Privacy Act as presently interpreted by the Courts and OMB guidelines offers little protection to individuals who are the subjects of computer matching.").

203. Electronic Record Systems, supra note 192, at 57.

204. 5 U.S.C. § 552a(b)(1988). The Privacy Act also requires that an agency "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." Id. at (e)(2).

205. Id. § 552a(r).

206. Id. § 552a(o)(1).

207. Id. §§ 552a(o)(B), 552a(u)(4)(A).

208. *See generally*, General Accounting Office, Computer Matching: Quality of Decisions and Supporting Analyses Little Affected By 1988 Act (1993) [hereinafter GAO, Computer Matching].

209. *See* id. at 22-24 (discussing the lack of standard guidelines in cost-benefit analyses).

210. *See* id. at 24-29 (citing the problems with the quality of agencies' cost-benefit analyses).

211. *See* 5 U.S.C. § 552a(r) ("Each agency that proposes to establish or make a significant

In addition to these procedures required before matching, the Computer Matching Act also creates important protections for the individual *after* data matching is completed. The necessary protections are spelled out in section (p) of the amended Privacy Act.[212] The first of these centers on the extent to which independent verification of the personal data applied in a match is required before the agency takes action regarding the individual. The amended Privacy Act requires either: (1) that an agency official make an independent verification of information before "adverse action" may be taken against "any individual whose records are used in matching programs," or (2) that the information is limited to the identification and amount of benefits paid by a source agency under a Federal benefit program and that "there is a high degree of confidence that the information provided to the recepient agency is accurate."[213] By allowing information to be found generically accurate, the second alternative weakens the requirement of independent verification.[214]

The obligation of independent verification of data is accompanied by a potentially more important post-match agency requirement. The Privacy Act now requires, "notice from such agency containing a statement of its findings and informing the individual of the opportunity to contest such findings."[215] Although the Privacy Act does not create substantive requirements for deciding when a match is appropriate,[216] it provides some procedural protections for the individual, including this post-match opportunity to object to the accuracy of the results. Through such safeguards, this statute provides important post-match protections, which represent the most important contribution of the Computer Matching Act to data protection. These procedures do not, however, prevent either Congress or agencies from making decisions about data matching in a low profile, ad hoc fashion. Both usually act without considering how a discrete match will add to the surveillance of the individual.

2. *Maintenance of Transparent Processing Systems*

The second element of the data protection model is transparency, which requires the application of personal information to be structured in a manner understandable to individuals. The Privacy Protection Study Commission developed a similar concept, which it called "openness."[217]

---

change in a system of records or a matching program shall provide adequate advance notice. . . . "); § 552a (u)(3) (describing the Data Integrity Board's function within agencies as an internal check against misuse of matching programs).

212. 5 U.S.C. § 552a(p).

213. Id.

214. This provision was added to the Privacy Act in 1990 by Pub. L. No. 101-508, 104 Stat. 1388 (1990) (codified at 5 U.S.C. § 552a(p)(A)(ii) (1994)).

215. 5 USC § 552a(p)(3)(A).

216. *But see* GAO, Computer Matching, supra note 208, at 22 (suggesting, in Table 3.1, that loss of privacy be figured into the cost-benefit analysis).

217. Personal Privacy, supra note 49, at 14.

In its official report, issued in 1977, this blue-ribbon panel stated that "by opening up record-keeping practices and by giving an individual opportunities to interact easily with a record keeper, particularly at crucial points in a record-keeping relationship, both individuals and organization will benefit."[218]

The Privacy Act does provide for transparency in federal agencies' data processing. Yet, its success is limited by two familar shortcomings of the Act: the provisions for "routine usages" and for data matching. In looking at the effect of these provisions on transparency, this Section explores additional aspects of the routine use exemption; in particular, it will examine the Privacy Act's requirements of actual notice of routine use and publication in the Federal Register of information regarding such data use. This Section also examines the Freedom of Information Act (FOIA), which indicates that third party access to personal information can be compatible with data protection. The FOIA is well integrated with the Privacy Act; these two laws set effective limits on third party access to personal information controlled by the federal government.

a. The Privacy Act and Transparency

The Privacy Act contributes to the transparency of federal agency data use by providing individuals with a right to access and a right to correct their records.[219] These significant interests will be discussed at greater length as critical procedural and substantive rights in the Article's next section. The Privacy Act also establishes the general rule that an agency is to "collect information to the greatest extent practicable from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs."[220] The requirement that data be collected directly from the individual, combined with the law's insistence that the data subject's consent be given before information collected for one purpose is applied to another,[221] should greatly contribute to personal knowledge of federal data use.

Despite its promising language, however, the Privacy Act has not created openness in agencies' collection and application of personal information. Once again, the routine use provision and data matching are primarily responsible for this failure. As this Article has demonstrated above, agencies have turned the routine use exemption into a large loophole by ignoring the compatibility requirement. In addition, two other statutory restrictions on routine uses, the provisions concerning *actual notice* of routine uses to the individual, and *publication* of all intended routine

218. Id. at 19.
219. 5 U.S.C. § 552a(d).
220. Id. § 552a(e)(2).
221. *See* id. § 552a(b) (setting out the conditions of disclosure for agencies).

uses in the Federal Register, have proven to be of limited assistance in improving the transparency of agency data use.

The most promising of these two provisions in relation to transparency is the requirement of actual notice. Section (e)(3) of the Privacy Act obliges agencies to "inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual" of (1) "the principal purpose or purposes for which the information is intended to be used," and (2) "the routine uses which may be made of the information."[222] This critical language represents an important attempt to make the federal government's use of personal information open and understandable. In practice, however, the "Privacy Act Statement" provided to the individual contains broad language that fails to convey a precise sense of the planned applications of the data.

The weaknesses of the Privacy Act statement are well known. The Privacy Protection Study Commission made perhaps the most authoritative criticism of practice in this area. The Commission noted that the typical Privacy Act Statement tends only "to state the obvious and does not explicitly spell out other possible uses of the information."[223] The Commission made these specific recommendations:

> [T]he Statement should describe those uses of information that could reasonably be expected to influence an individual's decision to provide or not to provide the information requested. Since the individual's decision may be influenced by the techniques used to verify the information he provides, the Statement should also include a description of the scope, techniques, and sources to be used to verify or collect additional information about him.[224]

The Commission's recommendations regarding greater specificity in Privacy Act Statements have not, however, been followed.

The "publication" requirement calls for agencies to print lists of all routine uses in the Federal Register.[225] Section (e) also requires publication in the Federal Register of lists of any "system of records" when it is established or revised.[226] In regard to this requirement, David Flaherty has remarked with some irony, "[o]nly avid consumers of the Federal Register would benefit from the public notice requirements of the law."[227] The descriptions of routine uses and of the establishment of a system of records provide only constructive notice to the individual. Nevertheless, publication of these lists in the Federal Register is directed

---

222. Id. § 552a(e)(3).

223. Privacy Protection Study Comm'n, supra note 190, at 89.

224. Id.

225. *See* 5 U.S.C. § 552a(e)(4)(D) (setting out the required contents of notice in the Federal Register).

226. Id.

227. Flaherty, supra note 2, at 341.

less towards private citizens than agencies and Congress. The publication requirement is intended to oblige agencies to set in writing limits on planned disclosures. Publication also assists Congress in its oversight of the processing of personal information by agencies. Yet, the publication of any system of records has certain flaws concerning the kind of notice provided to Congress; these shortcomings will be discussed in the section on legislative oversight presented below.[228]

Like the "routine use" exemption, the practice of data matching represents another limitation on the ability of the Privacy Act to create transparency of data processing. Although the federal government matches billions of records, most individuals are unaware of this practice. Nevertheless, some provisions of the Privacy Act do seek to create both constructive and actual notice of data matching. Just as publication in the Federal Register is required for routine uses and the establishment of systems of records, notice of planned data matches must also be filed in the Register.[229] In addition to the resulting constructive notice of data matching, *actual* notice must be provided to individuals *after* a match if the agency decides to take specific action based on this comparison of records.[230] This safeguard is accompanied by an additional guarantee that an individual may contest the accuracy of an agency's match before any negative action is taken.[231] Generally, however, individuals are unaware of how federal agencies are matching their personal information. This lack of knowledge represents a significant limitation on the Privacy Act's creation of transparency regarding federal data processing.

b. The Freedom of Information Act (FOIA) and Transparency

The FOIA contributes significantly to transparency of data processing in the United States. The FOIA was enacted to require the federal government, including agencies, to provide access to its records.[232] In contrast to the Privacy Act, the FOIA's access rights are not to persons named in the sought-after record but to the public at large.[233] Yet, the FOIA also offers agencies an important opportunity to balance these public access rights with concern for the privacy of the individuals named in governmental records.

The FOIA reflects a traditional American belief in the need for open government. It is a modern legislative articulation of a goal as old as the United States — the participation by a group of equal citizens in public

228. *See* infra part II.B.4.b.ii.
229. 5 U.S.C. § 552a(e)(12).
230. Id. § 552a(p)(3).
231. Id.
232. *See* Department of Air Force v. Rose, 425 U.S. 352, 360 (1976) (noting that FOIA reflects "a general philosophy of full agency disclosure. . . . ").
233. Thus, the Freedom of Information Act speaks of making information "available to the public." 5 U.S.C. § 552(a).

affairs. Although participation reguires that individuals receive information from the government, participation can be deterred by the excess exposure of personal information controlled by the government. The boundless collection, processing, and dissemination of personal data can have a deleterious effect on the ability of individuals to join in social discourse.[234] The FOIA recognizes the danger of this disenfranchisement by providing a level of transparency that permits certain limits on disclosures that invade personal privacy.[235] Understanding these limits initially requires, however, a discussion of the way that the FOIA and Privacy Act complement one another.

