William & Mary Bill of Rights Journal

Volume 4 (1995-1996)
Issue 2

Article 3

February 1995

Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection

Lillian R. BeVier

Follow this and additional works at: https://scholarship.law.wm.edu/wmborj

 Part of the Constitutional Law Commons

Repository Citation
Lillian R. BeVier, *Information About Individuals in the Hands of Government: Some Reflections on Mechanisms for Privacy Protection*, 4 Wm. & Mary Bill Rts. J. 455 (1995),
https://scholarship.law.wm.edu/wmborj/vol4/iss2/3

Copyright c 1995 by the authors. This article is brought to you by the William & Mary Law School Scholarship Repository.
https://scholarship.law.wm.edu/wmborj

INFORMATION ABOUT INDIVIDUALS IN THE HANDS OF GOVERNMENT: SOME REFLECTIONS ON MECHANISMS FOR PRIVACY PROTECTION

Lillian R. BeVier*

Information is the handmaiden of the modern activist state. In particular, information provided by individuals to government enables government to assess and collect taxes, to distribute social welfare benefits, and to pursue its regulatory agenda. Computer technology enhances the government's ability to gather, store, analyze, and process personal data. Computers make it easy for government agencies to share with one another information provided to them by individual citizens.

These facts bring issues of "informational privacy" to the fore. In this Article, Professor BeVier examines one such issue, namely that of unconsented-to use by government of accurate information provided by citizens about themselves. Professor BeVier frames the issue in part as a problem in the control of information *but primarily as a problem in the control of* government. *Neither the Privacy Act of 1974 nor the Computer Matching Act of 1988 nor the privacy exemptions of the Freedom of Information Act effectively constrain unconsented-to use or disclosure of personal data by federal agencies. Nor, she concludes, would the Data Protection Board advocated by most other commentators represent a genuine solution.*

* * *

The subject of this Article is identifiable personal data that individuals have supplied to government. The Article's focus will be on the legal and institutional mechanisms that presently protect the privacy of such data. In light of those mechanisms, the Article will inquire whether it is or should be true that information obtained from citizens by the government for one purpose should not be used for another purpose without the consent of the individual.

Information supplied by citizens to government is the indispensable handmaiden of the modern activist state.[1] Consider for a moment the num-

---

* Henry and Grace Charitable Foundation Professor of Law and Elizabeth D. and Richard R. Merrill Research Professor, University of Virginia Law School. I thank University of Virginia Law students Timothy Lawrie '96, and Jeffrey Doctoroff '97, for their able research assistance. Thanks also to my colleagues Richard Merrill and George Cohen for their helpful comments on an early draft; to the very knowledgeable participants in the Marshall-Wythe School of Law Symposium, *Access vs. Privacy*, held in March 1995, and to faculty colleagues at a University of Virginia summer round table discussion for helpful comments.

[1] One commentator has gone so far as to claim:

> Government *is* information. Its employees are nearly all information workers, its raw material is information inputs, its product is those inputs transformed into

ber, scope, and range of the government's activities, and recognize that essential informational corollaries exist for the efficient conduct of each. A full accounting of the occasions in which government, in legitimate—that is to say, constitutionally permitted—pursuit of one or another of its substantive ends, requires citizens to supply it with information about themselves would be pointlessly tedious and unmanageably long. A broad-brush reminder of some of government's most familiar and salient informational demands, however, will help the reader appreciate why the uses that government makes of the personal information that its citizens supply is a pervasive and significant issue.

The government collects revenue. In part because the Internal Revenue Code has become such a complex maze of deductions, exemptions, surcharges, and credits, citizens cannot pay taxes without at the same time providing the government with quite detailed information about their families, jobs, investments, misfortunes, and favorite charities.

The government spends the revenue it collects (and then some!). Among the many projects on which it spends money, the government administers a hugely complicated array of social welfare programs designed to benefit citizens who have a multitude of different needs. It subsidizes home mortgages and insures bank deposits. It supports medical research and contributes funds to provide medical care for elderly and indigent persons. It supplies funds for education, from Head Start programs to graduate student loans. It funds Aid to Families with Dependent Children and gives aid to veterans. It supplements the incomes of those who are poor, blind, aged, and disabled. If government is to achieve the redistributive purposes that these spending programs have been designed to accomplish, it must be able to require that benefit applicants provide it with truthful and appropriately detailed information about their circumstances, the occasion and nature of their needs, and their eligibility for assistance.

Government regulates practically every corner of our lives, including, to mention but a few: our employment practices; the safety of our worksites and their accessibility to disabled persons; the contents and effectiveness of the foods, drugs, and pesticides we market; the design of the airplanes, cars, buses, trains, and bicycles we ride; and the behavior of issuers of financial instruments in markets for publicly-traded securities. The government cannot fulfill its regulatory mission unless those who are subject to the regulations provide regulators with truthful and relevant information that will enable them to monitor the activities of the regulated entities for compliance.

---

policies, which are simply an authoritative form of information. So in a narrow sense, to consider government information policy is not far from considering the essence of government itself.

Harlan Cleveland, *Government Is Information (But Not Vice Versa)*, 46 PUB. ADMIN. REV. 605, 605 (1986).

The fact that the government collects such great quantities of data gives rise to concern in many corners that the data will be inappropriately disseminated, within government or to outsiders, or that it will be otherwise misused or abused. Recent advances in computer technology, which permit data to be manipulated, organized, compiled, transferred, distributed, and retrieved with hitherto unimaginable ease, exacerbate such concern.

This Article addresses an aspect of that concern, namely the question of what government does with individually identifiable information it collects from individuals about themselves. Though I acknowledge that a great deal of valuable proprietary business information—from trade secrets,[2] pesticide formulae,[3] employment practices,[4] airplane designs,[5] and the like—must be supplied to the government so that it can carry on its regulatory mission, and that guarding the confidentiality of this information poses a significant challenge of its own, this Article does not address that problem. Instead it follows the convention that has developed in the privacy literature and confines its inquiry to what that literature implicitly (and correctly) regards as the analytically separate question of how—and whether—to guard personal data. This Article describes and evaluates the most significant legal and institutional mechanisms that presently exist to protect identifiable personal data about individuals that the government has collected from them. It considers whether individuals have meaningfully enforceable rights, or even legitimately entertained expectations, of being able to control the use or dissemination—within the government itself or to outsiders—of personal information from or about them that the government has collected from them in pursuit of one facet or another of its vast and multifarious substantive mission.

Because privacy is so large and complex a topic, and because the legal and institutional mechanisms for protecting private information in government's hands are somewhat diffuse, a few words are in order to limit the scope and agenda of this Article. In that it proposes to *consider* certain questions rather than setting itself the task of definitively *answering* them, this Article's agenda is relatively modest. This Article will paint a complicated legal landscape with a broad brush, hopefully avoiding inaccuracies but deliberately omitting a myriad of detail. Rather than offering a detailed summary of a comprehensive research project, this Article offers what I believe is at least a provocative perspective,[6] aiming to identify some im-

---

[2] *See, e.g.*, National Parks & Conservation Ass'n v. Morton, 498 F.2d 765 (D.C. Cir. 1974).

[3] Ruckelshaus v. Monsanto Co., 467 U.S. 986 (1984).

[4] Chrysler Corp. v. Brown, 441 U.S. 281 (1979).

[5] G.S. Rasmussen & Assocs. v. Kalitta Flying Serv., 958 F.2d 896 (9th Cir. 1992), *cert. denied*, 113 S. Ct. 2927 (1993).

[6] In fact, this Article is a preliminary part of a comprehensive study, *Privacy in Telecommunications*, that I am undertaking for the American Enterprise Institute. In the

portant issues that the privacy community has sometimes tended to neglect, and to cast a different light on some familiar themes.

Any discussion that purports to be about "privacy" must begin by defining how it proposes to use the term. Privacy is a chameleon-like word, used denotatively to designate a range of wildly disparate interests—from confidentiality of personal information to reproductive autonomy[7]—and connotatively to generate goodwill on behalf of whatever interest is being asserted in its name. For example, more than a hundred years ago, in their classic article, Warren and Brandeis advocated protection for a "right to be let alone."[8] Seventy years later, in an influential synthesis of common law developments to date, Dean Prosser discovered that under the rubric of the "right of privacy," common law courts had protected plaintiffs from four quite distinct kinds of injuries: intrusion upon their solitude or into their private lives, public disclosure of embarrassing private facts, publicity putting them in a false light, and appropriation of the commercial value of their name or likeness.[9]

This Article is concerned with what commentators in recent years have begun denominating as a distinct interest in "informational privacy." Freedom from unwanted disclosure of personal data is perhaps the most important manifestation of the interest, but for its advocates, securing informational privacy requires more than just granting legal protection to secret-keeping. What advocates regard as being fundamentally at stake in the claim to informational privacy is *control* of personal information.[10] As Alan Westin explained in his seminal and much-cited study, to speak of a right of informational privacy is to invoke a "claim of individuals . . . to *determine*

---

course of that more comprehensive work, I will inevitably reconsider many of the conclusions expressed here. In addition, I anticipate that I will substantially revise the organizational framework. Thus it would be appropriate for the reader to regard the present analysis as provisional.

For a differing perspective on the nature of the problem involved in government collection, use, and dissemination of personal data, see Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 533 (1995), which was published just as the present Article was going to press, thus precluding the detailed response herein that it would have merited.

[7] The right to abortion was originally denominated as an aspect of a woman's right to privacy. Roe v. Wade, 410 U.S. 113 (1973).

[8] Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 193 (1890). The article has spawned a rich literature. *See, e.g.*, *Symposium: The Right to Privacy One Hundred Years Later*, 41 CASE W. RES. L. REV. 643 (1991).

[9] William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 389 (1960).

[10] *See* Marc Rotenberg, *In Support of a Data Protection Board in the United States*, 8 GOV'T INFO. Q. 79, 80 (1991) ("Privacy is the right of individuals to control the disclosure of personal information and to hold those accountable who misuse information, breach a confidence, or who profit from the sale of information without first obtaining the consent of the individual.").

for themselves when, how, and to what extent information about them is communicated to others."[11]

This Article is not concerned with every context in which informational privacy might be thought to be at risk. It does not address issues in the gathering and exchange of information by actors in the private sector.[12] Its concern is instead limited to the individual rights to control the use and dissemination of personally identifiable information *in the hands of government.* Specifically, its focus is on the use by government of information that individuals *have disclosed to the government,* or have revealed in the context of an encounter directly with the government, for purposes other than that for which they disclosed the information or for use in a context different from that in which it was revealed. Note that in being so limited, this Article addresses a "right of privacy" that has already been importantly compromised, for its subject is individuals' rights with respect to information that they have *already* disclosed to the government, either because the disclosure was an inevitable byproduct of a citizen-government encounter, or because individuals were required to reveal the information in order that the government could pursue one or another of the items on its constitutional, legislatively-endorsed, substantive agenda.

The inquiry does not address the Fourth and Fifth Amendment questions of when individuals have rights to *withhold* information from the government in what have come to be regarded as run-of-the-mill regulatory contexts. If those were the topics of this inquiry, it would be mercifully short. As Professor William Stuntz has convincingly demonstrated, when it came to a choice between protecting privacy by permitting citizens to resist the government's demands for information or facilitating an active regulatory agenda by allowing government to compel citizens to provide it with substantial amounts of information, the Supreme Court followed the prevailing political winds and chose to facilitate the regulatory agenda.[13] Except with respect to keeping secrets from the police, there is very little—if anything—left of individuals' *constitutional* claims to keep facts about them-

---

[11] ALAN WESTIN, PRIVACY AND FREEDOM 7 (1967) (emphasis added); *see also* CHARLES FRIED, AN ANATOMY OF VALUES 140 (1970) (noting that privacy is the "control we have over information about ourselves").

[12] For an informative treatment of some of the legal and policy issues that remain to be resolved with respect to informational privacy in the private sector, see Jonathan P. Graham, *Privacy, Computers, and the Commercial Dissemination of Personal Information,* 65 TEX. L. REV. 1395 (1987). For a paradigmatic cry of alarm about the threats that privately-held databases pose to informational privacy, see Peter Hernon, *Privacy Protection and the Increasing Vulnerability of the Public,* 11 GOV'T INFO. Q. 241 (1994).

[13] William J. Stuntz, *Privacy's Problem and the Law of Criminal Procedure,* 93 MICH. L. REV. 1016, 1048-60 (1995).

selves to themselves when government asks for information for a regulatory, revenue-collecting, or benefit-conferring purpose.[14]

This Article begins where Professor Stuntz left off. It assumes that the government did not abuse its constitutional authority nor infringe individual rights when it collected or gathered the information. Nevertheless, it assumes that it is relevant to ask whether individuals might assert some residual right or legitimate claim to "privacy," even over information they have already disclosed to the government. Contrary to Professor Stuntz's assertion that "a great deal of compelled information gathering occurs in ways that ensure that the information stays secret vis-à-vis the public" because "the federal Privacy Act often requires as much,"[15] the government's promise that it will not further disclose information that it has compelled citizens to supply is neither consistently enforced nor readily enforceable.[16] Taking as given that the government did not, in pursuing the substantive agenda that gave rise to its need for the information, act in excess of its constitutional power to tax, to spend money, or to regulate the activities of its citizens, this Article's analysis proceeds on the assumption that the questions of how, and how much—and even of what it means—to protect the privacy of individually identifiable information in the government's hands are not of constitutional dimension.[17] This assumption hardly means that the questions

---

[14] It has been suggested, for example, that when activity itself is constitutionally protected, it ought perhaps to be "immune from inquiry and dissemination by the government." Seth F. Kreimer, *Sunlight, Secrets, and Scarlet Letters: The Tension Between Privacy and Disclosure in Constitutional Law*, 140 U. PA. L. REV. 1, 132 (1991).

[15] Stuntz, *supra* note 13, at 1041-42.

[16] *See infra* text accompanying notes 99-110.

[17] Not everyone believes that failing to provide constitutional protection against disclosure by government of information it has collected from citizens is normatively appropriate. *See, e.g.*, Heyward C. Hosch III, Note, *The Interest in Limiting the Disclosure of Personal Information: A Constitutional Analysis*, 36 VAND. L. REV. 139, 191 (1983) (arguing that because disclosure of personal information by the government can irreparably harm an individual's right to control freely the direction of his life, such disclosures should be subject to constitutional review pursuant to a heightened rational basis standard of review); *see also* Francis S. Chlapowski, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 158-60 (1991) (arguing that the individual interest in informational privacy should be recognized as a constitutionally protected right); Robert S. Peck, *Extending the Constitutional Right to Privacy in the New Technological Age*, 12 HOFSTRA L. REV. 893, 898 (1984) (same); James J. Tomkovicz, *Beyond Secrecy for Secrecy's Sake: Toward an Expanded Vision of the Fourth Amendment Privacy Province*, 36 HASTINGS L.J. 645, 667-70 (1985) (same).

The Supreme Court has left open at least the possibility that it might consider imposing a constitutional duty to avoid unwarranted disclosure. In Whalen v. Roe, 429 U.S. 589 (1977), the Court rebuffed a privacy-based constitutional challenge to a New York statute that required "doctors to disclose to the State information about prescriptions for certain drugs with a high potential for abuse, and provide[d] for the storage of that information in a central computer file." *Id.* at 606 (Brennan, J., concurring). The

can be assumed to have been fully resolved. The absence of a constitutional command that privacy be protected is not the equivalent of a prohibition on greater protection, because the Constitution is neither the sole means by which government's power may be limited in privacy's name nor the sole repository of the nation's values. Scholarly commentators are free to suggest, and legislative policymakers are free to enact, further compromises of the privacy of the information that government collects from its citizens if they deem such compromises necessary to the achievement of more pressing public goals. They are also free to shore up privacy's existing, rather porous, legal protections if that seems to them to be the wiser course.