The relationship between the FOIA and the Privacy Act is somewhat complex. An essential concept regarding the FOIA is that it sometimes requires the government to disclose information, but never requires *nondisclosure.* In the words of the Supreme Court, the FOIA is "exclusively a disclosure statute."[236] The FOIA's nine exemptions from disclosure, including its two privacy exemptions, merely provide grounds for agencies to refuse to disclose information if they so choose.[237] The FOIA grants discretionary grounds for nondisclosure to the agency that has control of the records. At the same time, the requirements of the Privacy Act may still govern agency action. A request for personal data from an agency pursuant to the FOIA will lead to three possible outcomes, set forth in Table A.

First, when the FOIA requires *disclosure,* the Privacy Act cannot bar release of the information in question. The Privacy Act explicitly exempts from its nondisclosure requirements records for which the FOIA mandates disclosure.[238] However, the significant privacy exemptions of the FOIA will limit the amount of personal information that must be released under this law.[239] Second, when the FOIA does *not* require disclosure and a personal record is sought by a third party, an agency can use the Privacy Act to block disclosure.[240] Finally, when the FOIA does *not* require disclosure and release of the record is sought by the individual to whom it pertains, the Privacy Act can require disclosure to that individual. As the

234. *See* supra part I.A.

235. 5 U.S.C. § 552(b).

236. Chrysler Corp. v. Brown, 441 U.S. 281, 292 (1979). *See* Kenneth C. Davis, 1 Administrative Law of the Eighties § 5:8 (1989) ("No words in the FOIA can be reasonably interpreted to forbid disclosure in any circumstances.").

237. 5 U.S.C. §§ 552(b) 1-9.

238. Id. § 552a(b)(2) (providing that no agency shall disclose any record not required under § 552 (FOIA)); 552a(t)(2) (preventing agency from using § 552a (Privacy Act) to withhold access to records otherwise accessible under § 552 (FOIA)). *See e.g.,* United States Dep't of Navy v. FLRA, 840 F.2d 1131, 1137 (3d Cir. 1988) (discussing FLRA's disclosure of employees' names and addresses); Martin v. Office of Special Counsel, Merit Sys. Protection Bd., 819 F.2d 1181, 1184 (D.C. Cir. 1987) (explaining the Privacy Act's exemption from nondisclosure requirements for records disclosed under FOIA).

239. 5 U.S.C. § 552(b) (6)-(7).

240. FLRA v. Department of Treasury, Fin. Mgmt. Serv., 884 F.2d 1446, 1451-53 (D.C. Cir. 1989).

Tenth Circuit has observed, the Privacy Act "provides rights to the individual with respect to his own records greater than the rights of the public generally."[241] Even if certain information is protected from access by the individual, the government is still obliged "to disclose reasonably segregable portions of the document which do not fall within the exemption" to an individual who is mentioned in these records.[242]

Table A

FOIA	Privacy Act
1) FOIA requires disclosure; FOIA's privacy exemptions do not prevent disclosure	1) Privacy Act cannot stop disclosure
2) FOIA does not require disclosure	2) Privacy Act can block disclosure to a third party
3) FOIA does not require disclosure	3) Privacy Act can require disclosure to party mentioned in record who seeks record

Agency protection of privacy through application of the relevant FOIA privacy provisions is usually vigorous; moreover, case law supports this protection. Most importantly, the Supreme Court has held that the FOIA applies only to information about governmental activities.[243] According to the Court, the relevant test is whether "response to [a FOIA] request would . . . shed any light on the conduct of any Government agency or official."[244] Purely personal information about private individuals is not to be released because such disclosure would fail to advance the purpose behind the FOIA.[245] As a result of a carefully structured concern for both transparency and the concealment of personal information, the FOIA and

241. Wren v. Harris, 675 F.2d 1144, 1146 (10th Cir. 1982).

242. Nemetz v. Department of Treasury, 446 F.Supp. 102, 105 (N.D. Ill. 1978). *See also* May v. Department of the Air Force, 777 F.2d 1012, 1015 (5th Cir. 1985); Londrigan v. FBI, 670 F.2d 1164, 1170 (D.C. Cir. 1981).

243. Department of Defense v. FLRA, 114 S.Ct. 1006, 1012-13 (1994); Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 772 (1989).

244. *Reporters Comm.*, 489 U.S. at 772. For important decisions of lower courts applying this approach, see New York Times v. NASA, 782 F.Supp. 628, 632-33 (D.D.C. 1991); New York Times Co. v. NASA, 920 F.2d 1002, 1009-10 (D.C. Cir. 1990).

245. This approach has been praised on data protection grounds, see Fred H. Cate, et al., The Right to Privacy and the Public's Right to Know, 46 Admin. L. Rev. 41, 42-46 (1994). It has also been criticized as unduly restricting public access to governmental information. *See* Sean E. Andrussier, The Freedom of Information Act in 1990: More Freedom for the Government; Less Information for the Public, 1991 Duke L.J. 753, 757-58.

the Privacy Act work together to set effective limits on third party use of personal information in the control of the government.

3. *Assignment of Procedural and Substantive Rights to the Individual*

Although the Privacy Act grants some important rights to the individual, these interests generally are not effective in guiding the practices of federal agencies. The critical individual rights concern access to personal records and the opportunity to request their amendment.[246] Useful in reference to the individual's own files, these rights have not significantly improved agency compliance with the Privacy Act.[247] The ineffectiveness of the Act arises from the limited remedies available under this law; the Privacy Act does not give federal courts the power to order agencies to change their data processing practices.

Section (d) of the Privacy Act contains the critical language regarding the protection of access to records and the maintenance of their accuracy. It requires each agency "upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system" to "permit him . . . to review the record and have a copy made of all or any portion thereof in a form comprehensible to him."[248] When an agency fails to allow an individual access to her records, a limited injunctive remedy is provided.[249] The injunctive remedy following an access refusal is granted by a district court after its *de novo* review of the matter. The court "may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him."[250] The court may also assess reasonable attorney fees for a complainant who has substantially prevailed.[251]

In addition to providing individuals with this right of access, Section (d) also permits the amendment of personal information.[252] If an amendment request is refused, the individual may seek review of the agency decision.[253] Following a second refusal of amendment, the Privacy Act provides for judicial review.[254] This review is to be carried out *de novo* by a federal district court, which is not required to defer to either the agency's decision or the administrative record presented to it.[255] Furthermore, following an agency's refusal to amend, wide remedial

246. 5 U.S.C. § 552a(d) (1988).
247. For a discussion of the general shortcomings of these rights, see Flaherty, supra note 2, at 338-40.
248. 5 U.S.C. § 552a(d)(1).
249. Douglas Laycock, Modern American Remedies 215 (1985).
250. 5 U.S.C. § 552a(g)(1)(3)(A).
251. Id. § 552a(g)(3)(B).
252. Id. § 552a(d)(2).
253. Id. § 552a(d)(3).
254. Id. § 552a(g)(1)(A).
255. 5 U.S.C. § 552a(g)(1)(A).

powers are accorded the district court. These remedial powers provide the greatest injunctive authority found under the Privacy Act; they authorize the district court to "order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct."[256] Finally, in any case "in which the complainant has substantially prevailed[,]" the court "may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred."[257]

Only in these two circumstances, concerning the failure of the agency to provide access to an individual's record or to amend it, can the court issue injunctions. Under certain other conditions, the court can order limited damages. Such situations deal with agency failure: (1) to maintain records concerning an individual with adequate accuracy and completeness; or (2) to comply with other parts of the Privacy Act, such as its restrictions on disclosure or its provisions for fair information practices.[258] In cases of such agency failure, when the government is found to have acted intentionally or willfully, a court may order (1) "actual damages" to the individual,[259] (2) the costs of the action,[260] and (3) reasonable attorney fees.[261] The court cannot order the agency to change its practices. As the Ninth Circuit held in *Cell Associates v. National Institutes of Health*, "Congress did not intend to authorize the issuance of injunctions prohibiting the disclosure of protected materials" under the Privacy Act.[262]

Thus, individuals who seek to enforce their rights under the Privacy Act face numerous statutory hurdles, limited damages, and scant chance to effect an agency's overall behavior.[263] Other laws in the United States allow suits by citizens as a "private attorney general."[264] In this approach to litigation, the individual draws the federal courts and the government into a reasoned debate about the need to change or even restructure governmental practices.[265] Under the Privacy Act, in contrast, the citizen

256. Id. § 552a(g)(2)(A).

257. Id. § 552a(g)(2)(B).

258. Id. § 552a(g)(1)(C), (D).

259. Id. § 552a(g)(4)(A). There is some conflict among courts as to the meaning of "actual damages" under the Privacy Act. This term has been limited by some courts to pecuniary loss. Fitzpatrick v. IRS, 665 F.2d 327, 330 (11th Cir. 1982); DiMura v. FBI, 823 F.Supp. 45, 48 (D. Mass. 1993); Pope v. Bond, 641 F.Supp. 489, 501 (D.D.C. 1986).

In contrast, other courts have held that "actual damages" under the Privacy Act include damages for physical and mental injury for which there is competent evidence in the record, as well as damages for out-of-pocket expenses. Johnson v. Department of Treasury, 700 F.2d 971, 972 (5th Cir. 1983).

260. 5 U.S.C. § 552a(g)(4)(b).

261. Id.

262. 579 F.2d 1155 (9th Cir. 1978).

263. For a more general attack on a reliance on individual action to shape data protection practices and principles, see Bennett, supra note 2, at 156-58.

264. For an excellent introduction to such "structural" or "public law," see Robert Cover et al., Procedure 219-427 (1988); *see also* Abram Chayes, The Role of the Judge in Public Law Litigation, 89 Harv. L. Rev. 1281 (1976) (discussing public law litigation.)

265. As originally proposed, the Bill that became the Privacy Act did envision the creation

stands as an atomistic individual authorized to engage in litigation merely on a restricted basis. In its assignment of rights, the Privacy Act views data protection as a matter for the individual in relation to his data alone.

4. *Establishment of Governmental Oversight of Data Use*

Individual litigation under the Privacy Act is unlikely to lead to changes in an agency's practices or interpretation of its duties. In light of the restricted nature of individual remedies under this law, a special need exists for independent governmental oversight of agency data processing.[266] A data protection commission has three important roles. This independent body provides expertise in an area of rapid technological change. It also develops and monitors international agreements and foreign laws that affect data imports and exports. Finally, it supplies a focal point for a societal debate about information processing technology and practices. The types of data protection oversight existing in the United States fail in these roles.

The Privacy Act establishes different kinds of forums to oversee compliance with its provisions. It provides for two kinds of authorized monitors: *agency-internal oversight* by designated departmental officials and *agency-external oversight* by the Office of Management and Budget (OMB) and Congress. Neither mode of review has been particularly effective.[267]

---

of a Federal Privacy Board. At this time, Sen. Sam Ervin, the chief legislative sponsor of the Privacy Act, pointed to the urgent need for "foresight and the ability to forecast the possible trends in information technology before they actually take their toll." Introductory remarks on S. 3418, Cong. Rec., S6741 (May 1, 1974), *reprinted in* U.S. Congress, Legislative History of the Privacy Act of 1974, 5 (1976). Ervin's proposed Federal Privacy Board was to oversee the gathering and disclosure of personal information by "[f]ederal agencies, state and local governments, and private organizations." Id. Unfortunately, after this Bill's passage in the Senate, opposition in the House and from the Ford administration resulted in a compromise concerning institutional oversight. Flaherty, supra note 2, at 310-15. Rather than creating a Privacy Board, the Privacy Act created a more limited, blue-ribbon commission, the Privacy Protection Study Commission. This body issued a number of reports and went out of business, as required by law, two years after all its members were appointed.

This missed opportunity was the closest that the United States has come to having an independent data protection commission equivalent to those found in Europe.

266. For example, Robert Gellman has stated, "administrative privacy activities at the federal level have been fragmented, incomplete, and discontinuous." Robert Gellman, Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions, 6 Software L.J. 199, 238 (1993). In even more critical terms, David Flaherty has noted that, without a federal data protection agency in the United States, the "system for articulating privacy interests in a systematic fashion is woefully inadequate." Flaherty, supra note 2, at 382.

267. *See* supra part I.B.

a. Agency Internal Oversight

The Privacy Act sets up two kinds of intra-agency supervision of data processing practices. This oversight is carried out by the Privacy Act official and the Data Integrity Board. Although each of these institutional figures is of some value, neither is equivalent to an independent data protection authority.

i. The Privacy Act Official

As part of its evaluation of data processing practices in the United States, the Privacy Protection Study Commission suggested that each federal agency designate a single official to monitor implementation of the Privacy Act.[268] Following this recommendation, the OMB required agencies to designate a "Privacy Act official" with certain specified oversight responsibilities.[269] Yet, even in their limited role of evaluating agency compliance with the Privacy Act's requirements, these officials have been ineffective.

The General Accounting Office (GAO) has noted a number of weaknesses in the activities of Privacy Act officials.[270] First, the GAO states that these policy officials have limited responsibilities and scarce resources.[271] The Privacy Act official has not always been assigned key functions, such as overseeing compliance with the Privacy Act or training agency employees.[272] Instead, Privacy Act activities are dispersed throughout agencies.[273] Moreover, the Privacy Act official is usually a mid-level employee, assisted by little or no staff and allowed to work on compliance activities only part-time.[274] In sum, as an academic observer notes, "most Privacy Act officials are relatively invisible, especially in terms of actually influencing agency policy on surveillance."[275]

---

268. Personal Privacy, supra note 49, at 523. The Commission defined the official's responsibilities to include issuing instructions, guidelines, and standards and making such determinations as are necessary for the implementation of the Act. The official also would be responsible for taking reasonable affirmative steps to assure that all agency employees and officials responsible for the collection, maintenance, use, and dissemination of individually identifiable records are aware of the requirements of the Act. Id.

269. Flaherty, supra note 2, at 318.

270. *See generally*, General Accounting Office, Privacy Act: Federal Agencies' Implementation Can Be Improved (1986).

271. Id. at 2.

272. Id. at 8.

273. Id.

274. Id. at 20.

275. Flaherty, supra note 2, at 318.

ii. The Data Integrity Board

The Computer Matching Act, which amended the Privacy Act in 1988, requires the establishment of Data Integrity Boards (DIBs) to carry out intra-agency review of data matching activities.[276] A DIB must be established in each agency that conducts or participates in a matching program.[277] Each DIB is to consist of "senior officials designated by the head of the agency."[278] The duties of the DIB are to "review, approve and maintain" all written agreements establishing matching programs in order "to ensure compliance" with the guidelines of the Matching Act and "all relevant statutes, regulations and guidelines."[279] This statutory language gives authority to the DIB to deny agencies the ability to conduct matches. In addition, the DIB is to review matching programs to assess compliance with applicable laws and the continued justification for such disclosures.[280] Finally, the DIB is to compile an annual report describing the matching activities of the agency.[281]

Expectations for these Boards were somewhat low from the time of the enactment of the Computer Matching Act. Despite the somewhat broad statutory language, the legislative history to the Computer Matching Act states that it was *not* envisioned that Data Integrity Boards would "routinely undertake active investigations of matching programs."[282] As Robert Gellman has noted, "Congress did not assign the Data Integrity Boards a broad privacy policy role."[283] Indeed, DIBs are unlikely creatures for such a broad policy role because they lack the institutional independence necessary for aggressive scrutiny of the data matching activities of agencies.

The DIBs have functioned merely as institutions that review the housekeeping measures of the Matching Act. In carrying out such a limited role, they have avoided wider tasks. Two independent studies, one by the GAO and the other by a political scientist, have revealed important deficiencies of the DIBs. The GAO has criticized the DIBs' "weak level of review" of data matching.[284] Rather than deciding on whether to proceed with proposed matches, the Boards have checked on paperwork requirements.[285] The GAO found no case in which DIB oversight "led to permanent discontinuance or major modification of a computer matching

276. 5 U.S.C. § 552a(u)(1988).
277. Id. § 552a(u)(1).
278. Id. § 552a(u)(2).
279. Id. § 552a(u)(3).
280. Id. § 552a(u)(3)(B).
281. 5 U.S.C. § 552a(u)(3)(D).
282. Legislative History, Computer Matching Act, supra note 202, at 3137.
283. Gellman, supra note 266, at 225 (citation omitted).
284. GAO, Computer Matching, supra note 208, at 5.
285. Id. at 17-29.

program by any of the agencies."[286]

The other major study of DIBs also found oversight that was, at best, weak.[287] In carrying out interviews with members of these Boards, Priscilla Regan discovered that while some changes in matching agreements were made at the drafting stage due to a DIB's input, agencies were, to a large extent, developing a "boilerplate" matching agreement and using it for a variety of purposes.[288] Moreover, the membership of senior staff officials on the DIB did not stop the delegation of most responsibilities to staff and the transformation of the DIBs into "paper pushers rather than policymaking bodies."[289] This study concluded that "the DIB members have not used the boards as agents of change in computer matching procedures."[290] The analysis of both the GAO and Regan indicates that the focus of DIBs has been on routine compliance with the Privacy Act's computer matching provisions.

Evaluated against the standard of the three critical tasks of an independent data protection board, neither the Privacy Act official nor the Data Integrity Board have been successful. Although these institutions have considerable expertise regarding the Privacy Act and the information processing practices of federal agencies, they address these issues only on a part-time basis and only within the context of a narrow statutory mandate. As for their role in developing and monitoring international laws regarding data protection, these institutions of internal oversight are, by their nature, precluded from engaging in such tasks. Lastly, these institutions have not provided a focal point for societal debate about information technology. Here, too, the internal focus of the Privacy Act official and Data Integrity Board precludes such activity. The mid-level bureaucrats assigned to the role of the Privacy Act official and the more senior officials on the Data Integrity Board possess too restricted a portfolio of activities and too low a profile to stimulate the necessary societal consideration of data processing practices.

b. Agency External Oversight

In addition to the two kinds of agency internal oversight, supplied by the Privacy Act official and the Data Integrity Board, the Privacy Act establishes two forms of oversight external to federal agencies. The Office of Management and Budget (OMB) and Congressional subcommittees

286. Id. at 16-17.

287. *See* Priscilla M. Regan, Data Integrity Boards: Institutional Innovation and Congressional Oversight, 10 Gov't Info. Q. 443 (1993) (analyzing the effectiveness of Data Integrity Boards and matching agreements and concluding that direct oversight by an independent data protection board is necessary).