These realities are important to the analysis. When individuals are required to provide masses of information about themselves simply as a condition of being permitted to carry on one or another facet of their lives, to pursue their livelihood in a law-abiding way, or to receive a government benefit to which their circumstances and the terms of the governing statute entitle them, they have already ceded to the government an important measure of their practical capacity to control further uses of that information (not to mention their capacity to control the particular aspect of their lives which the information embodies). Acknowledgement of these realities—of the pervasiveness of compelled disclosure, of the variety and ubiquity of government programs that could not go forward without disclosure, and of the fact that sharing of personally identifiable information among government agencies is widespread and widely known to take place—brings the policy issue into focus. Acknowledging these realities also suggests that the analysis is likely to be unhelpful if it contents itself merely with trying to specify the substance of individuals' rights to control or the scope of government's duties to protect *information*. Such an analysis would be unhelpful because, however difficult the task of defining respective rights and

---

Court recognized that its "cases sometimes characterized as protecting 'privacy' have in fact involved at least two different kinds of interests. One is the individual interest in avoiding disclosure of personal matters, and another is the interest in independence in making certain kinds of important decisions." *Id.* at 598-600 (footnote omitted). The Court further recognized that the New York statute might impair both interests. *Id.* at 600. It held, however, that the statute did not "pose a sufficiently grievous threat to either interest to establish a constitutional violation." *Id.* Acknowledging that there may well be a "threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files," the Court nevertheless expressed itself satisfied that New York's statutory scheme evinced a "proper concern with, and protection of, the individual's interest in privacy." *Id.* at 605. Justice Stevens explicitly reserved the constitutional question that "might be presented by the unwarranted disclosure of accumulated private data—whether intentional or unintentional—or by a system that did not contain comparable security provisions." *Id.* at 605-06. It remains true, however, that the Court has not yet confronted such a question, much less decided that a constitutional duty of nondisclosure exists.

duties might be, the task of designing effective enforcement mechanisms to protect the rights and enforce the duties is even harder. In other words, the problem of privacy of information in government's hands ought to be seen as only partly a problem in the control of information; the problem ought to be seen most importantly as one in the control of *government*. When the problem is recognized for what it is, its intractability becomes more readily apparent.

The privacy issue is not customarily framed in the way this Article proposes to frame it. Indeed, the literature on the privacy of personal information in the hands of government tends to approach the issue as if it were principally about individual rights and government duties, as if "information" were a tangible item easily cabined within bureaucratic and legal boundaries, and as if the value of privacy itself were uncontested—albeit too often compromised. Ignoring the possible relevance of the fact that individuals must and do comply with demands for information about themselves from innumerable government agencies for innumerable different purposes, commentators frame the problem of what government does with that information as if the problem could be made to yield to a conventional analysis aimed at uncovering the values at stake and the threats to which they are so constantly subjected. In other words, many commentators seem to assume that the problem of what government does with personal information in its possession can be "solved" if only the substance of an appropriately conceived notion of privacy can somehow be "enacted" into law.[18] When these commentators run into difficulties with this approach, as they almost always do—when they are forced to acknowledge, for example, that the enactments themselves have less practical impact upon either bureaucratic behavior or government information management practices than their texts might suggest—they tend almost uniformly to call for the creation of a new, independent, federal agency: a Data or Privacy Protection Board.[19] They thus embrace "oversight" by one government agency of other government agencies as a workable solution to the problems of bureaucratic intransigence that data protection issues tend to encounter.

This Article suggests that a useful answer to the question of how to guarantee an appropriate amount of privacy for personal information that is legally in the hands of the government is not likely to emerge simply by adumbrating the parameters of individuals' normatively appropriate claims for control of the government's use and dissemination of data about themselves. Nor will an abstract pronouncement of the government's duties provide a genuine solution. As long ago as 1973, a Code of Fair Information

---

[18] *See, e.g.*, PRISCILLA M. REGAN, LEGISLATING PRIVACY at xiii (1995) (arguing that "[f]or those interested in protecting privacy, the dynamics of congressional policy-making point to the need to rethink the importance and meaning of the value of privacy").

[19] *See infra* text accompanying notes 239-50.

Practices was propounded by the Department of Health, Education and Welfare.[20] Among its principles were the following:

> 1) There must be no personal-data record-keeping systems whose very existence is secret.
> 2) There must be a way for an individual to find out what information about him is in a record and how it is used.
> 3) There must be a way for an individual to prevent information about him obtained for one purpose from being used or made available for other purposes without his consent.
> 4) There must be a way for an individual to correct or amend a record of identifiable information about him.
> 5) Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability for their intended use and must take reasonable precautions to prevent misuse of the data.[21]

No voices have been raised in dissent to the merits of these principles, and in fact they have been essentially "enacted" in the federal Privacy Act of 1974.[22] So long as these principles are stated in the abstract and presented as if implementing them is costless and does not require the potential sacrifice of other policies with which they might be in competition, such as efficient administration of government programs or effective enforcement of criminal laws, it is hard to imagine an argument on the merits that could be mounted against them.[23] Yet as I hope to demonstrate in the pages that follow, it is far more complicated to assure that in practice the government will act consistently with that which the principles require. Indeed, there is a question as to whether society is in reality as genuinely committed to implementing them as our facile agreement with their statement in principle might suggest. And unfortunately, on careful examination, the concept of a Data Protection Board as a cure for our failure to implement fully fair information practices has some hitherto unremarked flaws.

This Article will proceed as follows. Part I will frame the issue as a

---

[20] SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, U.S. DEP'T OF HEALTH, EDUC. & WELFARE, PUB. NO. (OS)73-94, RECORDS, COMPUTERS, AND THE RIGHTS OF CITIZENS (1973).

[21] *Id.* at 41.

[22] 5 U.S.C. § 552a (1994); *see infra* text accompanying notes 82-101.

[23] *Cf. Oversight of the Privacy Act of 1974: Hearings Before the Subcomm. on Government Information, Justice, and Agriculture of the House Comm. on Government Operations*, 98th Cong., 1st Sess. 273 (1983) [hereinafter *Hearings*] (testimony of John Shattuck, Legislative Director, ACLU) ("The Code of Fair Information Practices which constitutes the core of the statute is so general and abstract that it has become little more than precatory in practice, and has proved easy to evade.").

problem in the control of information. It will identify the threats with respect to the use and disclosure of information about which privacy advocates have expressed the most concern, concentrating on the "cornerstone" fair information principle that any information obtained for one purpose should not be used for another purpose without the consent of the person.[24] It will also try to identify exactly what privacy advocates have in mind when they talk about "abuse" and "misuse" of information in government's hands, and will describe how computers increase the challenge of devising and achieving effective institutional solutions to information management problems.

Part II will reformulate the issue, posing it not as one of the control of information but explicitly as an issue in the control of *government*. Part II will also offer a number of reasons why the task of formulating reliable strategies for protecting informational privacy is so formidable: privacy is, in practice and in principle, in genuine tension with other important substantive goals; individuals are not good guardians of their own privacy rights; government actors are poorly or unreliably motivated to protect citizens' privacy rights, and their performance as privacy protectors is difficult to monitor; and institutional solutions to the privacy problem are elusive because information itself is inherently difficult to contain within legal boundaries. To illustrate its principal themes, Part II will survey the present legal landscape at the federal level, focusing on the Privacy Act of 1974,[25] the Computer Matching Act of 1988,[26] and the Freedom of Information Act.[27] This Article will conclude by offering an admittedly skeptical analysis of the panacea that most privacy advocates continue to champion, namely a Federal Data Protection Board.

I.

A crucial beginning for an inquiry that frames the privacy issue as one of how to control information in the hands of government is to define, in the abstract, the parameters of *legitimate* governmental use of information that citizens provide to it, and whence the limits of legitimacy are derived. Much of the privacy literature is permeated with a vague Orwellian angst about this issue;[28] sometimes attempts are made to give the angst a genuine

---

[24] Rotenberg, *supra* note 10, at 81; *see also* JERRY BERMAN & JANLORI GOLDMAN, A FEDERAL RIGHT OF INFORMATION PRIVACY: THE NEED FOR REFORM 12 (Benton Foundation Project on Communications and Information Policy Options ed., 1989) (providing a way for an individual to prevent personal information obtained for one purpose from being used for another purpose without consent "became the heart of the Privacy Act and the information privacy legislation that followed").

[25] 5 U.S.C. § 552a (1994).

[26] 5 U.S.C. § 552a(o) (1994).

[27] 5 U.S.C. § 552 (1994).

[28] *See, e.g.*, DAVID FLAHERTY, PROTECTING PRIVACY IN SURVEILLANCE SOCIETIES 1

basis in reality. As one commentator has noted:

> The privacy literature is liberally sprinkled with horror stories about inaccurate, incomplete, irrelevant, or derogatory information maintained in files; about personal information kept far longer than is necessary; about access by unauthorized people and organizations; about data in the files of private and public bodies not authorized to receive them; about data being used out of context, for purposes other than those for which they were collected; and about deliberate intrusion and misuse of data files by unauthorized and authorized personnel.[29]

Thus, from the literature one senses that there is reason for grave concern that government soon will be—indeed that both government and private entities are at this very moment—*systematically* engaged in "abuse" and "misuse" of the vast amounts of personal information they have collected from all of us for such a wide variety of purposes. The cries of alarm become even more shrill when the overarching threat posed by computers' enhanced capacities to store and manipulate information is seen as looming over the scene.[30]

From the horror stories and the angst, one particular worry consistently emerges, namely, the apprehension that information gathered for one purpose will be used or disclosed for different purposes.[31] This concern arises, it is asserted, because "[m]ost individuals agree to provide personal information to . . . governments because the benefits gained . . . are worth the price of diminished privacy. *The cornerstone of that agreement, however, is the individual's assumption that the information will not be used for purposes*

(1989) ("[I]ndividuals in the Western world are increasingly subject to surveillance through the use of data bases in the public and private sectors, and . . . these developments have negative implications for the quality of life in our societies and for the protection of human rights."); Graham, *supra* note 12, at 1402 (suggesting that the "loss of privacy is the most serious casualty of the information age"); George B. Trubow, *Protecting Informational Privacy in the Information Society*, 10 N. ILL. U. L. REV. 521, 523 (1990) (declaring that personal privacy is "under siege").

[29] COLIN J. BENNETT, REGULATING PRIVACY: DATA PROTECTION AND PUBLIC POLICY IN EUROPE AND THE UNITED STATES 35-36 (1992) (footnote omitted).

[30] Rotenberg, *supra* note 10, at 79 ("The United States must move quickly to address the growing privacy problems that arise from the collection and transfer of personal information generated by computerized recordkeeping systems.").

[31] *See, e.g.*, Xavier R. Lopez, *Balancing Information Privacy With Efficiency and Open Access: A Concern of Government and Industry*, 11 GOV'T INFO. Q. 255, 257-58 (1994); John Shattuck, *In the Shadow of* 1984*: National Identification Systems, Computer-Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 1000 (1984).

other than those for which it was collected."[32]

This Article will focus principally on the issue of whether information obtained for one purpose should be used or disclosed, either within government or to outsiders, for another purpose without the consent of the person. The nature of the issue is surprisingly hard to pin down. The first question to ask is what might justify a principle that would prohibit unconsented-to use of information for other than the precise purpose for which it was disclosed. The answer is not immediately obvious. There is no data to support the empirical claim that people assume that information will not be used for other purposes. Indeed, many commentators implicitly acknowledge that in most cases, people make no assumption at all about what will happen to the information they supply. They are either careless[33] or clueless[34] about other uses that might be made of it. Indeed, if people did assume that information supplied for one purpose would not be used for other purposes, their assumption would be nothing if not counterfactual.[35] Whether people *ought* to be able to make such an assumption, however, is the real question to be answered. Perhaps it is reality and not people's mistaken assumptions that should be changed. The issue, then, is whether and under what circumstances such sharing should be considered *a priori* "abusive" of a fair information practice to which we genuinely wish to adhere—a practice which puts true information, already disclosed by individuals to the government for one purpose, to other uses for which it might be relevant. What unconsented-to "collateral uses" of true information deserve to be opprobriously labelled "abuses" or "misuses" of information, and why? These are the questions to which this Article will turn momentarily. First it is important to clarify what the "cornerstone principle"[36] of "no unconsented-to use of information" is *not* about.

The "cornerstone principle" is not about making use of inaccurate, irrelevant, or untimely information, nor is it about making decisions based on erroneous data.[37] There is, of course, an important individual and societal

---

[32] Carol R. Williams, Note, *A Proposal for Protecting Privacy During the Information Age*, 11 ALASKA L. REV. 119, 134-35 (1994) (emphasis added).

[33] Priscilla M. Regan, *Privacy, Government Information, and Technology*, 46 PUB. ADMIN. REV. 629, 633 (1986) ("Most people are so accustomed to disclosing information that they rarely think through all of the possible consequences.").

[34] Kreimer, *supra* note 14, at 115 ("[E]ven in the case of information revealed without unconscionable inducements, our intuitions have not caught up with our technology; we do not understand the scope of a disclosure into an electronic environment.").

[35] *See infra* notes 48-50 and accompanying text.

[36] Williams, *supra* note 32, at 134-35.

[37] *Cf.* Dennis Southard IV, *Individual Privacy and Governmental Efficiency: Technology's Effect on the Government's Ability to Gather, Store and Distribute Information*, 9 COMPUTER/L.J. 359, 370 (1989) (noting that when "large amounts of information are being handled, the potential for both intentional and accidental misuse exists,"

interest in not making decisions about individuals based on erroneous data about them. Indeed, this interest in the accuracy of government records is not only reflected in at least two provisions of the Code of Fair Information Practices;[38] it is also embodied in several provisions of the Privacy Act of 1974[39] and the Computer Matching Act.[40] It is quite uncontroversial to assert that we want systems of government record-keeping and information processing that reduce error as much as feasible, into which are built cost-effective mechanisms for correcting errors that do occur, and out of which have been squeezed, to the extent reasonably possible, the chance that remaining errors might become the basis for decisions that adversely affect individuals. Error-free information processing is not an attainable goal, but the impact of inevitable processing errors can be substantially ameliorated by the adoption of appropriate verification methods and decision-making processes.

Note, however, that record-keeping methods and decision-making processes are procedural strategies for avoiding errors. The need to devise such strategies as part of a program of "fair information practices" implies that information is "misused" or "abused" when decisions are based on data that lacks a secure factual foundation. It is not "fair" to use or disclose untrue information.

Note, on the other hand, that preventing unconsented-to disclosures has to do with the use and dissemination of *true*—not false or misleading or inaccurate—information. This fact raises the questions of how use or dissemination of true information could be "unfair," or could be said to represent a "misuse" or "abuse." By what criteria could use or dissemination of true information be called "unfair"? Put another way, what justifications support the claim that unconsented-to use or dissemination of true information is wrong in principle? One place to begin looking for answers to these questions, oddly enough, is with a brief list of contexts in which such disclosures or uses by government officials would probably be universally condemned: disclosure by government employees for their own personal gain or amusement of true information about individuals acquired by the government employees in the course of their official duties;[41] gratuitous or mali-

---

citing an example of one case in which the Massachusetts welfare department threatened to cut benefits to a woman because a bank account belonging to someone with a similar social security number had been erroneously attributed to her, and using the example of this one mistake to support the claim that "[a]s the use of new technology increases, so does the potential for *misuse*") (emphasis added).

[38] *See supra* text accompanying note 21.

[39] 5 U.S.C. §§ 552a(e)(5)-(6), (g)(1)(C) (1994).

[40] *Id.* § 552a(o)(1)(E), (J).

[41] For example, Internal Revenue Service employees in the southeastern United States examined returns of celebrities and even collected information on divorced individuals to sell to private investigators. Of 165 employees disciplined for these abus-

cious disclosure of information obtained under a statutory or otherwise legitimately relied-upon (because expressly tendered by a government official) promise of non-disclosure;[42] gratuitous or malicious public disclosure of intimate or personally embarrassing facts in a context in which disclosure could serve no conceivable public purpose; or use of legitimately acquired personal information to intimidate a government official's political enemies.[43] The common characteristic of these damnable practices is, of course, that each entails a breach of the public trust in that each entails a use or disclosure of information that serves no legitimate, legislatively-endorsed public policy goal. The "cornerstone principle" of "no unconsented-to use of information" condemns such practices. My point, though, is that it also condemns unconsented-to uses and disclosures, either those within government or to outsiders, *of accurate information already given to government for one legitimate, legislatively-endorsed purpose that would make a contribution to government's achievement of another legitimate, legislatively-endorsed purpose.* On what foundation rests the claim that such practices as these are so wrong in principle that preventing them is a "cornerstone" of a system of fair information practices?

The claim to informational privacy that is embodied in the supposed right to withhold consent from subsequent uses of true information about oneself does not rest on the societal value of accurate decisionmaking by government in individual cases; nor does it rest on the efficient achievement of the government's policy goals. Indeed, claims to informational privacy are in considerable tension with both accurate decisionmaking and efficient policy implementation. Informational privacy is about individual control of information regarding oneself. The instrumental function that privacy advocates believe a right to informational privacy serves is to support the freedom of self-definition, the freedom to "edit" ourselves as we go along. Informational privacy gives us "freedom to define ourselves," to let people know only that which we think they should know about us.[44] This freedom in turn enhances individual autonomy, for when people have control over information about themselves and can prohibit information disclosed for one

---

es, 36 were suspended, 17 fired, and the rest were reprimanded or sent to counseling. *See Invasion of Privacy: Some IRS Employees are Guilty of Snooping*, SAN DIEGO UNION-TRIB., Aug. 7, 1994, at G2.

[42] It is important to recognize that some "[p]romises of confidential treatment . . . are of little value . . . . [b]ecause such promises cannot vary the agency's duty under the FOIA to disclose all nonexempt information. . . ." Stephen S. Madsen, Note, *Protecting Confidential Business Information from Federal Agency Disclosure After* Chrysler Corp. v. Brown, 80 COLUM. L. REV. 109, 113 (1980).

[43] It was abuses such as these that led to consideration and eventual passage of the Privacy Act of 1974. For general background, see WAYNE MADSEN, HANDBOOK OF PERSONAL DATA PROTECTION 100-03 (1992).

[44] Charles Fried, *Privacy*, 77 YALE L.J. 475, 485 (1967).

purpose from being used for another, they are more able than they otherwise would be "to do what, for fear of an unpleasant or hostile reaction from others, they would otherwise not do."[45] Individuals suffer a "potential chilling effect on [their] exercise of . . . independent judgment" when they know that information about them may be used for a purpose different from that for which it was gathered or that it may be disclosed to someone with interests adverse to their own.[46] "The right to control the flow of information about oneself in order to escape unjustified social repercussions is essential to protect actual identity."[47]

A noteworthy feature of privacy advocates' arguments with respect to the interest in controlling the use and dissemination of information in the hands of government is that they do not view individuals' initial disclosures to the government itself as anything like a fatal compromise of the right to control information nor even a clear incursion on the subject's independent judgment. The initial disclosure is almost never completely voluntary, for it almost certainly is made in order to comply with the tax laws, to conform to the mandates of a particular regulatory regime, or to qualify for a government benefit of one kind or another. Although privacy advocates tend to dismiss arguments that the initial disclosure is appropriately deemed a "waiver" of rights with respect to subsequent use,[48] they also do not justify their opposition to subsequent disclosure on sustained arguments that the original disclosure was genuinely coerced. Nor do they confront certain obvious incongruities of their claims. On the one hand, privacy advocates assert that individuals have a "right" to insist that information about them be used only for the purpose for which it was gathered and that invasion of this right impairs the individual capacity for independent judgment.[49] On the other hand, they find themselves having to acknowledge both the legal reality that the "right" is simply not significantly protected by law, and the practical

---

[45] Graham, *supra* note 12, at 1411.

[46] Southard, *supra* note 37, at 370.

[47] Chlapowski, *supra* note 17, at 154; *see also* Arthur R. Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUM. RTS. L. REV. 1, 5-6 (1976) ("When a citizen knows that his conduct and associations are being put *on file* and that the information might be used to harass or injure him, he may become more concerned about the possible content of that file and less willing to risk asserting his expressional rights."); Peck, *supra* note 17, at 898-99 (1984) ("The chilling effect of a loss of privacy is the undesirable incentive to conform to perceived societal norms rather than assert one's individuality in ways that may threaten to cause a loss in personal or professional associations."); Tomkovicz, *supra* note 17, at 667 ("Just as confidentiality-type privacy, in general, permits individuals to be themselves, to behave and conduct their lives in ways that might otherwise be difficult and impractical, if not inconceivable, constitutional informational privacy enables people to enjoy and freely exercise other entitlements afforded by our free society.") (footnote omitted).

[48] *See* Kreimer, *supra* note 14, at 110-15.

[49] *Id.* at 113-14.

reality that in the modern world information about individuals is constantly, uncontrollably, and inevitably being cycled and recycled; it is the indispensable coin of social, commercial, and political exchange.[50] Thus, the idea that individuals in any meaningful sense can—or should be able to—"control" the circulation of facts about themselves does not mesh well with the realities of this complex, information-hungry world in which we live, this world in which the activist state has the biggest information-appetite of all.

In addition to their failure to come to grips with these practical realities, advocates of informational privacy as means to the end of self-definition tend to give short shrift to a powerful, principled counter-argument. Permitting individuals to control information about, and thus selectively to conceal, their past may indeed enhance their autonomy *ex ante* by permitting them to act without fear of an unfavorable reaction from others.[51] This freedom to engage in behavior that might evoke hostile reactions, however, is purchased at others' expense. Indeed, the freedom being advocated is susceptible to being recast in pejorative terms as a license to escape from responsibility for the consequences of one's actions. Giving individuals the right to control the use and dissemination of true information about themselves, and to limit its use and disclosure to the precise purpose *they* had in mind when they initially disclosed it, in effect would countenance the concealment by them of discreditable facts that would lower them in the esteem of others. "One incentive for responsible behavior associated with publicity is the concrete benefit of a good reputation."[52] The ability to conceal discreditable facts about oneself permits one to acquire that benefit without having to pay the full behavioral price. In the context of personal information in the hands of government, giving individuals the right to control information about themselves might permit them to avoid paying taxes they actually owe, to escape meeting support obligations to their children, to avoid paying legitimate debts, or to receive benefits to which they are not entitled. To embrace a principle that would countenance such results would seem to be the equivalent of endorsing the "fraudulent concealment" of personal information.[53]

---

[50] There are so many contexts in which information about individuals enhances opportunities for fruitful and productive exchange that citations to support the proposition in text seem superfluous. Consider, for example, how central the free flow of information about government and government officials is to a democracy, how essential information about the integrity and reliability of potential contracting partners is in a market economy, how significant to a satisfying social life and business career is one's reputation, which is the effective summation of available information about oneself. Indeed, the First Amendment itself testifies to the value of information about individuals, even to the point of privileging the publication of falsehoods so as not to chill the publication of the truth. *See* New York Times v. Sullivan, 376 U.S. 254 (1964).

[51] *See* Graham, *supra* note 12, at 1411.

[52] Kreimer, *supra* note 14, at 91.

[53] For the clearest exposition of the economic arguments in favor of a legal regime

At the very least, a stance embracing concealment raises the question of why individuals should have the right to conceal information about that which they fear others might consider to be their "defects," thus misleading people—or the government—into dealing with them on terms more favorable than they would if they knew the truth. It is hard to imagine that, on reflection, many individuals would choose to live in a world where everyone was free to conceal discreditable facts about herself. Such a world would be inherently unstable: individuals would search for—and no doubt find—so many means of bonding the trustworthiness of their self-disclosures that the baseline rule of "freedom to conceal" would tend to be overwhelmed by evasive tactics.[54]

Whether the substantive concerns that animate privacy advocates' arguments have secure normative or positive foundations, the fears of privacy advocates undoubtedly have been considerably exacerbated and in some ways transformed in recent years by the incredible advances in computer technology that have so vastly, and so incomprehensibly, increased the government's capability to gather, store, manipulate, organize, compile, transfer, distribute, and retrieve data.[55] Indeed, it is difficult to imagine

---

in which concealment of discreditable facts about oneself is treated similarly to fraud in the sale of goods, see Richard A. Posner, *Privacy, Secrecy and Reputation*, 28 BUFF. L. REV. 1, 11-17, 24-30 (1979); Richard A. Posner, *The Right of Privacy*, 12 GA. L. REV. 393, 394-404 (1978).

[54] *Cf.* George J. Stigler, *An Introduction to Privacy in Economics and Politics*, 9 J. LEGAL STUD. 623, 626 (1980) (observing that "[t]he failure of contracts to emerge which specify that the creditor may not sell the consumer credit information is in the interest of debtors, for whom credit would otherwise be more expensive"); Rubin E. Cruse, Jr., Note, *Invasions of Privacy and Computer Matching Programs: A Different Perspective*, 11 COMPUTER/L.J. 461, 472-75 (1992) (discussing verification function of computer-matching programs as means of detecting "malfeasant" images, which permits people to have more faith in the truthfulness of information, thus facilitating human relations).

Some commentators have argued that many of the untoward repercussions that follow from the dissemination of true information are themselves possibly unjustified. They flow, so it is suggested, from misassessments of the information's present relevance, or from too-pessimistic judgments about what the information signifies with respect to its subject. *See, e.g.*, Frank H. Easterbrook, *Privacy and the Optimal Extent of Disclosure under the Freedom of Information Act*, 9 J. LEGAL STUD. 775, 787-96 (1980) (outlining economic argument supporting refusal to disclose embarrassing personal details). Others have argued that with respect to certain intimate choices, especially those that are constitutionally protected, the case for informational privacy is at its strongest. *See, e.g.*, Kreimer, *supra* note 14, at 131-43.

[55] For two particularly comprehensive discussions of the ways in which computer technology not only exacerbates but changes the nature of the privacy problem in the activist state, see Paul Schwartz, *Data Processing and Government Administration: The Failure of the American Legal Response to the Computer*, 43 HASTINGS L.J. 1321 (1992), and Spiros Simitis, *Reviewing Privacy in an Information Society*, 135 U. PA. L.

how, without the aid of computers, an active government possibly could have digested all the information for which it has developed such an insatiable appetite. Be that as it may, three capabilities of the new technology simultaneously enhance the government's ability to collect and add value to information, exerting particular influence on the dimensions of the privacy problem.

Before describing these phenomena, however, it is perhaps useful to be reminded that information is a very desirable thing to have. Knowledge is power—so goes the cliché; and as one wag noted, "the only way that three people in Washington can keep a secret is if two of them are dead." As a practical matter, information was difficult to protect from unwanted disclosure even before the advent of computers. Information cannot be protected from unauthorized use or disclosure by the simple expedient of putting or keeping it in a secure physical location. Because it is intangible, information is easy to "steal." Thefts also often go undetected, because victims do not end up with less of anything tangible after the theft than they had before, and thus they do not "miss" whatever information was taken. Information has always had this characteristic.[56] Computer technology only exacerbated it.[57]

One way that the new technology has exacerbated the difficulty of protecting information stems from the enormous—indeed the exponential—increase in computer processing and storage capacity that recent years have witnessed. The federal government has not been slow to exploit this increased capacity for purposes of more efficiently administering its own programs. The government presently "utilizes the world's largest collection of computers,"[58] and spends more than seventeen billion dollars per year on information technology.[59] This vastly increased computer storage and processing capacity almost inevitably means that whatever *kinds* of misuses or abuses of personal information take place, their *numbers* are likely to increase.[60]

REV. 707 (1987).

[56] Edmund W. Kitch, *The Law and Economics of Rights in Valuable Information*, 9 J. LEGAL STUD. 683, 690-91 (1980).

[57] *See* Ann W. Branscomb, *Rogue Computer Programs and Computer Rogues: Tailoring the Punishment to Fit the Crime*, 16 RUTGERS COMPUTER & TECH. L.J. 1, 1-4 (1990); Brenda Nelson, Note, *Straining the Capacity of the Law: The Idea of Computer Crime in the Age of the Computer Worm*, 11 COMPUTER/L.J. 299, 316-19 (1991).

[58] Schwartz, *supra* note 55, at 1333.

[59] *Id.* at 1334.

[60] John A. McLaughlin, Comment, *Intrusions Upon Informational Seclusion in the Computer Age*, 17 J. MARSHALL L. REV. 831, 836 (1984) (suggesting that before the digital computer was introduced, "[p]ersonal information was difficult to secure and compile, making large quantities of information concerning one individual unavailable. Computer technology, however, has made these protections part of a lost era.") (foot-

A second important aspect of the new technology is what one commentator aptly describes as its capacity for "multifunctionality."[61] Once personal information is transformed into binary codes, "the computer can efficiently compare it and combine it with other digital data. The computer changes personal information into a fluid form, which allows it to be applied at many stages of administrative decisionmaking."[62] Multifunctionality permits such practices as *computer matching*, the electronic comparison of two or more sets of records to find individuals included in more than one database;[63] *computer assisted front-end verification*, which electronically accesses already existing databases in order to certify accuracy and completeness of personal information given at the time of an actual application for government benefits;[64] and *computer profiling*, which searches for specified elements or combinations of elements in a number of different record systems.[65]

Multifunctionality has obvious benefits. Computer matching helps detect and prevent fraud and improves management. Front-end verification helps in debt collection,[66] and assists in guaranteeing eligibility of benefit applicants before, rather than after, benefit payments begin, thus protecting program integrity. Profiling assists law enforcement agents to identify possible tax evaders and drug couriers.

Nevertheless, multifunctionality has potential shortcomings. Computer matches may produce excessive numbers of false positives—too many of their "hits" may turn out to be misses for the exercise to be worthwhile.[67] Profiling may tempt government officials to go on "fishing expeditions" rather than targeting their investigations to people reasonably suspected of crime.[68] Likewise, profiling might serve as a cover for racially motivated or otherwise illegitimately biased enforcement decisions.[69] On a more ephemeral but perhaps equally disturbing note, one commentator has noted the "se-

---

note omitted).

[61] Schwartz, *supra* note 55, at 1339.

[62] *Id.*

[63] *See* Regan, *supra* note 33, at 630.

[64] *Id.* at 632.

[65] *Id.*

[66] The Debt Collection Act of 1982, Pub. L. No. 97-365, 96 Stat. 1749 (codified as amended in scattered sections of U.S.C.), for example, requires applicants for federal loans to supply their Social Security numbers, and requires agencies to screen credit applicants against IRS files to check for tax delinquency.

[67] *See infra* note 71 and accompanying text.

[68] *See* SENATE REPORT ON THE COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988, S. REP. NO. 516, 100th Cong., 2d Sess. 7 (1988).