288. Id. at 449-52.

289. Id. at 456.

290. Id. at 455.

carry out this external scrutiny. As in the case of intra-agency oversight, the resulting kind of supervision of information processing falls considerably short of that of a data protection agency.

i. Office of Management and Budget

The Privacy Act provides the Office of the Management and Budget (OMB), an executive branch agency, with an important oversight role. In Section (v), this law requires the Director of the OMB to "develop and . . . prescribe guidelines and regulations for the use of agencies in implementing the provisions [of the Privacy Act]."[291] Section (v) also requires the OMB to "provide continuing assistance to and oversight of the implementing of this section by agencies."[292] The OMB also must oversee the activities of Data Integrity Boards.[293] The OMB has not vigorously executed these tasks.[294]

As part of its responsibility under the Privacy Act, the OMB has issued guidelines and a circular expressing a "general policy framework to Federal information use."[295] These documents reflect a hands-off policy; the OMB has refused to take an active role in supervising compliance with the Act. In 1983, a report of the House Committee on Governmental Oversight found, "[i]nterest in the Privacy Act at the Office of the Management and Budget has diminished steadily since 1975."[296] OMB's lack of interest in the Privacy Act remains unchanged.[297] Indeed, a recent proposed revision of the OMB circular concerning federal information use continues the tradition of a greater interest in "information resource management" than in data protection.[298]

Under the Computer Matching Act, the OMB has the responsibility to develop data matching guidelines and regulations for agencies.[299] It also has the authority to approve proposed data matches that have been rejected by DIBs.[300] These are relatively minor roles; as Robert Gellman has written, "The Computer Matching and Privacy Protection Act reflects a recent judgment by the Congress that only limited privacy monitoring and

---

291. 5 U.S.C. § 552a(v)(1) (1988).
292. Id. § 552a(v)(2).
293. Id. § 552a(u)(5)(B).
294. *See* Flaherty, supra note 2, at 316; Gellman, supra note 266, at 226.
295. Management of Federal Information Resources, 58 Fed. Reg. 36,068 (1993) (revision of Circular A-130) [hereinafter Circular A-130]. For an example of an OMB guideline, see, e.g., Privacy Act of 1974; Final Guidance Interpreting the Provisions of Public Law 100-503, Computer Matching and Privacy Act of 1988, 54 Fed. Reg. 25,818 (1989) [hereinafter OMB Guidelines].
296. 1983 House Committee Report, supra note 191, at 35.
297. Gellman, supra note 266, at 223-24.
298. Circular A-130, supra note 295, at 36,071-74.
299. 5 U.S.C. § 552a(u)(1)(B).
300. Id. § 552a(u)(5).

oversight can be expected from OMB."[301] Indeed, this congressional judgment has been confirmed by the OMB's behavior. The OMB's guidelines to the Act show a readiness to defer to agency decisions and to focus on the OMB's notion of the bottom line. For example, the OMB guidelines specify that a cost benefit ratio need not even be favorable for data matching to take place.[302] All that is required is some form of analysis to be undertaken before the matching begins.[303]

In general, the OMB has concentrated its energy on applying informational technology as a means of establishing rational control over administration. To an extent unforseeable in 1974, the year the Privacy Act was passed, the OMB has become an independent power center with responsibility for supervising federal paperwork, debt collection, and the reduction of the federal deficit.[304] To carry out these tasks, the OMB has advocated data matching, compatibility of information systems and interagency sharing of information technology. These policies have not been accompanied by great concern for data protection.

ii. Congress

The Privacy Act's chief mechanism for structuring congressional supervision is Section (o), which requires agencies to file "advance adequate notice with Congress of any proposal to establish or alter any system of records."[305] Yet, Section (o) notices furnish at best an incomplete picture of federal data processing practices. Since these notices cover only the establishment or alteration of a system of records, they can provide Congress with no insight into the *functioning* of existing systems. Evidence also exists that agencies are not carrying out their obligation to file these notices. In particular, GAO evaluation of these documents found that many were not current.[306] Discussions between the GAO and Privacy Act officers led to the explanation that "their limited resources" preclude review of each individual system notice.[307]

In addition to these shortcomings in the actual notices, the congressional attention given to these documents has been restrained in both style and quality. In practice, only the House Committee on Government Operations continuously monitors these reports. Through the efforts of the Government Operations' Subcommittee on Government

301. Gellman, supra note 266, at 226.

302. OMB Guidelines, supra note 295, at 25,828-29.

303. Id.

304. *See* Flaherty, supra note 2, at 327 ("Protecting privacy is a very minor part of OMB's multiple activities.").

305. 5 U.S.C. § 552a(o) (1988).

306. General Accounting Office, Privacy Act System Notices 6-9 (1987). The GAO's analysis of 53 system notices chosen at random from the Federal Register found "29 needed to be updated to reflect current conditions." Id. at 6.

307. Id. at 9.

Information, some changes have been made in planned systems.[308] Yet, this kind of oversight lacks the visibility required to impress recalcitrant bureaucrats. Agencies have, on occasion, simply ignored the subcommittee's comments and suggestions.[309] The Computer Matching Act's amendments to the Privacy Act also provide for a review of computer matching by these congressional committees.[310] No reason exists to expect this review to be any more effective than that of system of records notices.

As part of its responsibility to monitor the Privacy Act, the House Subcommittee on Goverment Information not only has examined Privacy Act notices, but also has held a number of hearings and commissioned studies by the GAO.[311] These activities seek to draw the public's attention to international developments and to stimulate societal debate about information technology. Despite these efforts and the unmatched expertise of the subcommittee staff,[312] the result has fallen far short of corresponding efforts by data protection agencies. The relative lack of resources and the relatively low profile of these legislative branch institutions has reduced the resonance of such efforts.

The external oversight of the OMB and congressional committees have not fulfilled the necessary roles of a data protection commission. First, the OMB is more interested in the application of information technology than in developing the expertise necessary for it to play a critical role in data protection. It also has played no part in developing and monitoring international laws. Finally, the OMB has not tried to stimulate societal discussion of data processing and information technology. The House Committee on Government Operations, while unable to fulfill a role equivalent to that of a data protection commission, indicates the potential for such an institution in the United States. Indeed, over the last two years, bills introduced in both the Senate and the House sought to establish an institution of independent oversight of governmental data processing. These bills have not been enacted.[313]

In the federal regulation of the use of personal information by governmental agencies, all four elements of the data protection model are present to some extent. Yet, none of these four elements is structured in an entirely satisfactory manner. The lack of effective independent

---

308. *See* 1983 House Committee Report, supra note 191, at 38.

309. Id. at 39-55.

310. 5 U.S.C. § 552a(r).

311. As an example of such a hearing, see 1983 House Committee Report, supra note 191, at 15. As an example of a GAO report carried out in response to a request of this Committee, see GAO, Computer Matching, supra note 208.

312. *Cf.* Flaherty, supra note 2, at 318 (noting the "few federal officials who have acquired considerable expertise over time" and who "constitute an informal network of data protection officials").

313. *See, e.g.*, Privacy Protection Act of 1993, S. 1735, 103d Cong., 1st Sess. (1993). Individual Privacy Protection Act of 1993, H.R. 135, 103d Cong., 1st Sess. (1993).

oversight[314] places great stress on the role of individual enforcement; unfortunately, as already noted, the nature of the remedies available to the individual make such self-help incapable of shaping overall agency use of personal information.

C. State Legislation and the Participatory Model

State data protection law in the United States is largely unchartered territory.[315] This status is due in part to the large number of jurisdictions and the myriad paths that the fifty state lawmakers have taken.[316] Some data protection exists in every state, but no two states have adopted precisely the same system of regulation. To add further to the complexity of this regulation, state constitutional provisions can create rights of privacy with implications for data protection.

Despite the various approaches to data protection, some similarities among the states can be identified. One similarity with generally positive implications for data protection is represented by the group of state statutes whose existence derives from federal mandates. Examples of such measures are state laws regulating access to educational records and child abuse data banks.[317] Although these statutes provide important protection

---

314. Although international experience indicates that independent oversight is important and entails only relatively modest costs, Congress has not yet created such a government institution. Indeed, the lack of enthusiasm for creating new governmental bureaucracy has not been restricted to Congress. For example, Ann Windham Wallace, the head of the U.S. Office of Consumer Affairs during the Bush Administration, expressed her opposition to the creation of a data protection board in the United States in these terms, "While I am the first to say that business should be more sensitive to consumer attitudes toward privacy, I would be the last to advocate another government bureacracy for that purpose. I believe that we currently have the mechanisms we need to address privacy issues." Wallace Calls For Stronger Privacy Laws, But No Data Protection Board, Privacy Times, May 8, 1991, at 5. Whether the attitude of the Clinton administration to the creation of a data protection board will ultimately be more favorable is not clear. At any rate, privacy issues have not been a top level concern of the administration.