[69] *See* Kenneth J. Langan, Note, *Computer Matching Programs: A Threat to Privacy?*, 15 COLUM. J.L. & SOC. PROBS. 143, 147 (1979).

ductive precision" of the answers given by computers;[70] another has warned of the consequences of the "loss of context" that automated processing creates: "The very moment the matching begins, the data are itemized and disconnected from their original collection situation. Yet neither hard facts nor judgments can be separated at will from their context without distorting the information. Consequently, every step toward routinized processing accentuates the danger of misrepresentations and false conclusions."[71] The trick for information managers and privacy policymakers is to devise strategies that enable government to maximize the efficiencies that multifunctionality makes possible while minimizing the harm it might cause.

The third noteworthy aspect of the new technology is that it permits decentralization of government control of information. The ability to store information on discs permits widespread sharing of data in computer form. Minicomputers, as ubiquitous in government offices as in the private sector, permit individual users to gain access to centralized records, and allow individual users to create their own databases. That computer records systems can be directly linked via telecommunications systems not only accounts for a substantial increase in the exchange of information within government and among agencies, but also greatly increases the number of people having access to that information.[72] The decentralization that the new technology permits magnifies the already substantial difficulty of maintaining confidentiality of information within government, and throws a roadblock in the way of monitoring employee compliance with rules intended to guard the confidentiality of personal information.

II.

The legal landscape with respect to the use and disclosure of information about individuals in government's hands is dominated, though not quite controlled, by three generic statutes. First, there is the Privacy Act of 1974;[73] second, there is the Computer Matching and Privacy Protection Act of 1988 (the Computer Matching Act),[74] which is part of the Privacy Act; and third, the Freedom of Information Act (FOIA),[75] which occupies a prominent place in the federal statutory terrain. I shall discuss each of these major legislative initiatives in turn, hoping to illustrate the issues in the control of *government* that efforts to protect the privacy of personal information present.

---

[70] Schwartz, *supra* note 55, at 1341.

[71] Simitis, *supra* note 55, at 718.

[72] *See* Regan, *supra* note 33, at 629; Schwartz, *supra* note 55, at 1334.

[73] 5 U.S.C. § 552a (1994).

[74] 5 U.S.C. § 552a(o) (1994).

[75] 5 U.S.C. § 552 (1994).

In addition, specific statutory provisions impose particularized nondisclosure obligations on certain agencies, including the Internal Revenue Service[76] and the Census Bureau.[77] Except to note their existence, this Article shall not discuss these statutes. Such a project would be well worth undertaking, but to attempt to cast light on the operation of particular species of privacy protection would require a depth of inquiry into the bureaucratic culture of specific agencies that would carry this Article beyond its intended scope.

Before proceeding to the statutory analysis, it is useful to make the following important point: Once individuals have disclosed information about themselves to the government, unconsented-to use or disclosure of that information by the government can take place in two paradigmatically different contexts. The first is use by or disclosure to another agency within government, for the purpose of preserving the integrity of government benefit programs, or of aiding law enforcement, or of collecting debts. The second context in which unconsented-to use or disclosure of information supplied to government can take place is disclosure outside the government, pursuant, for example, to a FOIA request from a non-governmental entity. Although the distinction is seldom explicitly recognized, nor is its analytical importance often acknowledged in the literature, the two contexts tend to implicate different privacy concerns as well as to generate different interests in disclosure.

Consider first the use or disclosure of information by the agency to whom it is given to another agency within government. Although such unconsented-to disclosure might result in adverse consequences to the individual—the termination of government benefits, for example, or the levy of additional tax liability—it is not likely to result in the kind of personal embarrassment that would follow from disclosure of intimate or embarrassing

---

[76] *See, e.g.*, I.R.C. § 6103 (1988 & Supp. V 1993) (making tax returns and return information confidential and not subject to disclosure unless authorized by Congress); I.R.C. § 7431 (1988) (creating a civil remedy for unauthorized disclosures). For a review of the legal issues surrounding unauthorized disclosures of tax return information, see Allan Karnes & Roger Lively, *Striking Back at the IRS: Using Internal Revenue Code Provisions to Redress Unauthorized Disclosures of Tax Returns or Return Information*, 23 SETON HALL L. REV. 924 (1993).

[77] *See, e.g.*, 13 U.S.C. §§ 8-9 (1994) (providing for the confidentiality of census data). These sections have been strictly enforced against the government. *See, e.g.*, McNichols v. Klutznick, 644 F.2d 844, 846 (10th Cir. 1981) (holding that cities may not discover raw census data in suits to challenge representative apportionment by population based on those data), *aff'd sub nom.* Baldridge v. Shapiro, 455 U.S. 345 (1982). For a brief discussion praising the Census Bureau's protection of confidentiality, and linking that protection to the public's willingness to participate in the census, see Harry A. Scarr, *Privacy Protection and Data Dissemination at the Census Bureau*, 11 GOV'T INFO. Q. 249 (1994).

facts about oneself to one's neighbors or friends.

In order to put the "privacy as control over unconsented-to use" issue in the context of information-sharing within government into stark relief, assume that the information being shared is relevant to the purpose of both agencies; that the sharing is done not by rogue employees acting on a whim, but rather pursuant to officially endorsed agency policy; that the information is timely and true; that either the disclosing or the receiving agency could legitimately require the individual to whom the information pertains to supply it before taking action either to benefit or to disadvantage her; and that the individual would have neither a Fourth nor a Fifth Amendment right to refuse to disclose the information to either agency. On this set of assumptions, the "privacy interest" with regard to the information would seem to recede into virtual inconsequence, if not to disappear altogether. The respective agencies' substantive power of control over the facet of life to which the information pertains, and their concomitant entitlement to demand that the information be supplied, would quite dwarf an individual's claim of a residual right to "control the information" itself and to limit its use or disclosure to the particular purpose for which it was disclosed. The point here is not that the individual would have "waived" her privacy interest by the initial disclosure for a particular purpose to a particular agency. Rather, the point is that vis-à-vis the government generally, and its demands that citizens supply it with personal information in connection with its regulatory, welfare, revenue-raising, or crime-fighting agenda, an individual has very little in the way of a "privacy interest" to be waived. Moreover, on the specified set of assumptions, the public interest in disclosure by one agency to another would also appear to be quite high, because it is a function of the information's relevance and contribution to the receiving agency's substantive agenda.

Now turn to the second context in which unconsented-to use or disclosure of information supplied to the government takes place: namely, the context in which the government reveals the information to outsiders. A familiar example of this is disclosure of information pursuant to a FOIA request. In this context, it would be quite inappropriate to make the set of assumptions that expose the weakness of the "privacy as control of information" claim where the disclosure is from one government agency to another. The principal reason is that, unlike a government agency with whom information germane to its purposes is shared by the agency to whom it was initially given, a private requester has no colorable legal entitlement to the information apart from that conferred upon her by FOIA.[78] However worthy her motives, moreover, and however widely beneficial the uses to which she intends to put the information, a private requester cannot claim to be

[78] *See* United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 780 (1989).

doing the public's business in the same sense that a governmental agency can. Notably, disclosure of personal information to a private requester carries a much greater potential to embarrass, to annoy, or to subject the individual to harassment and intrusions on her seclusion than does intra- or inter-governmental disclosure. In other words, disclosure of personal information in government's hands to outsiders is far less likely to serve a legislatively-endorsed public interest, and far more likely to invade a substantial privacy interest, than is sharing the same information within the government.

Regarding disclosure of information in government's hands, the law reflects the significant differences between the privacy and the disclosure interests implicated by unconsented-to use or disclosure of information by the government to other governmental agencies and to private requesters.[79] As will be described in more detail below, the Privacy Act and the Computer Matching Act, for example, place relatively few substantive barriers in the way of inter- or intra-governmental sharing of personal information, thus illustrating both the relative weakness of the privacy interest and the relative strength of the interest in disclosure in the context of information shared by the government with other government agencies. FOIA, on the other hand, exempts information whose disclosure would invade personal privacy from the otherwise pervasive obligation upon agencies to disclose their records.[80] Moreover, as FOIA has come to be interpreted by the Supreme Court, where privacy interests would be threatened by disclosure, the statute mandates disclosure of only that information which serves *FOIA's* legislatively

---

[79] In his provocative essay, Seth Kreimer speaks of two ways in which the "expansion of government knowledge translates into an increase in the effective power of government." Kreimer, *supra* note 14, at 5. The first, and more mundane, arises from the sharing of computerized personal information among government agencies, which permits government to enforce existing laws more efficiently. *Id.* The second, quite different kind of increase arises from what Kreimer implies is a consciously deployed governmental strategy to use the volume of information controlled by it "to sanction disfavored activities by the simple act of public disclosure." *Id.* at 6. Kreimer's essay focuses on the latter. It describes the conflict between "exposure" ("sunlight") of information in government's hands as a punishment, a deterrent, and a component of informed democratic decisionmaking, and "secrecy" of such information as necessary to the protection of "sanctuaries of private liberty from state intervention." *Id.* at 7. Little, if anything, in either the text or the legislative history of FOIA would support the conclusion that FOIA embodies the self-conscious enlisting by government of the power of disclosure to punish or deter disfavored private activities. Instead, the Act is exclusively concerned with disclosure to citizens of what "*their government* is up to." *Reporters Comm.*, 489 U.S. at 773 (emphasis added). Nevertheless, the important point is that disclosure to the public, represented by a FOIA requester, of personal information in the hands of government both implicates different privacy interests and serves generically different public purposes than does disclosure of the same information to another government agency.

[80] 5 U.S.C. § 552(b)(6) (1994).

endorsed "central purpose" of contributing significantly to public understanding of the operations of the government.[81] Thus FOIA's exemptions, and the Court's interpretation of the disclosure interest against which they are to be weighed, mirror both the relative strength of the privacy interest and the relative narrowness of the disclosure interest in the context of sharing information with outsiders.

A. The Privacy Act

The Privacy Act of 1974[82] establishes general requirements for the management of personal records by agencies of the executive branch of the federal government. It gives citizens the right to learn how agencies collect, maintain, use, and disseminate personal information.[83] It grants individuals rights of access to personal information maintained about them, and permits them to seek amendment of any incorrect or incomplete information.[84] In fact, the Privacy Act might be considered an "enactment" of the Code of Fair Information Practices. At least insofar as the practices of agencies of the federal government are concerned, the Privacy Act purports to address all the major concerns of privacy advocates.

By requiring federal agencies to give a variety of notices, both to individuals and to the public, the Privacy Act addresses the concern that there be no secret system of records. At the point of data collection, for example, an agency must inform individuals of its authority to request the information, of the purposes for which the information is to be used, of the routine uses which may be made of the information, and of the effects on the individual of not supplying it.[85] When agencies establish or revise a system of records, they must publish a notice in the Federal Register to that effect, including specific information about the system.[86] This required disclosure of the very existence of record systems has been termed "one of the demonstrable, continuing benefits of the Privacy Act in controlling surveillance."[87]

The Privacy Act addresses the concern that individuals be able to find out what personal information about them is in the file and how it is being used by granting individuals the right to review this information in a government agency's "system of records."[88] It also requires agencies to keep

---

[81] *Reporters Comm.*, 489 U.S. at 773-77.
[82] 5 U.S.C. § 552a (1994).
[83] *Id.* § 552a(e)(3)-(4).
[84] *Id.* § 552a(d)(1)-(2).
[85] *Id.* § 552a(e)(3).
[86] *Id.* § 552a(e)(4).
[87] FLAHERTY, *supra* note 28, at 321.
[88] 5 U.S.C. § 552a(d)(1).

accounts of disclosures of records[89] and to make such accounts available to individuals named in the records.[90] The concern that individuals be given a way to correct or amend records of identifiable information about themselves is met by granting them the right to challenge the content of such records for accuracy, completeness, relevance, and timeliness.[91]

The Privacy Act also addresses the concern that individuals be able to prevent information obtained for one purpose from being used or made available for other purposes without their consent. In a provision said to be "the heart of the Privacy Act"[92] despite its being subject to a number of significant exceptions,[93] the Act prohibits disclosure of personal information by an agency without the subject's consent.[94] Finally, the Act addresses the concern for reliability and the need to prevent misuse (due to poor quality) of personal data by imposing a number of quality-control obligations on agencies. For example, agencies must maintain only information that is relevant and necessary to accomplish a purpose of the agency;[95] when possible, agencies must collect information directly from the subject individual;[96] they must maintain records "with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual";[97] and they must make reasonable efforts to assure, prior to releasing any records, that they are "accurate, complete, timely, and relevant."[98]

The Act addresses—or purports to address—the concern that the government will unjustifiably disclose personal information or put information gathered for one purpose to a different use, to the (presumably unjustified) disadvantage of the individual. Subject to a number of specific, and important, exceptions,[99] it prohibits disclosure of personal information by an agency without the subject's consent[100] and requires agencies to keep accurate accountings of the disclosures that are made.[101]

The unfortunate reality, however, is that the Privacy Act is a paper tiger. For two principal reasons, the Act has failed to achieve its objectives. One reason is that the Act's substantive provisions are riddled with loopholes

---

[89] *Id.* § 552a(c)(4).
[90] *Id.*
[91] *Id.* § 552a(d)(2).
[92] BERMAN & GOLDMAN, *supra* note 24, at 12.
[93] The exceptions are listed in 5 U.S.C. § 552a(b)(1)-(12).
[94] 5 U.S.C. § 552a(b).
[95] *Id.* § 552a(e)(1).
[96] *Id.* § 552a(e)(2).
[97] *Id.* § 552a(e)(5).
[98] *Id.* § 552a(e)(6).
[99] *Id.* § 552a(b)(1)-(12).
[100] *Id.* § 552a(b).
[101] *Id.* § 552a(c).

and laced with exceptions. The second is that the "individual rights" enforcement model upon which the Act is based is, in several important respects, inadequate to the task.

The "individual rights" enforcement model translates into a heavy—indeed, an excessive and surely unrealistic—enforcement burden upon individuals:

> The Privacy Act requires that individuals be aware of their rights, understand the potential threats posed by agency collection and use of such information, and be willing to invest the time and money necessary to protect their interests. These requirements place a burden on the individual. Every time an individual comes in contact with a bureaucracy seeking personal information, he or she must question the purposes for which information is sought and the necessity of each item of information.
>
> To ensure that information is not misused, the individual must follow up to make sure that no new information is added to the file, and that the uses and disclosures of information are in keeping with the agency's stated purposes. If individuals find that files contain inaccurate or irrelevant information, or that information is used for improper purposes, then they need to know what legal remedies are available and take action against the agency. Such a procedure means that individuals need to be conscious of their rights at every stage of the information-handling process. Most people are so accustomed to disclosing information that they rarely think through all of the possible consequences. In addition, the time, and secondarily, the money, necessary to monitor the status of one's personal information and to take legal action are prohibitive for the average individual.[102]

---

[102] Regan, *supra* note 33, at 633; *see also* Rotenberg, *supra* note 10, at 87 (regarding putting the burden on individuals for identifying improper data collection practices and making corrections in personal records, "[w]hen information is shared across the Federal government or between public and private organizations, it becomes increasingly difficult to identify problems and resolve complaints"); Schwartz, *supra* note 55, at 1380 (noting that "if the 'laymen' in Congress are unable to understand data processing systems within government bureaucracy, the ordinary citizen has no hope of comprehension. Data subjects are unlikely to have the resources and technical expertise to understand the arrangement of information processing, the employment of their personal data, and the extent of their rights."); Donsia R. Strong, Note, *The Computer Matching and Privacy Protection Act of 1988: Necessary Relief from the Erosion of the Privacy Act of 1974*, 2 SOFTWARE L.J. 391, 413 n.135 (1988) (observing that "individuals do not litigate potential claims because the data may have been transferred without a given

In addition to the inordinate general difficulties with which the Act confronts individual enforcers, the Act creates some specific obstacles to vigorous individual enforcement. For example, notices about the existence and revision of records appear in the Federal Register,[103] which is not easily accessible to individuals. Indeed, it has rightly been described as an "arcane . . . source of information for the general public."[104] Moreover, the remedies provided in the Act do not suggest that Congress intended to encourage aggressive individual enforcement. The Act gives federal courts limited authority. The courts can issue injunctions "in only two instances: to amend (i.e., correct) the individual's record, 5 U.S.C. § 552a(g)(2)(A), and to order an agency to produce agency records improperly withheld from an individual, 5 U.S.C. § 552a(g)(3)(A)."[105] In other words, an individual cannot by injunction stop an agency from violating the Act in the future,[106] with the result that the government "may keep its practices unaltered and litigate the occasional claim."[107] Nor does the fact that individuals will "litigate the occasional claim" represent a formidable threat to the government. The Act permits individuals to recover damages only if a violation has an "adverse effect" on them,[108] only if the court finds that the agency acted "in a manner which was intentional or willful,"[109] and only in the amount of "actual damages" sustained.[110]

More importantly, the Privacy Act is a paper tiger because loopholes in, and exceptions to, its substantive provisions significantly reduce its effective scope.[111] For example, agency heads may by rule exempt some systems of records from compliance with the access and disclosure provisions of the Act, including those maintained by the CIA, the Secret Service, and other law enforcement agencies; those maintained for statistical purposes; and those compiled in the course of determining eligibility for various federal

---

individual's knowledge and they may not know of the injury; the chances of succeeding are slim; their financial resources may be limited; and/or the size of the agency may be intimidating").