315. *See, e.g.*, Arthur Bonfield & Michael Asimow, State and Federal Administrative Law 536-54 (1989) (leading casebook concerned with state administrative law but concentrating almost entirely on the *federal* freedom of information act rather than on state law in this area). *But see* Bruce D. Goldstein, Comment: Confidentiality and Dissemination of Personal Information: An Examination of State Laws Governing Data Protection, 41 Emory L.J. 1185 (1992) (carrying out an ambitious study of this field). This Comment develops three "models" of state data protection law: the "blanket," the "classified," and the "stratified" approaches. Id. at 1186-87. Although this work is extremely insightful on a number of points, I am not sure that the three models are, in fact, conceptually different enough, either in theory or in practice, to support the underlying classification scheme. As Goldstein himself admits, "Such models are not intended to be mutually exclusive or absolute. As described, they overlap significantly, particularly in instances where a state statute fits predominantly in one category, but uses aspects of other models." Id. at 1187 n.5.

316. *See* Goldstein, supra note 315, at 1185-87.

317. The relevant federal mandating statutes are the Family Educational Rights and Privacy Act, 20 U.S.C. § 1232g (1990), and the Child Abuse Prevention and Treatment Act, 42 U.S.C. § 5106a (1983). For criticism of the approach taken by most states in the maintenance of data banks with information regarding cases of child abuse, see Note, The Constitutionality

for certain groups of personal data, they sometimes have significant weaknesses. In addition, since these state laws regulate only narrow sectors of data use, they cannot substitute for more comprehensive data protection laws at the state level.

As this Article has previously noted, the Privacy Act serves as a comprehensive fair information practices statute for federal agencies. The Act places restrictions on the collection and processing of personal information and provides rights for the individual whose data are processed.[318] Unfortunately, most states do not have similar omnibus data protection laws; only thirteen states have general statutes that establish fair information practices for the government's processing of personal information.[319] In the majority of states, scattered laws provide only limited protections for personal information in the public sector. These statutes typically apply only to certain types of information or certain kinds of processing activities.[320]

The absence of omnibus laws at the state level creates gaping weaknesses. Without these laws, some or all of the four elements of the data protection model are often absent from state law. The weakness of this approach is revealed by the numerous states which have enacted specific laws protecting confidentiality of the records of public libraries, but which have not enacted laws protecting far more sensitive data in the government's control.[321]

The weaknesses of state data protection law are heightened by the effect of state-level Freedom of Information Acts (FOIA). All states have statutes that regulate public access to governmental records; only some of these laws take, however, the path of the federal statute and provide explicit protection for privacy. The resulting situation is often highly unsatisfactory; the absence of an omnibus data protection act and the presence of a freedom of information law can create strong pressure favoring the release of personal information. As a result, the state can disclose highly sensitive data.

---

of Employer-Accessible Child Abuse Registries, 92 Mich. L. Rev. 139, 172-82 (1992). *See also* infra notes 357-58 and accompanying notes.

318. *See* supra part II.B.

319. These thirteen states are Alaska, California, Connecticut, Hawaii, Indiana, Massachusetts, Minnesota, New Hampshire, New York, Ohio, Utah, Virginia, and Wisconsin.

For the applicable statutes, see Alaska Stat. § 44.99.300 (1993); Cal. Civ. Code § 1798 (West 1995); Conn. Gen. Stat. Ann. § 4-190 (West 1994); Haw. Rev. Stat. § 92F (1989); Ind. Code § 4-1-6 (1993); Mass. Gen. L. ch. 66A, §§ 1-3 (1994); Minn. Stat. § 13.01 (1995); N.H. Rev. Stat. Ann. § 7-A:1 (1994); N.Y. Pub. Off. Law § 91 (McKinney 1995); Ohio Rev. Code Ann. § 1347.01 (Anderson 1994); Utah Code Ann. § 63-2-101 (1994); Va. Code Ann. § 2.1-377 (Michie 1994); Wisc. Stat. Ann. § 19, subch. III & IV (West 1994).

320. *See, e.g.*, Tenn. Code Ann. § 10-7-301(2) (1987) (stating that confidential records are public records designated confidential by statute); Tenn. Code Ann. § 12-4-414 (1987) (addressing the confidentiality of payroll records).

321. *See, e.g.*, Ark. Code Ann. §§ 13-2-703 to -704 (Michie 1993) (governing the disclosure of information held by libraries and other public facilities).

Arkansas provides a good example of a state with such a patchwork structure to data protection. In Arkansas, there is neither a state constitutional provision protecting privacy nor an omnibus data protection act for the public sector. Individual laws do protect, however, some information controlled by the state, such as library records.[322] Arkansas also has a strong tradition of open access to governmental files as expressed in the state's Freedom of Information Act.[323] This law contains no general privacy exemption. Its only mention of privacy concerns state-controlled personnel records, whose disclosure is prevented only "to the extent that disclosure would constitute [a] clearly unwarranted invasion of personal privacy."[324] In addition to its specific exemptions for certain categories of records,[325] the Arkansas FOIA also exempts from disclosure any information that other statutes require to be held confidential.[326]

Established case law holds that the Arkansas FOIA is to be construed liberally to encourage the purpose of the act, which is providing the public with access to governmental records.[327] The Arkansas Supreme Court's decision in *McCambridge v. The City of Little Rock* offers an example of the broad disclosure permitted under this state FOIA.[328] The case concerned a grisly murder and suicide in Little Rock. John Markle, a local stockbroker facing financial troubles and possible criminal charges, had murdered his wife and two children, and then taken his own life.[329] Among other issues, the Arkansas Supreme Court addressed whether the privacy rights of Markle's mother could bar release of certain documents related to the event. These documents included police crime scene and pathologist photographs, her son's diary, and a letter her son had left for her at the crime scene.[330]

The Arkansas Supreme Court found that all these documents were to be released under the state FOIA. In holding that the photographs should be released, the court admitted that the crime scene and pathologist photographs were "horrible and sickening, as are all such multiple murder photographs." Yet, it nevertheless ruled that the public had "strong interests in depicting how the multiple murders occurred, why the police

322. Id.

323. Id. §§ 25-19-101 to -107.

324. Id. §§ 25-19-105(b)(10).

325. Other records among the limited group exempted from public inspection are (1) state income tax records; (2) medical, scholastic, and adoption records; and (3) grand jury records. Id. § 25-19-105(b).

326. As Arkansas' FOIA states, all records are open to inspection "[e]xcept as otherwise specifically provided . . . by laws specifically enacted to provide otherwise." Ark. Code Ann. § 25-19-105(a).

327. Rehab Hosp. Servs. Corp. v. Delta-Hills Health Sys. Agency, Inc., 687 S.W.2d 840 (Ark. 1985); Laman v. McCord, 432 S.W.2d 753 (Ark. 1968).

328. 766 S.W.2d 909 (Ark. 1989). For an excellent discussion of *McCambridge*, see John J. Watkins, Arkansas Freedom of Information Act 154-57 (2d ed. 1994).

329. *McCambridge*, 766 S.W.2d at 909-12.

330. Id.

considered the case closed as a triple murder-suicide matter, and why no further action should be taken."[331] The court found that the diary and the letters to Markle's mother related to the public's strong interest in "announced solution to crime"[332] and ordered that these documents also be disclosed to the public.

Arkansas is not the only state without a coherent expression of the four elements of the data protection model. Florida also lacks a comprehensive data protection statute for the public sector, having only isolated parts of the data protection model expressed in its law.[333] For example, although the practice of data matching is entirely unregulated by Florida law,[334] many Florida state agencies employ computer matching: A survey of eleven agencies found 18 million records matched in one year alone.[335] The absence of regulation of this widespread practice alone raises serious doubts regarding the existence in Florida of a statutory fabric for the processing of personal information. Moreover, no state agency in Florida carries out independent oversight of matching or other data protection issues.

The data protection vacuum in Florida is highly problematic. Florida, like Arkansas, has a strong tradition of "open government."[336] The Florida Constitution reflects this strong emphasis on access to governmental records:

> Every natural person has the right to be let alone and free from governmental intrusion into his private life except as otherwise provided herein. This section shall not be construed to limit the public's right of access to public records and meetings as provided by the law.[337]

This text explicitly limits part of the higher law of Florida, namely its constitutional right of privacy, with one type of lower law—open government statutes.

The Florida Public Records Law, the state's freedom of information act, protects from release only public records designated confidential by

---

331. Id. at 915.

332. Id.

333. Florida Stat. Ann. § 119.011 (West 1990). On several occasions, a fair information practices act has been introduced without success by the Florida Legislature Joint Committee on Information Technology Resources. *See, e.g.*, Florida Legislature Joint Committee on Information Technology Resources, Fair Information Practices (1987).

334. *See* Florida Legislature Joint Committee on Information Technology Resources, Florida's Information Policy: Problems and Issues in the Information Age 109 (1989) [hereinafter Joint Committee, Florida's Information Policy] ("No state law uniformly regulates computer matching in Florida agencies and consequently no legislative oversight of such activities exists.").