[103] 5 U.S.C. § 552a(e)(4).

[104] FLAHERTY, *supra* note 28, at 321.

[105] Edison v. Department of the Army, 672 F.2d 840, 846 (11th Cir. 1982).

[106] *Hearings*, *supra* note 23, at 240 (testimony of Ronald Plesser, former general counsel, Privacy Protection Study Commission).

[107] Schwartz, *supra* note 55, at 1379 n.283.

[108] 5 U.S.C. § 552a(g)(1)(D) (1994).

[109] *Id.* § 552a(g)(4).

[110] *Id.* § 552a(g)(4)(A). Some courts hold that "actual damages" include damages for physical and mental injury. *See* Johnson v. Department of Treasury, 700 F.2d 971, 986 (5th Cir. 1983). Other courts hold that "actual damages" limits plaintiffs to recovery of pecuniary losses. *See* Fitzpatrick v. IRS, 665 F.2d 327, 331 (11th Cir. 1982).

[111] *See generally* PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 515-26 (1977) (discussing use limitation and information management principles) [hereinafter STUDY COMMISSION REPORT].

positions.[112] Furthermore, although the Act defines "record" as "any item, collection, or grouping of information about an individual that is maintained by an agency,"[113] and thus could potentially cover "every record that contains any kind of information associated with that individual,"[114] the Act's definition actually only *applies* to a record that is retrieved from a "system of records" by the "name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual."[115] Thus, the Act does not in fact restrict disclosures of every "record" that contains any kind of individually identifiable information. None of the Act's protections accrue to an individual whose records are not accessed by name, identifying number, symbol, or other identifying particular. Accordingly, "many records containing sensitive personal information"[116] are effectively beyond the Act's protection, an observation whose accuracy several courts have confirmed.[117]

The most worrisome loophole, however, is the Act's allowance of all disclosures for a "routine use,"[118] which the Act defines as a "purpose which is *compatible* with the purpose for which [the information] was collected."[119] The Act itself does not prescribe a standard of compatibility, and each agency head is accordingly the "ultimate arbiter of what it means" insofar as her own agency's practices are concerned.[120] The Privacy Protection Study Commission discovered after the Act had been in force for

---

[112] 5 U.S.C. § 552a(k).

[113] *Id.* § 552a(a)(4).

[114] Hosch, *supra* note 17, at 149.

[115] 5 U.S.C. § 552a(a)(5).

[116] Hosch, *supra* note 17, at 149.

[117] *See, e.g.*, Chapman v. NASA, 682 F.2d 526, 529-30 (5th Cir. 1982) (holding that notes taken by a supervisor in evaluating employees for job assignments or promotion are not "systems of records" because they were kept in the personal files of the supervisor and never integrated into any system of records); American Fed'n of Gov't Employees v. NASA, 482 F. Supp. 281, 282-83 (S.D. Tex. 1980) (holding that sign-in/sign-out sheets for federal employees are not a "system of records" because they do not contain specific, personal information); Jackson v. Veterans Admin., 503 F. Supp. 653, 655-56 (N.D. Ill. 1980) (holding that information communicated in a phone call is not a "system of records" because it is not retrievable by means of a personal identifier); Smiertka v. United States Dep't of Treasury, 447 F. Supp. 221, 228 (D.D.C. 1978) (holding that information pertaining to the requester need not be disclosed unless the information is retrievable by means of the requester's own name or other personal identifier, and "[t]hat it can be easily retrieved in some other way by some other identifier is wholly beside the point").

[118] 5 U.S.C. § 552a(b)(3). For a thorough discussion of the "routine use" exception, see Todd R. Coles, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957 (1991).

[119] 5 U.S.C. § 552a(a)(7) (emphasis added).

[120] *See* FLAHERTY, *supra* note 28, at 323.

only two years that, while some agencies interpreted "routine use" narrowly, others interpreted it very broadly, permitting such practices as disclosure to another agency "'to the extent that the information relates to the requesting agency's decision on the matter.'"[121] The *President's 1982-83 Annual Report on the Agencies' Implementation of the Privacy Act* concluded:

> even a casual examination of agencies' routine uses suggests that agencies interpret the concept of compatibility to permit uses that are neither functionally or programmatically related to the original collection purpose. In some cases this is due to requirements imposed by statute . . . . In other cases, it is due to a deliberate interpretation on the part of the agency that a particular disclosure would be "necessary and proper" to the operation of a governmental program. This interpretation looks more to the literal definition of compatibility—capable of existing together without discord or disharmony.[122]

OMB guidelines issued in 1982, before the Computer Matching Act was enacted, deemed computer matching a "routine use."[123] Furthermore, the OMB seemed to encourage and promote data sharing among federal agencies,[124] rather than constraining sharing according to what might have been thought to be the spirit of the Privacy Act,[125] by inviting agencies to "seek to satisfy new information needs through legally authorized interagency or intergovernmental sharing of information."[126]

Accordingly, it may well be the case that the observer who asserted at the Privacy Act Oversight Hearings in 1983 that "[i]f someone looks at the Privacy Act and thinks that it does, in fact, limit disclosure, I think that

---

[121] STUDY COMMISSION REPORT, *supra* note 111, at 517 (quoting 41 Fed. Reg. 40,015 (1976)).

[122] Management of Federal Information Resources, 50 Fed. Reg. 52,730, 52,751 (1985); *see also* FLAHERTY, supra note 28, at 323

[123] Privacy Act of 1974; Revised Supplemental Guidance for Conducting Matching Programs, 47 Fed. Reg. 21,656, 21,657 (1982).

[124] Management of Federal Information Resources, 50 Fed. Reg. at 52,751.

[125] *Cf.* BERMAN & GOLDMAN, *supra* note 24, at 14 ("Congress' [sic] original intent in enacting the Privacy Act was thwarted by the government's interpretation of the 'routine use' exemption . . . .").

[126] *Id.*

person is sorely mistaken"[127] painted a more accurate picture of the reality of the Act's bite than would emerge from simply parsing its text. In fact:

> Because no external agent actually audits or really questions the information-handling practices of federal agencies [and because each agency accordingly has almost complete autonomy to interpret the Act according to its own understanding], it is impossible to know how the Privacy Act's standards are being applied in practice, although considerable skepticism has been expressed over the years.[128]

Finally, until relatively recently at least, the Privacy Act's commitment to nondisclosure was in apparent tension with, and in some cases expressly trumped by, the Freedom of Information Act's commitment to disclosure. Among the several exceptions to the Privacy Act's prohibition on agency disclosure of personal information to third parties is an express exemption for disclosure that is "required under section 552 of this title"[129]—that is, for disclosures required by FOIA. FOIA in turn requires that agencies provide the public with access to federal agency records, and that "any person" making an appropriate request be given access to inspect and copy such records.[130] FOIA is based on the proposition that, just as information about citizens and their activities is the handmaiden of the modern activist state, information about government is the handmaiden of democracy.[131] Moreover, under FOIA, once characterized by an astute commentator as "an extraordinary piece of antiprivacy legislation,"[132] disclosure is mandatory

---

[127] *Hearings*, *supra* note 23, at 224 (testimony of Ronald Plesser, former general counsel, Privacy Protection Study Commission).

[128] FLAHERTY, *supra* note 28, at 322.

[129] 5 U.S.C. § 552a(b)(2) (1994).

[130] 5 U.S.C. § 552(a)(2) (1994).

[131] James Madison is everyone's favorite authority for the wisdom of the Act's underlying purposes:

> A popular Government, without popular information, or the means of acquiring it, is but a Prologue to a Farce or a Tragedy; or, perhaps both. Knowledge will forever govern ignorance: And a people who mean to be their own Governors, must arm themselves with the power which knowledge gives.

Letter from James Madison to W.T. Barry (Aug. 4, 1822), *in* 9 THE WRITINGS OF JAMES MADISON 103, 103 (Gaillard Hunt ed. 1910).

Not everyone agrees that making information about government more readily available ought to be as high a priority as the Act makes it, *see, e.g.*, Antonin Scalia, *The Freedom of Information Act Has No Clothes*, REGULATION, Mar.-Apr. 1982, at 14, or even that it serves democracy particularly well, *see, e.g.*, Frank H. Easterbrook, *The State of Madison's Vision of the State: A Public Choice Perspective*, 107 HARV. L. REV. 1328, 1343 (1994).

[132] Easterbrook, *supra* note 54, at 776.

unless one of nine exceptions permitting, but not requiring, nondisclosure applies.[133] This Article now turns to a more detailed examination of the intersection between FOIA's disclosure mandates and the protection of personal privacy.

B. The Freedom of Information Act

By its own terms, FOIA does not require agencies to be completely oblivious to privacy concerns. "To the extent required to prevent a clearly unwarranted invasion of personal privacy," FOIA permits an agency to "delete identifying details" when it publishes opinions, policy statements, and the like, so long as the agency complies with the mandate that "the justification for the deletion shall be explained fully in writing."[134]

FOIA's most important privacy protections, however, are contained in two of the nine exemptions, which explicitly permit agencies to resist disclosure when necessary to protect the privacy of individuals. Subsection (b)(6) exempts from mandatory disclosure "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy,"[135] and (b)(7) exempts records or information compiled for law enforcement purposes to the extent that the production of such records "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[136]

In recent years, the Supreme Court has interpreted these provisions so as to enhance agencies' ability to invoke them as shields to repel requests that records containing personally identifiable information about individuals be released.[137] Before turning to these cases, however, it is important to recognize that FOIA's other provisions, its basic structure, and the bureaucratic incentives it creates generate considerable tension between the government's obligation to protect citizens' privacy on the one hand and its obligation to conduct its business openly so as to be accountable to its citizens on the other.

In this regard, consider first the Act's overall design and the incentives of the bureaucrats subject to its provision. The Act's formal provisions are heavily tilted toward disclosure. Whereas the exemptions are permissive,[138] disclosure is mandatory—all documents not specifically exempted *must* be

---

[133] 5 U.S.C. § 552(b)(1A)-(9).

[134] *Id.* § 552(a)(2)(C); *see also id.* § 552(b) (providing that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt").

[135] *Id.* § 552(b)(6).

[136] *Id.* § 552(b)(7).

[137] *See infra* text accompanying notes 160-206.

[138] Chrysler Corp. v. Brown, 441 U.S. 281, 293-94 (1979).

disclosed.[139] The Act provides sanctions against officials who improperly withhold information,[140] but not on those who improperly release information.[141] Judicial review of agency decisions to withhold is also "stacked by the statute in favor of disclosure."[142] The Act places the burden on a withholding agency to justify nondisclosure,[143] and permits prevailing plaintiff-requesters to be awarded attorney's fees.[144] More important perhaps is that the individuals about whom the information is sought—namely, those persons with the greatest, indeed the only personal, stake in confidentiality—seem rarely to be parties to litigation over the privacy exemptions.[145] Those individuals must depend on government officials—whose personal and professional agendas are likely to differ quite markedly from the individuals' own—to identify, articulate, and vigorously defend their privacy interests.[146] "Sometimes the government's interests will overlap those of the person whose privacy is at stake; more often they will not."[147] In addi-

---

[139] 5 U.S.C. § 552(a) ("Each agency *shall* make available to the public . . . .") (emphasis added); *see also* Department of the Air Force v. Rose, 425 U.S. 352, 371-75 (1976) (discussing Congressional intent behind Exemption 6).

[140] 5 U.S.C. § 552(a)(4)(F)-(G).

[141] Compare, for example, the sanctions that apply when government officials violate the Privacy Act. *See supra* text accompanying notes 105-10.

[142] Easterbrook, *supra* note 54, at 797.

[143] 5 U.S.C. § 552(a)(4)(B).

[144] *Id.* § 552(a)(4)(E).

[145] ALLAN R. ADLER, LITIGATION UNDER THE FEDERAL OPEN GOVERNMENT LAWS 139 (1992) (noting that "[c]ases in which data subjects seek to enjoin its release under the FOIA are quite rare").

[146] *Cf.* Lawrence A. Silver, *Reverse Freedom of Information Act Litigation in a Non-Commercial Setting: The Case of Professor Doe*, 31 CLEV. ST. L. REV. 455, 474 (1982) ("It is troubling that . . . the rights . . . of a person threatened with a possible invasion of privacy should only have the protection offered by a litigant with interests quite divergent from his own."); Heather Harrison, Note, *Protecting Personal Information From Unauthorized Government Disclosures*, 22 MEM. ST. U. L. REV. 775, 790 (1992) (suggesting that individuals are "forced to rely on the government to protect their privacy interests with the very real possibility that the government may choose not to withhold the information if no governmental interest is jeopardized").

[147] Easterbrook, *supra* note 54, at 800. Occasionally these real parties in interest manage to make their voices heard during the litigation. *See, e.g.*, New York Times Co. v. NASA, 920 F.2d 1002, 1009 (D.C. Cir. 1990) (In the course of remanding to the district court for a determination of whether disclosure of the tape of the voice communication from the doomed Challenger Space Shuttle would constitute a clearly unwarranted invasion of personal privacy, the D.C. Circuit held the tape to be information that "applies to an individual" and thus a "similar file" within Exemption 6, and noted that the "families of the astronauts attempted to explain *in camera* the basis for their privacy claims."); *cf.* Madsen, *supra* note 42, at 112-13. In discussing agency incentives with respect to the invocation of FOIA Exemption 4, which protects trade secrets and confidential commercial or financial information from mandatory disclosure, Madsen

tion, although the deadlines are often honored in the breach, the Act requires those officials to decide quickly whether to act to protect privacy; they must determine whether to comply with any FOIA request "within ten days" of its receipt.[148]

Just as is the case with respect to agency implementation of the Privacy Act, generalization about how FOIA is actually administered is exceptionally risky. Like the Privacy Act, FOIA applies to *all* federal agencies, each one of which is pursuing its own distinct substantive mission and generating its own unique bureaucratic culture.[149] Similarly,

> [a]dministering the Act is in many ways a discretionary task that continues to present two challenges largely ignored by statutory and case law, directives and regulations, and personnel practices despite a 20-year history. The first emanates from the nature of information as a product; the second from defining the position of "access professional."[150]

With respect to the first challenge, many records must be examined on a case-by-case basis, and much turns on the "position, background, and training"[151] of the administrator making the decision of whether to disclose. With regard to the second challenge, there is still no uniform job description, set of qualifications, or consistently identifiable career path for the "access professionals" who make most of the government's FOIA decisions. "Inevitably and frequently, people with such differing backgrounds and

---

noted:

> Several factors . . . may lead administrators to invoke the fourth exemption sparingly. First, agency personnel sometimes elect to disclose confidential business information despite the exemption, believing that the public interest in disclosure outweighs potential harm to submitter interests. In addition, agencies typically gain little by invoking the exemption and may not wish to assume the burden and risk of litigation with the requester solely to protect the submitter's interests. Moreover, it is often not apparent that the exemption applies to particular information. The statutory language is opaque, and the judicial tests evolved for applying it require a knowledge of the submitter's circumstances that few administrators will possess. When coupled with the prodisclosure pressures of the FOIA and the tremendous number of FOIA requests some agencies must process, these difficulties of interpretation make inadvertent disclosures especially likely.

Id. (footnotes omitted).

[148] 5 U.S.C. § 552(a)(6)(A)(i).

[149] On the importance of agency culture to the way in which legislative directives are actually implemented, see JAMES Q. WILSON, BUREAUCRACY: WHAT GOVERNMENT AGENCIES DO AND WHY THEY DO IT 14-28 (1989).

[150] Lotte E. Feinberg, *Managing the Freedom of Information Act and Federal Information Policy*, 46 PUB. ADMIN. REV. 615, 617 (1986).

[151] *Id.*

professional training disagree over whether certain documents should be released."[152] Nevertheless, with respect to the privacy/access tension, if bureaucratic incentives are systematically skewed, it seems a fair bet that the skew is in exactly the opposite direction from that which the "public interest" would seem to require. On the one hand, bureaucrats would seem to have little natural inclination to honor the "public's right to know" with regard to the bureaucrats' actions, especially if to do so might render them vulnerable to being charged with misfeasance or just plain poor judgment.[153] On the other hand, the bureaucrats themselves will not suffer personal embarrassment or other untoward personal consequences if information entrusted to their agency is wrongfully used or disclosed. When the government's own interest overlaps with individuals' privacy interests, it would seem as likely as not that it is the agency's assessment of how best to advance its own interest, at least as much as its genuine and consistently dependable commitment to protecting privacy, that explains the agency's decision to claim the exemption. The point here is not that bureaucrats never invoke the privacy provisions, or that when they do so they never act in good faith. Rather, the point is simply that protecting privacy is likely to be a matter of secondary priority, at best a side-constraint, in the bureaucrats' own conception of where their duties lie and how they ought to do their jobs.[154]

In addition to the basic tilt away from aggressive privacy protection created by the formal provisions and basic structure of FOIA, the fact seems to be that the bureaucratic deck is stacked to tilt in a similar direction. In setting its agenda and determining whether to invoke the privacy exemption, each agency can be expected to give privacy protection a back seat to its own primary enforcement mission. And there are likely to be few, if any, internal "bureaucratic rewards for attempting to give privacy a higher visibility."[155]

---

[152] *Id.*

[153] For a helpful brief recounting of the history of the Act, tracing its history from "a long tradition of departmental control of information," through the Administrative Procedure Act of 1946 and its weak and vague provisions granting public access to certain administrative materials, to the "revolutionary" Freedom of Information Act of 1966 and its "broad norm of disclosure and access with relatively narrow exceptions," see Glen O. Robinson, *Access to Government Information: The American Experience*, 14 FED. L. REV. 35, 35-41 (1983).

[154] As one privacy advocate asserted: "When privacy requirements conflict with other Federal agency goals, there is little guarantee that individual rights will prevail." Rotenberg, *supra* note 10, at 87; *see also* Trubow, *supra* note 28, at 542 (noting that "[a] concern for privacy is the natural enemy of a government bureaucrat who pursues agency objectives with costs and efficiency in mind").

[155] Robert M. Gellman, *Fragmented, Incomplete, and Discontinuous: The Failure of Federal Privacy Regulatory Proposals and Institutions*, 6 SOFTWARE L.J. 199, 238

The tension between the government's obligation to protect personal information it collects from disclosure and its FOIA-imposed obligation to conduct its business openly was for several years exacerbated by judicial interpretations that rendered a coherent account of FOIA's privacy exemptions impossible.[156] Courts failed to articulate a consistent conception of the nature and extent of the privacy values that FOIA's nondisclosure provisions were intended to advance or to announce criteria for determining when invasions of privacy would be clearly or plainly unwarranted. Beginning in 1982, with its unanimous decision in *United States Department of State v. Washington Post Co.*,[157] the Supreme Court began the process of clarifying the purpose and legal effect of FOIA's privacy exemptions. It did this by more clearly specifying the nature of the "personal privacy" interests that the Act was intended to protect and by articulating a rather narrow "public interest in disclosure" against which the privacy interest was to be balanced.[158] The clarification came none too soon: as early as 1981, federal agencies were overwhelmed by FOIA requests and most of the requests came from persons who were not the Act's obviously intended beneficiaries, and who wanted the information for purposes seemingly quite different from those the Act had been intended to serve.[159]

In *Washington Post*, the Court resolved a question that had divided the lower courts for several years. The case concerned the meaning of FOIA Exemption 6, which permits the withholding of "personnel and medical files and *similar files* the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[160] The issue that *Washington Post* resolved was how to interpret the phrase "similar files." A number of courts, including the D.C. Circuit in the case below,[161] had interpreted the language to apply only to those records which contain "information of the same magnitude—as highly personal or as intimate in nature—as that at

---

(1993).

[156] For a useful description and analysis of the law as it was in 1980, see Anthony T. Kronman, *The Privacy Exemption to the Freedom of Information Act*, 9 J. LEGAL STUD. 727 (1980).

[157] 456 U.S. 595 (1982).

[158] *Id.* at 599-602. For a useful account of the cases, see Fred H. Cate et al., *The Right to Privacy and the Public's Right to Know: The "Central Purpose" of the Freedom of Information Act*, 46 ADMIN. L. REV. 41 (1994).

[159] Cate et al., *supra* note 158, at 43 (finding that by 1981, the "vast majority of the FOIA requests were made by business executives or their lawyers who . . . 'astutely discerned the business value of the information which government obtains from industry while performing its licensing, inspecting, regulating, and contracting functions'") (footnote omitted).

[160] *Washington Post*, 456 U.S. at 595 (quoting 5 U.S.C. § 552(b)(6) (1994)) (emphasis added).

[161] Washington Post v. United States Dep't of State, 647 F.2d 197 (D.C. Cir. 1981), *rev'd*, 456 U.S. 595 (1982).

stake in personnel and medical records."[162] Under this reading, the information sought by the *Washington Post*—information indicating whether certain Iranian nationals held valid U.S. passports—was subject to mandatory disclosure because it was "less intimate than information normally contained in personnel and medical files."[163]

The Supreme Court rejected this reading of the statute. It held that Congress did not intend to limit Exemption 6 to "a narrow class of files containing only a discrete kind of personal information. Rather, '[t]he exemption [was] intended to cover detailed Government records on an individual which can be identified as applying to that individual.'"[164] Of course, Exemption 6 does not permit nondisclosure of all individually identifiable information, only that information the release of which would constitute a "clearly unwarranted invasion" of a particular individual's personal privacy.

Exemption 7(C), which permits nondisclosure of records compiled for law enforcement purposes, is similarly limited to situations in which production "could reasonably be expected to constitute an unwarranted invasion of personal privacy."[165] Thus, important issues remained to be resolved after *Washington Post*, namely, what kinds of privacy interests did FOIA's privacy exemptions intend to protect from what kinds of invasions, and by what criteria was an invasion to be judged "unwarranted."

The Court went far toward answering each of these questions in *United States Department of Justice v. Reporters Committee for Freedom of the Press*,[166] another unanimous decision and by far the Court's most important pronouncement on the subject of FOIA's privacy exemptions. At issue in *Reporters Committee* was whether disclosure of FBI "rap sheets" "could reasonably be expected to constitute an unwarranted invasion of personal privacy"[167] and thus be withheld pursuant to Exemption 7(C).[168] The re-

---

[162] *Id.* at 198-99 (citing Simpson v. Vance, 648 F.2d 10, 13-14 (1980) and Board of Trade v. Commodity Futures Trading Comm'n, 627 F.2d 392, 398 (D.C. Cir. 1980)) (internal punctuation omitted).

[163] *Washington Post*, 456 U.S. at 598.

[164] Id. at 602 (quoting H.R. REP. NO. 1497, 89th Cong., 2d Sess. 11 (1966) *reprinted in* 1966 U.S.C.C.A.N. 2418, 2428) (alteration in original).

[165] United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 749-50 (1989).

[166] 489 U.S. 749 (1989).

[167] *Id.* at 749-50.

[168] Note that Exemption 7(C) is broader in permitting nondisclosure than Exemption 6, because 7(C) does not require the invasion of personal privacy to be "clearly" unwarranted, and it permits nondisclosure not if disclosure *would* constitute a privacy invasion, but merely if it "could reasonably be expected to" do so. *Compare* 5 U.S.C. § 552(b)(6) *with id.* § 552(b)(7). Nevertheless, the particular 7(C) issues that the Court addressed in *Reporters Committee*—the nature of the privacy interest and the nature of the interests that would warrant invading it—are identical to the issues that an Exemption 6 case would present.

questers argued that the events summarized in rap sheets had previously been disclosed to the public, and that information contained in the sheets was thus already publicly available, albeit in scattered and hard-to-obtain form.[169] Accordingly, they claimed, the subjects' privacy interest in avoiding disclosure of the facts contained in the rap sheets' compilation "approache[d] zero."[170]

In rejecting this argument, Justice Stevens made two important points about the nature of the privacy interests that FOIA protected. First, information may be classified as "private" even if, though it has once been disclosed, it is "'not freely available to the public.'"[171] Rap sheets, representing "the compilation of otherwise hard-to-obtain information,"[172] contain information that is not "freely available." "Plainly there is a vast difference between the public records that might be found after a diligent search of courthouse files, county archives, and local police stations throughout the country and a computerized summary located in a single clearinghouse of information."[173] Moreover, in various provisions of the United States Code, including those of FOIA itself, the Court discerned a "careful and limited pattern of authorized rap sheet disclosure,"[174] which indicated that the sheets were restricted "'to the use of a particular person or group or class of persons.'"[175] In phrases certain to appeal to advocates who evince particular concern about the privacy threat that computers pose, the Court recognized "the power of compilations to affect personal privacy that outstrips the combined power of the bits of information contained within."[176] The Court even found congressional support in the Privacy Act for its conclusion that "a strong privacy interest inheres in the nondisclosure of compiled computerized information."[177]

The second important point in Justice Stevens's rejection of the requesters' argument that the subjects' privacy interest in nondisclosure of their rap sheets "approache[d] zero"[178] came by way of the explicit recognition that there is a "privacy interest in keeping personal facts away from the public eye."[179] Justice Stevens endorsed by implication the government's self-imposed obligation, if not its constitutional duty, to avoid

---

[169] *Reporters Comm.*, 489 U.S. at 764.

[170] *Id.* at 763.

[171] *Id.* at 763-64 (quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1804 (1976)).

[172] *Id.* at 764.

[173] *Id.*

[174] *Id.* at 765.

[175] *Id.* (quoting WEBSTER'S THIRD NEW INTERNATIONAL DICTIONARY 1804 (1976)).

[176] *Id.*

[177] *Id.* at 766.

[178] *Id.* at 763.

[179] *Id.* at 769.

public disclosure of information it has collected "which is personal in character and potentially embarrassing or harmful if disclosed."[180]

Having thus established that subjects of FBI rap sheets had a substantial privacy interest in the information contained therein, Justice Stevens turned to the question of whether the invasion of privacy that rap sheet disclosure entails would be *warranted.* Resolution of this question, Justice Stevens announced, could not properly be made to turn on either the purpose for which the request for information was made or on the identity of the requester.[181] Instead, in passages significant for the extent to which they tended to reduce the areas of inevitable tension between the goals of the Privacy Act and FOIA's commands, and for narrowly limiting FOIA's disclosure mandates to those that serve the Act's "central purpose," Justice Stevens held that "whether disclosure of a private document . . . is warranted must turn on the nature of the requested document and its relationship to the basic purpose of the Freedom of Information Act to open agency action to the light of public scrutiny."[182] That basic purpose is served by disclosure of "[o]fficial information that sheds light on an agency's performance of its statutory duties,"[183] but not "by disclosure of information about private citizens that is accumulated in various governmental files . . . that reveals little or nothing about an agency's own conduct."[184] Put somewhat differently, "the FOIA's central purpose is to ensure that the *Government's* activities be opened to the sharp eye of public scrutiny, not that information about *private citizens* that happens to be in the warehouse of the Government be so disclosed."[185]

Finally, the Court turned its attention to the ultimate decision that was required by FOIA to be made with respect to all the exemptions: whether the public interest in disclosure outweighed "the interest Congress intended the Exemption to protect."[186] In language that seemed to expand the reach of its holding well beyond the specific facts of the case before it, the Court held

---

[180] *Id.* at 770 (quoting Whalen v. Roe, 429 U.S. 589, 609 (1977)).

[181] *Id.* at 771-72.

[182] *Id.* at 772 (quoting Department of Air Force v. Rose, 425 U.S. 352, 372 (1975)) (internal quotation omitted).

[183] *Id.* at 773.

[184] *Id.*

[185] *Id.* at 774. For commentary critical of the Court's "central purpose" test, see Eric J. Sinrod, *Blocking Access to Government Information under the New Personal Privacy Rule*, 24 SETON HALL L. REV. 214 (1993); Glen Dickinson, Note, *The Supreme Court's Narrow Reading of the Public Interest Served by the Freedom of Information Act*, 59 U. CIN. L. REV. 191 (1990).

[186] *Reporters Comm.*, 489 U.S. at 776.

> as a categorical matter that a third party's request for law enforcement records or information about a private citizen can reasonably be expected to invade that citizen's privacy, and that when the request seeks no "official information" about a Government agency, but merely records information that the Government happens to be storing, the invasion of privacy is "unwarranted."[187]

In *United States Department of State v. Ray*,[188] the Court returned to FOIA Exemption 6. The issue was whether Exemption 6 permitted deletion of the names of individual Haitian refugees from reports, disclosed pursuant to a FOIA request, of interviews by State Department personnel of persons who had been involuntarily returned from the United States to Haiti.[189] Both the requesters and the government acknowledged that the reports were "similar files" within the meaning of Exemption 6, as interpreted by *Washington Post*: they "unquestionably appl[ied] to . . . particular individuals."[190] Therefore, resolution of the case turned on whether disclosure would constitute a "clearly unwarranted invasion"[191] of those individuals' privacy. The Court held that it would.

First, the reports implicated a significant privacy interest because they contained personal details, because disclosure of individual names might lead to possible retaliation against the repatriated Haitians, and because interviews had been conducted pursuant to promises of confidentiality.[192] Significantly, the Court thought it was not merely the disclosure of the list and of identifying information that represented a threat to privacy. Instead,

> whether disclosure of a list of names is a "significant or a *de minimis* threat depends upon the characteristic(s) revealed by virtue of being on the particular list, and the consequences likely to ensue." . . . [D]isclosure of the interviewees' names would be a significant invasion of their privacy because it would subject them to possible embarrassment and retaliatory action.[193]

---

[187] *Id.* at 780.

[188] 502 U.S. 164 (1991).

[189] *Id.* at 166.

[190] *Id.* at 173.