335. Id. at 108.

336. *See* Matthew D. Bunker et. al., Access to Government-Held Information in the Computer Age, 20 Fla. St. U. L. Rev. 543, 593 (1993) ("[Florida] has possibly the strongest presumption favoring disclosure of government records of any state.").

337. Fla. Const. art I, § 23.

law.[338] As a result, certain patient records under state control and records concerning elder abuse are exempted from disclosure.[339] Yet, the general rule, as stated by the Florida Legislature's Joint Committee on Information Technology Resources, is "the Public Records Law makes virtually all types of personal information subject to public disclosure."[340] However, Florida does not merely disclose information to the public; like several other states, it sells driver license information and other state information to direct market mailers.[341]

Other states do a far better job in establishing the four elements of the data protection model. Of the fourteen states with fair information practice laws, California has the most comprehensive approach to data protection. Its system of legal regulation includes constitutional law, a fair information practices act, and a freedom of information act that pays careful attention to data protection concerns.

The California constitutional right to informational privacy is notable for its high level of protection. In fact, the California Constitution not only contains an explicit mention of "privacy," it also reflects a specific intention to protect personal information.[342] Moreover, unlike most constitutional rights, the California constitutional right to informational privacy also applies to the private sector.[343] Important judicial decisions have developed California's constitutional right to informational privacy in the context of both the public and private sectors.[344] Indeed, the case law

---

338. Fla. Stat. Ann. § 119.07(3)(a) (West 1982).

339. *See* id. § 119.07(3)(v) (exempting medical records detailing "name, residence, or business address, social security number. . ." and other personal information from the mandatory release provisions of the act).

340. Joint Committee, Florida's Information Policy, supra note 334, at 131.

341. *See* Florida Legislature Joint Committee on Information Technology Resources, Electronic Records Access: Problems and Issues 129 (1994) ("Not only does the public have access to the individual's driver's history, including the personal information compelled by the agency, but the Department routinely provides its records to direct marketing organizations and insurance companies.").

342. The first section of the first article of the California Constitution contains a clause protecting informational privacy. This provision states "all people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and *privacy*." Cal. Const. art. 1, § 1 (emphasis added). A popular referendum added this mention of privacy to the California Constitution in 1974.

Not only is the word "privacy" used in the state constitution, but this term, which can refer to many different interests in American law, extends to the objectives of data protection in a computer age. This connection between privacy and data protection was explicitly made at the time of the creation of this constitutional amendment; the proof can be found in the statements of the provision's proponents that were included in the official election brochure issued during the popular referendum. The Election Brochure is reprinted in its entirety in an appendix to J. Clark Kelso, California's Constitutional Right to Privacy, 19 Pepp. L. Rev. 327, 480-84 (1992).

343. *See* Hill v. NCAA, 865 P.2d 633, 644-45 (Cal. 1994) (holding that California's state constitutional right to privacy may be enforced against private parties).

344. Id.; White v. Davis, 533 P.2d 22 (Cal. 1975); Central Valley Chapter v. Younger, 262

regarding the effects of this constitutional right in the private sector is particularly rich, ranging from cases that protect the privacy of information relating to AIDS patients to those that constitutionalize the tort right of privacy.[345] In the public sector, the California Supreme Court and lower courts have applied this state constitutional right to address issues relating to the transparency of information use and the kinds of rights available to the individual.[346] As a result of these important judicial opinions, California has the strongest constitutional scheme of data protection in the United States.

In addition to its constitutional protections for data protection, California also has created a significant statutory framework to govern how state agencies use personal information. In its Information Practices Act of 1977, California supplemented its constitutional protection by creating a statutory framework for application of personal information.[347] The California law establishes a number of fair information practices including limitations on the collection of unnecessary data and a requirement that agencies maintain in their records only information "relevant and necessary to accomplish a purpose of the agency required or authorized by the California Constitution or statute or mandated by the federal government."[348] Elements of transparency are also provided for individuals.[349] As part of this process, California has placed limits on data matching.[350] The state also provides rights to the individual, who can

---

Cal. Rptr. 43 (Cal. Ct. App. 1989); Gunn v. California Employment Dev. Dep't, 156 Cal. Rptr. 584 (Cal. Ct. App. 1979).

345. *Hill*, 865 P.2d at 633; Urbaniak v. Newtown, 277 Cal. Rptr. 354 (Cal. Ct. App. 1991).

346. *White*, 533 P.2d at 233-34 (Cal. 1975); Heda v. Superior Court, 275 Cal. Rptr. 136, 137 (Cal. Ct. App. 1990); Division of Medical Quality Bd. v. Gherardini, 156 Cal. Rptr. 55, 60 (Cal. Ct. App. 1979).

347. Cal. Civ. Code § 1798 (Deering 1994).

348. Id. § 1798.15.

349. *See e.g.*, id. § 1798.17 (requiring certain information regarding authority for data collection and plans for data use to be provided to individuals on any form used to collect personal data).

350. The Information Practices Act begins by setting general *limits on secondary uses* of information that agencies collect. Cal. Civ. Code § 1798.24 (Deering 1994). An agency may not disclose any personal or confidential information unless it fits into the disclosure exceptions as codified. Id. This section allows disclosures within no fewer than twenty-three categories. The most important of these exceptions concern disclosure:

(1) to the individual to whom the record pertains;

(2) to others with the prior written consent of the individual, "but only if such consent has been obtained not more than 30 days before the disclosure, or in the time limit agreed to by the individual in the written consent";

(3) to a person representing the individual or the individual's guardian or conservator;

(4) to an agency pursuant to a determination "that compelling circumstances exist which affect the health or safety of an individual, if upon the disclosure notification is transmitted to the individual to whom the information pertains at his or her last known address"; and

(5) pursuant to a search warrant.

inspect and amend her personal information which is maintained by an agency.[351]

A final issue regarding the Fair Information Practices Act concerns the extent to which it provides for independent governmental oversight of processing practices. Currently, California does *not* have such oversight. As originally enacted, the Information Practices Act of 1977 did establish an agency with oversight responsibilities: the Office of Information Practices.[352] This agency was located in the Executive Office of the State Personnel Board. It assisted individuals in identifying records containing their personal information and investigated violations of the Fair Information Practices Act. In addition, the Office possessed the power to develop model guidelines and to mediate disputes about data processing practices between other state agencies and a complaining individual. Despite the considerable promise of this approach, in 1991, the California Legislature, as a cost saving measure, repealed the portion of the Information Practices Act establishing this oversight agency.[353]

Id. §§ 1798.24(a)-(c), (i), (l).

Disclosure exceptions also place restrictions on *data matching* by state agencies. *See* id. §§ 1798.24(e), (h). Such sharing of data can take place *within* the state government or with *outside* entities. *See* id. § 1798.24(p) (allowing disclosure "to another person or governmental organization to the extent necessary . . . for an investigation by the agency for failure to comply with a specific state law which the agency is responsible for enforcing.").

Sharing of data with governmental entities *outside the state government*, such as federal agencies or agencies in other states, can only take place if a California or federal law requires that the information be transferred. Id. at § 1798.24(f). The requirement of statutory authorization sets a high standard for data matching. Indeed, this requirement is more demanding than that of the federal Computer Matching Act, which permits matching following written agreement between the agencies and some other procedural safeguards. *See* supra part II.B.1.b.

In contrast, data matching *within the state government* does not require a statutory authorization, but only a level of congruence with the duties of the recepient agency as expressed in the state constitution or statutory law. In the language of the applicable statute, California state agencies may share information with one another when such a transfer is necessary to perform "constitutional or statutory duties, and the use is compatible with a purpose for which the information was collected and the use or transfer is accounted for . . . ." Cal. Civ. Code § 1798.24(e) (Deering 1994). The most important safeguard here is this law's *compatibility* requirement. Agencies are also required to "keep an accurate accounting of the data, nature, and purpose of each disclosure of a record made . . . ." Id. at § 1798.25. These safeguards on data matching to other state agencies represent a significant advance over those numerous states that leave this practice unregulated.

351. As the Act states, "Each individual shall have the right to inquire and be notified as to whether the agency maintains a record about himself or herself." Id. § 1798.32.

352. The relevant sections of the law were codified at Cal. Civ. Code §§ 1798.4-.8 (repealed 1992).

353. Although no independent governmental oversight exists in California, some assistance is currently provided to citizens by the newly founded Privacy Rights Clearinghouse, which is located at the University of San Diego School of Law's Center for Public Interest Law. This organization receives funding through the Telecommunications Education Trust, established by the California Public Utilities Commission. Center for Public Interest Law, First Annual Report of the Privacy Rights Clearinghouse (1994).

The Privacy Rights Clearinghouse is merely a consumer education program; it provides

Important elements of the model of data protection law have also been implemented in Minnesota,[354] New York,[355] and Wisconsin.[356] These states form, however, an exception to a generally poor level of state data protection law. As noted earlier in this section, one response to this unsatisfactory situation has been federal mandates that oblige states to create data protection measures. These mandates are tied to the receipt of federal funds; for example, if a state wishes to receive federal funds for its institutions of higher education, it must provide data protection for student records.[357] Another federal mandate exists for information in data banks regarding child abuse; Congress has provided funds for states that wish to establish these banks and set requirements for how this information will be collected, stored and disseminated.[358]

---

citizens with information and referrals to other services. The Clearinghouse provides a toll free number for consumers to report privacy abuses and to request information. It also publishes reports on emerging issues and provides a series of one page "fact sheets" to citizens.

354. The Minnesota Government Data Practices Act offers an example of a well thought-out and carefully organized data protection act. Minn. Stat. § 13.01(2) (1982). Minnesota provides a particularly *clear specification of collection purposes.* Id. § 13.02. This right to notice when an agency collects personal data is referred to as the "Tennessen Warning." Id. § 13.04(2); *see also* Donald A. Gemberling & Gary A. Weissman, Data Privacy: Everything You Always Wanted to Know About Minnesota Government Data Practices Act, 8 Wm. Mitchell L. Rev. 573, 586-87 (1982) (discussing the use of the Tennessen Warning).

In Minnesota, *oversight and supervision* of data protection practices is provided by the Commissioner of the Department of Administration. Minn. Stat. § 13.06 (1)-(6). Perhaps the two most important powers of the Commissioner are to promulgate rules that implement the Data Practices Act and to hear appeals from determinations of an agency that contested data are accurate. Id. §§ 13.04(4)(a), 13.07. The Commissioner's initial duty in such cases is "try to resolve the dispute through education, conference, conciliation or persuasion." Id. § 13.04(4)(a). The Commissioner may also refer the matter to mediation. Id. If these efforts are unsuccessful, the Commissioner is either to dismiss the appeal or hold a formal hearing. Id. As a Minnesota Appellate Court has stated, when holding such a hearing the Commissioner "is required to adopt her own findings of fact and to draw her own conclusions from these facts." Hennepin County Community Serv. Dep't v. Hale, 470 N.W.2d 159, 165-66 (Minn. Ct. App. 1991).

355. New York is another state with both a fair information practices law and an oversight institution. N.Y. Pub. Off. Law § 91 (McKinney 1988). The oversight institution is the Committee on Open Government. Id. § 89(2). The Committee is to assist the data subject by investigating data processing practices and issuing advisory statements to agencies. Id. § 93(2). In these statements, the Committee is "to define whether the maintenance of the system is within the lawful authority of the agency." Id. § 93(3).

356. Wisconsin's data protection law features a fair information practices act, which sets procedural limits on computer matching. Until recently, it also established some governmental oversight of the state's data processing practices. Wis. Stat. Ann. § 19.62-19.80 (West Supp. 1994). This oversight was provided in Wisconsin by the Privacy Advocate and Privacy Council. Id. §§ 19.625, 19.63. This structure of oversight was, however, abolished, after a little more than a year. Capital Insights: Cheesehead Blues!, Privacy Times, June 2, 1995, at 1. State budgetary concerns led to the demise of data protection oversight in Wisconsin. Id.; Wisconsin Privacy Council Warns Against Overuse of the Social Security Number, Privacy Advocate, June 19, 1995 (press release on file with the *Iowa Law Review*).

357. 20 U.S.C. § 1232g(b) (1988).

358. For a case finding certain aspects of such a state registry to be deficient, see Hodge v.

The latest example of the trend of federally mandated, state data protection law concerns disclosure of motor vehicle registration information. In the United States, motor vehicle registration and the licensing of drivers takes place on the state, not the federal, level. This information typically includes details about the registered vehicle (model, year of manufacturing) and the driver's name, age, height, weight, and visual acuity.[359] In each state, the respective Department of Motor Vehicles also takes and stores photographs of the driver.[360] In some states, including California, the fingerprints of drivers are collected.[361]

A majority of states have traditionally released motor vehicle registration and driver license information upon request – in some states for free and in others for a fee.[362] The sale of this information can represent a significant source of state income; for example, Michigan raised over a half-million dollars in this way in 1993.[363] Motor vehicle information is avidly sought by direct market mailers who consider it a particularly critical source of age data. As one firm's "data-acquisition director" has stated, "If the volume of age data goes down, that important variable will shrink, and models are going to be less effective. Consequently, profit margins are going to shrink."[364]

Some states have permitted drivers to prevent the release of this information without their permission (an "opt out" program); others have flatly refused the release of these data. According to one recent estimation, twenty states have an opt out program and ten states prohibit the release of both driver license information and vehicle registrations.[365] Recently, this regulatory picture has dramatically changed. The last Congress passed legislation requiring states to allow drivers at least a chance to opt out before their information is released.[366] This law provides an important minimum level of data protection.

Despite the positive effect of federal mandates of data protection in important sectors, this approach cannot, however, take the place of state omnibus laws that institute fair information practices. Federal mandates

---

Carroll County Dep't of Social Servs., 812 F. Supp. 593, 602 (D. Md. 1992).

359. *E.g.*, Cal. Code Regs. tit. 13, § 20.04 (1994) (listing the essential elements of identification for a driver's license).

360. *E.g.*, id. § 20.04 (a)(6).

361. Id. § 330.06 (requiring a completed fingerprint to be submitted with a license application).

362. Paul M. Alberta & Ray Schulz, Driver Privacy Bill Could Kill Motor Lists, 16 Direct Marketing News, Feb. 7, 1994 at 1.

363. Paul M. Alberta, Michigan Senate Mulls Bill to Cut Motor List Access, 16 Direct Marketing News, Mar. 7, 1994 at 1.

364. Alberta & Schulz, supra note 362, at 1 (quoting Tom Atkinson, data acquisition director of the Donnelly Marketing Firm).

365. Id. In addition, three states prohibit only the release of driver license information, and four states refuse the release of only vehicle registration. Alberta, supra note 363, at 1.

366. Driver's Privacy Protection Act of 1994, Pub. L. No. 103-322, 108 Stat. 1796, 2099-2102 (1994) (codified at 18 U.S.C.A. § 2721 (1994)).

can supplement existing state protections in instances in which national uniformity is necessary or state protections have lagged. Yet, such a method makes regulation of the state government's use of data protection the exception and not the rule. Many areas will not be covered by state statutes put in place through federal requirements. For these situations, a more comprehensive safety net must be created. To do so, a fair information practices law should be enacted in all states.

III. TOWARDS AN EXPLANATION OF THE AMERICAN DIFFERENCE

This Article has shown that American law in the public sector includes the participatory model of data protection. It has examined data protection law in various forms—constitutional law, federal statutes, and state regulation. The resulting picture represents sometimes quite subtle regulatory variations on a single theme: the extent to which American law merely responds to a notion of informational seclusion or concerns itself with privacy as participation.

Despite the recognition in the public sector of the privacy-as-participation data protection model, the legal system in the United States has not entirely succeeded in expressing it on the federal level and has generally faltered at the state level. To be sure, actual levels of protection in any given European nation also will exhibit weaknesses when compared with this data protection model.[367] Yet, even if European law sometimes fails to measure up to this ideal, some international experts have argued that Europe offers a level of data protection generally superior to that found in the United States. For example, in his study of comparative data protection law, David Flaherty concludes, "The United States carries out data protection differently than other countries, and on the whole does it less well."[368] In the more recent judgment of Colin Bennett, the American approach is "largely ineffectual in practice."[369] Although this Article has shown the existence of common ground for comparison of European and American data protection law, the United States appears less than successful in its application of the data protection model. An explanation for the American difference in data protection is possible.

The United States treats the government's application of personal information differently than most European nations because its citizens have a different attitude towards the state. To be sure, government in the United States and Europe plays, in many ways, the same role;[370] even

---

367. When Europeans apply data protection laws to judge the permissibility of proposed data transfers, they should compare the reality of protection in a given European nation with the actual legal protections in America. The resulting comparisons of domestic European and United States data protection laws should be made in an attempt to harmonize the world's data protection law at a high level.

368. Flaherty, supra note 2, at 305.

369. Bennett, supra note 2, at 199.

370. *See, e.g.*, Susan Rose-Ackerman, American Administrative Law Under Siege: Is Germany a Model?, 107 Harv. L. Rev. 1279, 1281 (1994) (discussing the similarities and

though American constitutional law does not require attention to the positive goals of a social state, federal and state governments often undertake this task. At the same time, considerable defensiveness, if not hostility, often remains towards this role. For example, even in the characterization of Marmor, Mashaw and Harvey, three academics who are far from conservative, American law has merely created an "insurance/opportunity state."[371] By this term, the authors indicate that the state insures a broad strata of the population from impoverishment due to loss of a breadwinner's salary and offers help to those who have been denied opportunity.[372]

Yet, even beyond the notion of insurance/opportunity, the American state has evinced broad concern for the social, political and physical environment.[373] In both the United States and Europe, the government now accepts varying levels of responsibility for the well-being of citizens in an enlarged "social sphere" that is a domain of political choice and social experimentation.[374] As a result, a flood of statutes and other legal schemes of regulation have modified both the common law and civil code. Yet, these similarities cannot mask a profound, continuing American ambivalence about state power.

The activist state in America is a late invention; the activities of Franklin Roosevelt in response to the Great Depression of the 1930s represent the decisive moment in its creation.[375] Towards this recent creation, however, Americans have nourished an ambivalent, if not schizophrenic, attitude. At the same time that citizens of the United States eagerly accept the fruits of state activism (as shown in the broad popularity of Medicare and Social Security),[376] they also feel unease or even outright hatred for the idea of governmental activism.[377] Compared to Europeans,

---

differences of American and German administrative law in the context of analyzing proposals for administrative reform in the United States).