[191] *Id.* at 166.

[192] *Id.* at 165, 170, 176-77.

[193] *Id.* at 176 n.12 (quoting National Ass'n of Retired Fed. Employees v. Horner, 879 F.2d. 873, 877 (D.C. Cir. 1989), *cert. denied*, 494 U.S. 1078 (1990)) (internal quotation marks removed).

The second reason that the invasion of privacy occasioned by disclosure of the interviewees' names would be "clearly unwarranted" was that it would not shed any light on the "[g]overnment's conduct of its obligation," and thus would not serve FOIA's purpose of informing citizens as to the actions of their government.[194]

The Court refused in *Ray* to address the question of whether other derivative public benefits that disclosure might generate would ever justify disclosure of information where disclosure would invade significant privacy interests without serving FOIA's core purpose. Nevertheless, in *United States Department of Defense v. Federal Labor Relations Authority (FLRA)*,[195] Justice Thomas's opinion for a unanimous Court[196] squarely held that "the *only* relevant 'public interest in disclosure' to be weighed in this balance is the extent to which disclosure would serve the 'core purpose of the FOIA,' which is 'contribut[ing] significantly to public understanding *of the operations or activities of the government.*'"[197] The case thus solidified *Reporters Committee*'s interpretation of FOIA as containing a "core purpose" limitation on agencies' statutory obligation to disclose information claimed to be exempt from disclosure,[198] and rendered implausible the prospect of any future claim that derivative uses of disclosed information would prove weighty enough to compel disclosure.

In addition to closing off the "derivative use" avenue, the Court in *FLRA* resolved certain lingering tensions between the Privacy Act's prohibitions on disclosure and FOIA's disclosure mandates. In *FLRA*, the requesters were the collective bargaining representatives of federal employees under the Federal Service Labor Management Relations Statute (Labor Statute).[199] They sought disclosure of the home addresses of federal civil service employees.[200] The Court began its analysis of the disclosure issue with the Labor Statute, which required the release of home addresses to bargaining representatives unless the disclosure would be "prohibited by law."[201] The Court's next analytical step was to hold that the employee address records were "records" whose disclosure was *prohibited* by the

---

[194] *Id.* at 178.

[195] 114 S. Ct. 1006 (1994).

[196] Justices Souter and Ginsburg concurred in the judgment. *Id.* at 1017 (Souter, J., concurring in judgment); *id.* (Ginsburg, J., concurring in judgment).

[197] *Id.* at 1012 (quoting United States Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 775 (1989)) (first emphasis added) (alteration in original).

[198] *Id.* at 1012.

[199] *Id.* at 1009.

[200] *Id.* at 1008.

[201] *Id.* at 1011 (quoting 5 U.S.C. § 7114(b)(4)(B) (1988 & Supp. IV 1992)) (emphasis removed).

Privacy Act unless it was *required* by FOIA.[202] Finally, the Court held that disclosure was not required by FOIA because it "would constitute a clearly unwarranted invasion of personal privacy."[203] While disclosure indeed might vindicate the policies behind the Labor Statute,[204] it would not further the only interest relevant for FOIA purposes, namely, "'the citizens' right to be informed about what their government is up to.'"[205] Because the Court found that the public interest in disclosure was practically nil, it required only a "very slight" privacy interest to outweigh it, and the employees' "nontrivial" privacy interest "in avoiding the influx of union-related mail, and, perhaps, union-related telephone calls or visits" was easily found to be sufficiently weighty.[206]

This line of Supreme Court decisions has dissolved some of the genuine uncertainties about how to reconcile the formal commands of the Privacy Act and FOIA. Nevertheless, the decisions, though welcome, will not necessarily have a significant impact on actual bureaucratic practice—and there's the rub. While providing agency lawyers with legal ammunition and a coherent rationale with which to defend their privacy-based refusals to disclose, and heightening their sometimes languishing awareness of the Privacy Act and privacy values, the decisions do not by any means guarantee a future dependable congruence between bureaucrats' conflicting incentives: to guard other people's privacy, or to save themselves the trouble and make it easier to achieve their own agency's agenda. Nor do the cases make up for the otherwise ineffectual enforcement provisions of the Privacy Act. Nor, finally, do the cases even change the legal reality that, when the information sought to be released by a FOIA request is not covered by the Privacy Act, its nondisclosure is permissive, not mandatory—even if disclosure would constitute a "clearly unwarranted invasion of personal privacy."[207] Because many agencies already have taken evasive action with respect to getting their records out from under the Privacy Act's coverage,[208] this standard would seem to provide a major loophole. Thus, when all is said and done, clarifying the meaning of FOIA's privacy exemptions may have been necessary to resolve the tension between privacy and access with respect to dis-

---

[202] *Id.* at 1012.

[203] *Id.*

[204] For criticism of *FLRA* on grounds that it unduly undermined the congressionally-endorsed policy in favor of collective bargaining implicit in the Labor Statute, see Michael M. Lowe, *The Freedom of Information Act in 1993-1994*, 43 DUKE L.J. 1282, 1294-1307 (1994).

[205] *FLRA*, 114 S. Ct. at 1013-14 (quoting Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 773 (1988)).

[206] *Id.* at 1015.

[207] United States Dep't of State v. Ray, 502 U.S. 164, 166 (1991) (quoting 5 U.S.C. § 552(b)(6) (1994)).

[208] *See* STUDY COMMISSION REPORT, *supra* note 111, at 518-21.

closure to FOIA requesters of personally identifiable information, but it was hardly sufficient.

C. The Computer Matching and Privacy Protection Act of 1988

In 1977, the then Department of Health, Education and Welfare (HEW) instituted a program called "Project Match," subtitled "A Nationwide Program to Expose Employees on the Federal Payroll Who Are Illegally Receiving AFDC (Aid to Families with Dependent Children) Payments."[209] Justified as so many subsequent matching programs have been as a tool for preventing fraud, waste, and abuse in the administration of government benefit programs, Project Match compared state welfare rolls with lists of federal employees in order to determine whether individuals who were drawing government benefits were in fact eligible to receive them.[210] Project Match was controversial both as a matter of policy and law. To answer the legal objections, HEW prepared a formal defense of the program, particularly in terms of the project's conformity with the Privacy Act.[211] Little dispute arose about the technical merits of HEW's legal arguments. Still, as one observer noted, the very fact that the Privacy Act was not an obstacle to Project Match served as just "another reminder that the Act, for all of its merits, does not affect substantive policy decisions about the uses of personal data, only the procedures to be followed once those uses are determined."[212] Another prominent privacy advocate made an even stronger claim about computer matching's compatibility with the underlying premises of the Privacy Act:

> Computer matching directly challenges congressional findings about the need to protect personal privacy set forth in section 2(a) of the Privacy Act, and the spirit, if not the letter, of computer matching is directly contrary to the intentions and aspirations of Congress set forth in the legislative history of the Privacy Act. The need for privacy safeguards holds true today with respect to the practice of computer matching.[213]

---

[209] Langan, *supra* note 69, at 144.

[210] *Id.* at 144, 148-50.

[211] *Id.* at 148-50.

[212] *Id.* at 150 (citing PROJECT ON PRIVACY AND DATA COLLECTION, AMERICAN CIVIL LIBERTIES UNION FOUNDATION, THE PRIVACY REPORT 7 (1978)).

[213] FLAHERTY, *supra* note 28, at 346.

The stated goal of Project Match itself was limited to detecting whether federal government employees were receiving AFDC benefits,[214] but Project Match was merely the first of many matching programs. Indeed, in the late seventies and early eighties, extravagant claims abounded about the efficiencies that this "spectacularly effective technique"[215] could achieve: "AFDC data was soon being matched against Social Security Administration earning records, Federal civilian and military payroll data; Veterans Administration records were being matched against supplemental security income (SSI) files and each state's AFDC data was being matched with other states."[216] Matching can be and has been used to detect "unreported income, unreported assets, duplicate benefits, incorrect social security numbers, overpayments, incongruous entitlements (SSI checks mailed to deceased individuals, mothers claiming more children than exist), present addresses of individuals (Parent Locator Service, Student Loan Defaulters), and providers billing twice for the same service."[217] Today, according to a recent GAO study, most computer matches are done for debt collection purposes or to determine eligibility for government benefits.[218]

Prior to the Computer Matching Act, most of the data exchanges for the matching programs described above were justified by government officials under the "routine use"[219] exception to the Privacy Act, which allows disclosure of data "for a purpose which is compatible with the purpose for which it was collected."[220] Whatever doubts might have existed about the integrity of the rationale, "[c]ompatibility appear[ed] to be a broad enough standard to encompass any use which [was] not contrary to the original purpose; thus using the information to uncover welfare cheats among the ranks of service personnel could be labeled routine."[221]

Not all the computer matching that took place was at the agencies' initiative; between 1976 and 1986, Congress passed a number of statutes either encouraging the exchange of information or specifically authorizing comput-

---

[214] Langan, *supra* note 69, at 144.

[215] OFFICE OF TECHNOLOGY ASSESSMENT, FEDERAL GOVERNMENT INFORMATION TECHNOLOGY: ELECTRONIC RECORD SYSTEMS AND INDIVIDUAL PRIVACY 50 (1986) [hereinafter OTA, ELECTRONIC RECORD SYSTEMS] (quoting OMB Deputy Director Joseph Wright).

[216] MADSEN, *supra* note 43, at 111.

[217] OTA, ELECTRONIC RECORD SYSTEMS, *supra* note 215, at 39.

[218] GENERAL ACCOUNTING OFFICE, COMPUTER MATCHING: QUALITY OF DECISIONS AND SUPPORTING ANALYSES LITTLE AFFECTED BY 1988 ACT 10 (1993) [hereinafter GAO, COMPUTER MATCHING].

[219] 5 U.S.C. § 552a(b)(3) (1994).

[220] *Id.* § 552a(a)(7).

[221] Langan, *supra* note 69, at 149.

er matches.[222] Thus, as noted by the Office of Technology Assessment in 1986, "congressional actions appear[ed] to be contradictory."[223]

A general consensus began to emerge that even though few, if any, matching programs were in technical non-compliance with either the Privacy Act or other statutory provisions, Congress had neither addressed nor resolved the basic policy conflict that widespread use of computer matching had created between the efficient management of government programs and the rights of individuals with respect to intra- or inter-governmental disclosure of personal information. The individual rights guaranteed by the Privacy Act—to notice, access, and correction of records; to information that is timely, relevant, and complete; and the prevention of information being used without consent—seemed to be compromised by matching programs even if they were in technical compliance. The Executive Branch had not filled the policy breach by providing either meaningful guidelines for, or effective oversight of, matching programs.[224] Skepticism existed in some quarters

---

[222] Statutes implicitly authorizing computer matching are summarized in OTA, ELECTRONIC RECORD SYSTEMS, *supra* note 215, at 44-46. They include the Paperwork Reduction Act of 1980, Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended in scattered sections of 20 U.S.C., 44 U.S.C.); the Federal Managers Financial Integrity Act of 1982, 31 U.S.C. §§ 1105-1106, 1108, 1113, 3512 (1988); the Debt Collection Act of 1982, Pub. L. No. 97-365, 96 Stat. 1749 (codified as amended in scattered sections of 5 U.S.C., 18 U.S.C., 26 U.S.C., 28 U.S.C., 31 U.S.C.); and the Deficit Reduction Act of 1984 (DEFRA), Pub. L. No. 98-369, 98 Stat. 494 (codified as amended in scattered sections of U.S.C.). Statutes explicitly authorizing matching are listed in OTA, ELECTRONIC RECORD SYSTEMS, *supra* note 215, at 46. They include the Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520 (codified as amended in scattered sections of U.S.C.); the Social Security Amendments of 1977, Pub. L. No. 95-216, 91 Stat. 1509 (codified as amended in scattered sections of 2 U.S.C., 26 U.S.C., 33 U.S.C., 42 U.S.C.); the Food Stamp Act Amendments of 1980, Pub. L. No. 96-249, 94 Stat. 357 (codified as amended in scattered sections of 7 U.S.C., 26 U.S.C., 42 U.S.C.); the Food Stamp and Commodity Distribution Amendments of 1981, 7 U.S.C. §§ 2012, 2014-2016, 2018-2020, 2023-2027, 2029, 2270 (1994); the Department of Defense Authorization Act of 1983, Pub. L. No. 97-252, 96 Stat. 718 (codified as amended in scattered sections of 10 U.S.C., 22 U.S.C., 38 U.S.C.); and the Deficit Reduction Act of 1984 (DEFRA), Pub. L. No. 98-369, 98 Stat. 494 (codified as amended in scattered sections of U.S.C.).

[223] OTA, ELECTRONIC RECORD SYSTEMS, *supra* note 215, at 43.

[224] *See* Gellman, *supra* note 155, at 224-25 (summarizing OMB oversight of matching activity in the late 1970s and asserting that the Computer Matching Act "was passed in part because of dissatisfaction with OMB's guidance and oversight"). David Flaherty quotes the House Report on the Matching Act to the effect that "[g]uidance issued by OMB has been largely ignored by agencies and unenforced by OMB. There is no meaningful oversight of computer matching in the Executive Branch." FLAHERTY, *supra* note 28, at 357 (quoting HOUSE COMM. ON GOVERNMENT OPERATIONS, COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1988, H.R. REP. NO. 802, 100th Cong., 2d Sess. 11 (1988), *reprinted in* 1988 U.S.C.C.A.N. 3107, 3117).

about whether, in fact, the benefits of all the matching programs outweighed their costs.[225] Furthermore, there appeared to be reason for concern about the accuracy of the data produced by the matches, and, in particular, about the due process rights of individuals against whom adverse action might be taken on the basis of erroneous "hits."[226]

In response to these concerns, Congress passed the Computer Matching and Privacy Protection Act of 1988,[227] which became effective on January 1, 1990. The Act does not address the most important substantive question of what criteria ought to govern the decision to implement a particular matching program. Also, the Act applies only to the computerized comparison of records for the purpose of establishing or verifying eligibility for federal benefit programs, or recouping payments or delinquent debts under such programs.[228] The Act, however, creates procedural and administrative barriers to the execution of future matching programs. The barriers are designed, for example, to force agencies to consider the costs and benefits of matches before undertaking them,[229] and to assure that adverse action will not be taken against individuals unless the data adverse to them is independently verified and they are given an opportunity to contest the data.[230]

The Act requires that agencies engaging in computer matching must do so pursuant to written matching agreements that state such things as the purpose and legal authority for the match, the justification for the matching program, its anticipated results, a description of the records to be matched, procedures for notice to applicants, in addition to procedures for verification, retaining, destroying, and ensuring the physical safety of records.[231] The Act further requires agencies that engage in computer matching programs to establish Data Integrity Boards to oversee matching activities, to review and approve matching agreements, to conduct cost-benefit analyses, and to make annual reports on matching activities.[232] The Data Integrity Boards do not perform a "broad privacy policy role,"[233] and the Computer Matching Act itself creates neither an enforcement mechanism nor a timeta-

---

[225] SENATE COMM. ON GOVERNMENTAL AFFAIRS, THE COMPUTER MATCHING AND PRIVACY PROTECTION ACT OF 1987, S. REP. NO. 516, 100th Cong., 2d Sess. 14-15 (1988).

[226] *Id.* at 7. A "hit" is "[i]nformation on one or more data elements in two or more automated files that appear to be identical or similar (name, Social Security number, address, date of birth, and the like)." GAO, COMPUTER MATCHING, *supra* note 218, at 59.

[227] 5 U.S.C. § 552a(o) (1994).

[228] *Id.* § 552a(a)(8)(i)(I)-(II).

[229] *Id.* § 552a(u)(4)(A).

[230] *Id.* § 552a(p)(A)(i), (B).

[231] *Id.* § 552a(o)(A)-(G).

[232] *Id.* § 552a(u)(1), (3)(A)-(D).

[233] Gellman, *supra* note 155, at 225.

ble for compliance with its requirements. The Act's emphasis on "due process and administrative goals" has been praised as reflecting "a shrewd political assessment of how best to persuade Congress to act."[234]

The title of the most comprehensive study of the Computer Matching Act's operation to date, a GAO report to a subcommittee of the House Committee on Government Operations, indicates the extent of the Act's effect. Entitled *Computer Matching: Quality of Decisions and Supporting Analyses Little Affected by 1988 Act*,[235] the GAO report concluded that literal compliance with the Act's mandates had not significantly enhanced the quality of agency decisionmaking with reference to whether particular matching programs should be undertaken.[236] Pursuant to the Act, agencies had made some changes in their planning and in the procedures they followed when they implemented computer matches, yet "despite these changes, agencies generally were not providing full and earnest reviews of proposed matches."[237] Moreover, OMB at that time had not yet issued the required guidelines and regulations "for the use of agencies in implementing" the Act's provisions.[238] In other words, far from solving the question of how to control substantively the way government officials use personal information disclosed to them, the Computer Matching and Privacy Protection Act seems merely to have changed only the nature of the procedural hoops through which bureaucrats must jump. Accordingly, the Act cannot be said to represent a genuine institutional solution to the issue of data sharing within the government.

D. A Federal Data Protection Board?

In terms of privacy as control over information, the substantive question to ask about all forms of data sharing within the federal government is the one so cogently expressed by prominent privacy activist David Flaherty: "whether a person's privacy is in fact invaded in any meaningful way if his or her record in a federal information system is simply checked along with millions of others for compliance with a particular requirement."[239] Unfortunately, Flaherty himself does not genuinely attempt to grapple with the question. Instead, he invokes the mantra-like claim of privacy advocates—the "standard fair information practice is that an invasion of privacy certainly occurs if the data were not collected from individuals with such a

---

[234] FLAHERTY, *supra* note 28, at 357.

[235] *See* GAO, COMPUTER MATCHING, *supra* note 218.

[236] *See id.* at 3, 20.

[237] *Id.* at 3.

[238] Such guidelines were required by 5 U.S.C. § 552a(v)(1) (1994).

[239] FLAHERTY, *supra* note 28, at 352.

purpose in mind."[240] This claim both begs the question and rests on a shaky normative foundation.[241] Finally, as Flaherty himself acknowledges throughout his book, the "standard fair information practice" that he describes is rarely implemented in the actual conduct of the federal government's business.[242]

Indeed, the characterization of federal privacy protection as "fragmented, discontinuous, and incomplete" is apt; and though not all commentators use such terms, they do tend to gravitate to the same solution—the creation of a "permanent [f]ederal agency"[243] vested with "overall responsibility of safeguarding informational privacy with respect to federal records."[244] "Of the four major privacy studies identified in the last twenty years, three recommended the establishment"[245] of such a permanent agency, and almost all of the countries in the European Community have them in some form or other.[246]

The recommendation that the United States get on the bandwagon is grounded principally in commentators' dissatisfaction with the Executive Branch's, and especially the OMB's, weak leadership on privacy issues,[247] and in the commentators' recognition of the limitations of the Privacy Act and the Computer Matching Act.[248] A Privacy Protection Board could cure some of these problems, so commentators claim, by bringing more visibility to the issue of personal information collection and use, by providing a single locus for identifying privacy problems and resolving complaints, by placing limitations on agency collection of information, and by overseeing the quality of data in government record systems.[249] "When privacy requirements conflict with other agency goals, there is little guarantee that individual rights will prevail *absent oversight from an independent board.*"[250] The assumptions buried in this statement that must be addressed are, first, that *with*

---

[240] *Id.* at 352-53.

[241] *See supra* text accompanying notes 49-54.

[242] *See generally* FLAHERTY, *supra* note 28.

[243] Robert M. Gellman, *An American Privacy Protection Commission: An Idea Whose Time Has Come . . . Again*, 11 GOV. INFO. Q. 245, 245 (1994).

[244] Trubow, *supra* note 28, at 530.

[245] Gellman, *supra* note 155, at 236.

[246] For a recent, thorough account of other countries' policies, see generally FLAHERTY, *supra* note 28.

[247] *Cf.* Gary Bass & David Plocher, *Strengthening Federal Information Policy: Opportunities and Realities at OMB*, 3 SOFTWARE L.J. 413, 430 (1989) ("Privacy . . . has been turned inside out by OMB's shortsighted interest in easing restrictions on government use of information about individuals.").

[248] *See, e.g.*, BERMAN & GOLDMAN, *supra* note 24.

[249] Regan, *supra* note 33, at 633.

[250] Rotenberg, *supra* note 10, at 86-87 (emphasis added).

oversight from an independent board, individual rights will prevail and, second and more importantly, that individual rights *should* prevail.

For several reasons, it seems quite unlikely that in the foreseeable future Congress will create such an independent board or, even if one is created, that Congress will empower it effectively to override the data management policies of other government agencies, especially with respect to exchange of data within the government. Define "informational privacy" as the substantive right to prevent unconsented-to use or disclosure of information. Scrutinize the provisions of the privacy legislation that Congress has already passed. Recognize that *in fact* Congress never has substantively valued informational privacy, and certainly has not valued it more than or even as much as government efficiency. The Privacy Act is well-nigh unenforceable, the Computer Matching Act is both substantively toothless and severely compromised by the several statutes that expressly authorize matching, and FOIA would probably still be "an extraordinary piece of anti-privacy legislation"[251] had the Supreme Court not stepped in to fill the privacy breach. In the face of Congress's historically weak commitment to personal privacy, legislative proposals for establishing a Privacy Protection Board have always had to swim upstream. Not surprisingly, such proposals have always failed, and their present prospects seem no brighter.

Public angst about how much personal information is contained in government files, about how it is handled, and with whom in government it is shared has never translated into effective political support for a powerful institutional remedy. Apart from isolated horror stories, oft-invoked accounts of the vastly increased *potential* for privacy invasions that computers' enhanced storage and processing capacity signify, alarming (because they contain such big numbers) statistics referring to the immense quantities of information in government files, and considerable evidence of rampant government use of personally identifiable information for different purposes than for which it was obtained, there exists surprisingly little hard evidence of systematic *abuse* by government of personal information. When specific privacy problems become salient, specific, rather than generic, solutions are enacted.[252] Despite the fact that these specific pieces of legislation tend to represent the exercise by Congress of its own responsibility for actually

---

[251] Easterbrook, *supra* note 54, at 776.

[252] *See, e.g.*, the Video Privacy Protection Act, 18 U.S.C. § 2710 (1994) (passed in 1988 in response to disclosure by media of movies rented by Supreme Court nominee Robert Bork, the Act restricts access to consumer video cassette rental and sales information); Right to Financial Privacy Act, 12 U.S.C. §§ 3401-3422 (1994) (passed in 1978 in response to United States v. Miller, 425 U.S. 435 (1975), which sustained the constitutionality of subpoena of records of deposits and checks kept by a bank pursuant to requirements of the Bank Secrecy Act, the Act establishes procedures for disclosure of bank records to the government, and gives the depositor rights to notice and challenge).

addressing the policy problems of what tradeoffs between privacy and other values ought to be made, privacy advocates tend to discount these "secular" approaches.[253] They seem to be convinced that only a "central agency" can adequately protect privacy across-the-board, and that an across-the-board solution is both appropriate and feasible.[254] In the current deregulatory climate, however, political capital seems unlikely to be available for the creation of another layer of bureaucracy, even one with such a benign and seemingly uncontroversial mission as that of protecting informational privacy.

Nevertheless, assume for the moment that creation of a Privacy Protection Board, with broad power to monitor and control other agencies' data collection and protection policies, were to become politically realistic. Then the assumptions that underlie the arguments in favor of such a board would have to be examined, and one would have to ask whether creation of such a board would be a wise, much less a genuine, solution to an actual problem. An attitude of complacent indifference to privacy concerns is not what would warrant skepticism about such proposals. Rather, skepticism seems a wholly appropriate response when one takes a hard look at the character of the privacy issue itself, and at the intractable nature of the tension between efficiently achieving the goals of an activist state and genuinely protecting individuals from unconsented-to disclosures of information about themselves.

In the first place, no single federal agency could in reality make, much less effectively enforce, federal privacy policy. Widespread endorsement of generally-phrased Fair Information Practices hides the important reality that there neither is nor ever really could be *one* privacy policy, at least not one of sufficient determinacy to be of actual use in resolving actual controversies. The right to control the use and dissemination of information about oneself is not absolute; most privacy advocates recognize this fact,[255] despite their frequent unqualified invocations of the right.

Accordingly, the proper resolution of each privacy issue—the appropriate answer to each question of whether a particular unconsented-to use ought to be permitted—is highly context-specific. Proper resolution depends on a multitude of variables including the purpose for which use or disclosure is desired and the efficiency gains its use would generate; the extent to which non-disclosure would permit the data subject to misrepresent herself to the recipient agency; the purposes for which the information was original-

---

[253] *See, e.g.*, Gellman, *supra* note 155, at 236.

[254] *Cf.* Rotenberg, *supra* note 10, at 86-87.

[255] *See, e.g.*, Paul M. Schwartz, *The Protection of Privacy in Health Care Reform*, 48 VAND. L. REV. 295, 333-34 (1995) ("[A]ny assignment of rights to individuals must be limited in scope. The law should not create an absolute right of control or a quasi-property interest in one's personal data . . . . because of the variety of critical social interests that can support access to any individual's personal data.").

ly collected; the kind of information at issue (whether of a highly personal, intimate, or embarrassing nature); the subjective or objectively reasonable expectations of the data subject with respect to its subsequent use; and the unjustified adverse consequences that might befall the individual if the information is used for a different purpose. In other words, not only does the strength of the individual privacy interest vary with the context, but so does the importance of the government interests that stand in opposition to it. Moreover, it is not easy to develop methods for *valuing* the competing interests when the government has acquired the information at issue in a more or less coercive context instead of in furtherance of a voluntary exchange, and when the subjects of the information are not themselves parties to the inter- or intra-governmental sharing. In the private sector, because businesses can gain by satisfying their customers' preferences for privacy, and thus have incentives to do so, markets can develop to measure both the demand for privacy on the one hand, and the value of data sharing on the other. This is not to say that the private sector is presently as responsive to customers' privacy desires as its customers would like;[256] rather, it is to note that in the private sector genuine incentives exist to do so because market participants can appropriate the gains from getting the "privacy vs. disclosure" calculation right. When information is in the government's hands, no such incentives exist because government officials cannot internalize the gains from satisfying citizens' demands for privacy. Accordingly, the possibility that government actors will make the right trade-offs is far more remote.

One inevitable consequence of context-dependency and of the pervasive indeterminacy of the relative values of privacy and sharing is that reasonable people will differ about whether the proper balance has been struck in each case, and whether privacy policy has been implemented too much or too little. By reason of the fact that both context-dependency and value indeterminacy are endemic to privacy issues, a Privacy Protection Board would inevitably find itself unable to articulate a coherent, consistent, predictable, genuinely useful set of guidelines for resolving conflicts. Nor, because reasonable people will continue to disagree, would such a board be able to achieve consensus over time that privacy was ever being sufficiently protected.

To advocate a Privacy Protection Board is implicitly to discount the significance of context-dependence. Worse still, it requires glossing over the fact that privacy itself is a contested value. Citing public opinion polls and

---

[256] Indeed, there is reason to believe that the private market for information about consumers still has considerable room for improvement with respect to satisfying consumer preferences for privacy. For description of some of the issues confronting database marketers in the private sector, and suggested guidelines to improve the practices of database marketers, see Frank V. Cespedes & H. Jeff Smith, *Database Marketing: New Rules for Policy and Practice*, SLOAN MGMT. REV., Summer 1993, at 7.

surveys,[257] the writings of Privacy Protection Board proponents convey the impression that genuine agreement exists among Americans that privacy is not sufficiently protected, and, accordingly, that a Protection Board would have a relatively simple task of effectuating a widely shared understanding of how much privacy we really want.[258] In fact, however, there is substantial disagreement—both in the abstract and on a case-by-case basis—about how much privacy is the right amount and about how much of other good things we should be willing to give up for it.[259]

At a more mundane level, a Privacy Protection Board presents a question about the allocation of resources and raises the issue of what would in fact be required in the way of "oversight" to keep track effectively of the sharing of information within government. The federal government is so huge and sprawling, its uses of personal information so multifarious, its records systems so massive and decentralized, its privacy practices so much a product of particular agency cultures and agendas, that actually to oversee, monitor, and standardize the government's information policies would be a task of monumental, if not insuperable, difficulty. Were such a task to be undertaken, its successful achievement would require a commitment of political will, financial resources, and staff energy the magnitude of which is daunting to contemplate.

Without such a huge commitment, a Privacy Protection Board might be able to accomplish the considerably more modest task of simply making privacy a more salient issue, of "bring[ing] more visibility to the issue of personal information collection and use."[260] This would be perhaps a worthwhile achievement, but it would not be an unambiguous gain. Again, it is important to remember that the normative foundations of the claim to informational privacy with respect to data already disclosed to the government are far from impregnable, and that there is little empirical support for assertions that individuals subjectively or realistically entertain expectations that information they provide for one use will not be used for another.

---

[257] *See generally* HARRIS-EQUIFAX, CONSUMER PRIVACY SURVEY 1992, at 15 (1992) (reporting that 78% of Americans say they are very or somewhat concerned about threats to personal privacy as compared to 64% in 1978); HARRIS-EQUIFAX, HEALTH INFORMATION PRIVACY SURVEY 1993, at 25 (1993) (reporting that 79% of American population is very or somewhat concerned about threats to personal privacy).

[258] Rotenberg, *supra* note 10, at 80 ("Concerns about privacy protection are widely shared by the general public.").

[259] *Cf.* Simitis, *supra* note 55, at 742-46 (discussing the difficulties that all countries experience in monitoring privacy, because the task "consists not of helping government enforce its policies but of preventing both government and private institutions from overstepping" boundaries, and noting that "the possibility of conflict . . . is ever present").

[260] Regan, *supra* note 33, at 633.

Finally there is a real question as to whether privacy would be enhanced—or put at even greater risk—if control of personal data collection and use were centralized in one super governmental agency. In a way, the proposal for a Privacy Protection Board seems a little like recommending that the fox, albeit dressed up as a benign and friendly farmer, guard the chickens. The tyranny imagined in the Orwellian nightmare depended not merely upon government pursuing a deliberate course of information manipulation and ceaseless surveillance, but also on the centralization of all data about everyone in one government agency. "[O]ne of the most practical of our present safeguards of privacy is the fragmented nature of present information . . . . A central data bank removes completely this safeguard."[261] The government certainly has the capacity to create a central data bank, but nothing indicates that one exists or is even being contemplated. To the contrary, what presently exists are lots of *un*central data banks. So long as our government's system of personal data *protection* remains "fragmented, discontinuous and incomplete," so will its systems of data *collection*, *dissemination*, and *use*. Unless the mere existence of information in government files is an invasion of privacy, it may well be that the very diffusion of data and data banks within the government, the diversity and *de*centralization of data collection and data protection practices within the myriad federal agencies are not the problem, but the solution.

[261] *The Computer and Invasion of Privacy: Hearings Before the Special Subcomm. on Invasion of Privacy of the House Comm. on Government Operations*, 89th Cong., 2d Sess. 6 (1966) (statement of Rep. Frank Horton of New York).