371. Theodore Marmor et. al., America's Misunderstood Welfare State 31 (1990).

372. Id.

373. See, e.g., Bruce Ackerman, Reconstructing American Law 1 (1984) ("By saying that we live in an activist state, I mean to mark a special feature of our self-consciousness: An awareness that the very structure of our society depends upon a continuing flow of self-conscious decisions made by politically accountable state officials.").

374. As Bruce Ackerman has written:

> Poverty, racism, and sexism are not inexorable givens; they are the consequences of systematic practices in which state officials are self-consciously involved—from the moment at which they grant or deny an impoverished mother a free abortion to the moment at which Medicare sustains, or fails to sustain, the last effort to prolong life.

Id. at 2. *See* Cass Sunstein, Well-Being and the State, 107 Harv. L. Rev. 1303, 1324-27 (1994) (initiating "a process by which the components of well-being would become a substantial part of political debate" requires government to develop an annual "quality of life" report).

375. For a concise description of these events, see Kermit L. Hall, The Magic Mirror: Law in American History 267-85 (1989).

376. Marmor et. al., supra note 371, at 15-19.

377. *See* Peter H. Schuck, Rethinking Informed Consent, 103 Yale L.J. 899, 901 (1994) (noting Americans "abiding, almost obsessive suspicion of state power").

Americans accept only partially the notion of an activist national government. On a deeper level, strong beliefs in individualism and freedom from regulation remain unchanged and unchallenged in the national consciousness.

Ronald Reagan's extraordinary popularity as President was due largely to his ability to tap into this powerful current. In his words, "well-intentioned individuals thought if they were given the power[,] they could right every wrong," but "there's a well-known road paved with good intentions."[378] For him, a regulatory morass was leading Americans straight to hell. Reagan saw himself as an "old sheriff" empowered by the American people to stop "government regulation of private activity" except in "some limited circumstances."[379]

Seven years after the Reagan presidency, part of the political consciousness of many Americans still views government regulation as only an exception, and yearns for a minimalization of the state's activity. Thus, in the last national election, the (unsuccessful) Republican candidate for one of California's seats in the Senate, earnestly declared, "I want a government that does nothing."[380] In somewhat more modest terms, the Republican's election manifesto, the Contract with America, stressed both individual liberty and limited government.[381] This vision is not restricted to that of Reagan or Gingrich Republicans. In John Cheever's journals, amidst the description of his struggles with fleeting artistic inspiration, sexual urges, and alcoholism, the reader suddenly discovers this entry, "And I wake happily from another dream in which I think I live and walk in an accomplished, representative government that is efficient, visionary, and victorious. Bureaucracy has vanished, along with small pox, and we have gone on to better things."[382] In Cheever's dream, government is still possible without bureaucracy.

In the United States, an ambivalence about government has meant skepticism about finding ways for it to *empower* people. The desire for a minimalistic state offers a reason not to regulate. As a result, in the context of data protection, individual self-determination often is seen simply as a pre-existing quality whose protection merely requires an *absence* of state power. The notion of privacy as the absence of government appears most clearly in the lack of federal attention to needed amendments in the

---

378. Ronald Reagan, Remarks at the Annual Meeting of the National Association of Towns and Townships, (Sept. 12, 1983) *in* Pub. Papers 1253.

379. Ronald Reagan, Remarks to Administration Officials on Domestic Policy, (Dec. 13, 1988) *in* Pub. Papers 1617; Letter to the Speaker of the House of Representatives and the President of the Senate Transmitting Annual Economic Report of the President, (Jan. 10, 1989) *in* Pub. Papers 1707.

380. R.W. Apple Jr., The 1994 Campaign: California Senator Struggles for the Senate: In California, A Daily Quest for Cash, N.Y. Times, Oct. 20, 1994, at A-1.

381. Newt Gingrich, Dick Armey, and the House Republicans, Contract with America 4 (1994).

382. Benjamin Cheever et. al., The Journals of John Cheever 340 (1991).

Privacy Act and the failure of many states to create omnibus data protection statutes.[383] It also appears in the lack of independent government oversight of data processing activities.[384] The current low-key American approach to privacy avoids much hard work and many difficult decisions.

Protection of informational privacy does not require a "sheriff," but intelligent choices that structure the flow of personal data. The activist state requires personal information about those whom it is expected to serve and assist. The information society relies on banks of personal data to respond to and shape consumer demand. Yet, the individual's decisionmaking capacity requires that the law set limits to these information flows. The American concept of privacy will not help in creating a data protection law until it concerns itself in a careful and consistent fashion with the protection of the conditions for communal life.

CONCLUSION

The United States possesses the means for data protection: It has a system of legal rules that structure the application of personal data. In this, it shares the conception of data protection held by countries around the world. This Article has argued, however, that such a structure should orient itself not around information seclusion, which forbids the collection and utilization of personal information, but rather around the idea of participation. In a democratic society, individual decisionmaking takes place without and within the life of the community. As a result, data protection law in the computer age should respond by creating social patterns of access to and limitations on the use of personal information.

More specifically, data protection law must concern itself with decisionmaking relating to two critical areas: deliberative autonomy and deliberative democracy. The resulting participatory model of data protection law is best organized through attention to four critical elements: (1) the creation of a statutory fabric that defines obligations with respect to the use of personal information; (2) the maintenance of transparent processing systems; (3) the assignment of limited procedural and substantive rights to the data subject; and (4) the establishment of effective governmental oversight of data use.

This Article has found that American data protection law recognizes the value of privacy as participation; however, it does not yet completely reflect this paradigm. On the level of higher law, the effect of constitutional protections in the United States tends to be strongest when the state's information processing involves issues directly touching the political process. Thus, the state's collection of personal data about members of political groups or its release of personal information that affects the

383. *See* supra parts II.B. & C.

384. *See* supra part II.B.4.

electoral franchise should be subject to searching judicial scrutiny. In contrast, the constitutional protection of the individual's deliberative autonomy has been less certain. The two critical provisions are the Fourth Amendment and *Whalen v. Roe*'s right of informational privacy.

The Fourth Amendment protects the informational seclusion of the individual. Its safeguarding of this realm of seclusion, moreover, occurs only through the protection of a warrant requirement that usually focuses on adequate process rather than the reasonableness of a proposed search. The American right of informational privacy hovers between privacy paradigms of participation and seclusion. Some courts apply *Whalen v. Roe* in a fashion that considers the impact on deliberative autonomy of the state's collection of personal information; other courts view *Whalen* as establishing a restricted right that protects only the information trails of fundamental activities.

An evaluation of statutory protections revealed that the Privacy Act provides the most comprehensive federal structuring of information privacy in the public sector. This law attempts to create a framework that includes all four of the elements of the model of data protection; it reflects a concern for the model of privacy as participation. Yet, the Privacy Act's actual implementation of this model has considerable weaknesses.

The Privacy Act's attempt to create a statutory fabric of defined obligations is undercut by its routine use exemption and lack of substantive limitations on computer matching. Problems with transparency under the Privacy Act concern agencies' exploitation of the routine use exemption, widespread data matching, and vague Privacy Act statements. Considered in tandem with the FOIA, the Privacy Act does, however, heighten the transparency of federal data use by providing important access rights to information. Concerning third party access to personal information, these two laws have been read and applied together in a fashion that is consistent with respect for personal privacy.

The Privacy Act creates the third element of the model of data protection, the assignment of procedural and substantive rights to the individual, but only on a limited basis. Moreover, the remedies available under the Privacy Act are narrow and are unlikely to lead to changes in an agency's data processing practices. These restricted remedies make the fourth element of the data protection model, the independent governmental oversight of data processing activities, particularly important. This Article has discussed the important kinds of activities which a data protection oversight agency should carry out. Unfortunately, the forms of external and internal agency review provided under the Privacy Act do not fulfill these requirements. Existing oversight occurs in a low profile fashion that is unable to stimulate the necessary societal debate about information processing technology and practices.

At the state level, American data protection law is considerably less successful than at the federal level. A general lack of state omnibus laws creates weaknesses in the type of data protection provided. Strong state

traditions of governmental information disclosure create an additional problem. Although this practice contributes to the transparency of data processing on the state level, it can also lead to the release of personal information without adequate consideration of data protection. The trend of federal mandates of state data protection cannot substitute for a comprehensive state approach that should begin with an omnibus law.

In the United States, data protection law in the public sector occurs through an interplay of different kinds of law and institutions. Data protection is found not only in constitutional and statutory law, but, due to the American tradition of federalism, in federal and state law. Moreover, such institutions as courts and administrative bodies act to develop the data protection standards of federal, state, constitutional, and statutory law. This intricate, multi-layered approach is not without promise in fashioning law in an age of rapid change and in an area involving complex technology. Yet, the American approach to data protection can function effectively only if carried out through careful and consistent regulatory efforts. As part of this effort, all states should enact a fair information practices law. Moreover, the creation of a federal data protection commission in the United States is necessary. This institution would play a significant part in an ongoing societal evaluation of the effectiveness of data protection.

In the computer age, individual freedom cannot rest on a dream of being let alone by an ever-reduced government. Today, the safeguarding of liberty requires a legally structured pattern of access to and limitations on the use of personal information. The state has a critical role in ensuring that the processing of personal information is compatible with the individual's ability to participate in democratic self-rule.