Privacy: Its Role in Federal Government Information Policy

DAVID F. LINOWES
COLIN BENNETT

Introduction

THE CONTINUOUS TENSION BETWEEN bureaucratic values and democratic control has been complicated in recent years by the rapid development of information technology and by its application to the agencies of government. As sophisticated computer and communications equipment has been introduced into public agencies, so information has become far easier to collect, store, manipulate, and disseminate. On the one hand, this has enhanced the management, decision-making, and analytical capabilities of governmental organizations. However, the advantages that contemporary data-processing techniques have brought are offset by certain dangers. In particular, the immense capability to control vast quantities of *personal* information on individual citizens has generated a worldwide concern about the potential for bureaucratic surveillance and about the consequent erosion of personal privacy.

The gradual realization of these dangers over the last twenty years has motivated most Western democracies to provide a policy response in the form of "privacy" or "data-protection" laws. Data-protection laws are confined to that aspect of privacy protection that arises from the collection, use, and disclosure of information on identifiable individuals. *Privacy* is used here to encapsulate the broad social value rather than

David F. Linowes is Boeschenstein Professor of Political Economy and Public Policy, University of Illinois at Urbana-Champaign and former Chairman, U.S. Privacy Protection Study Commission; and Colin Bennett is Assistant Professor, Department of Political Science, University of Victoria, British Columbia, Canada.

the specific policy area. *Data protection* (the European nomenclature, translated from the German *Datenschutz*) is a more accurate title for this group of policies whose main purpose is to regulate the collection, storage, use, and transmittal of personal data. Hence the Privacy Act, strictly speaking, is a data-protection law similar in purpose to those in Europe. Data-protection policy satisfies the right to privacy. But that right means more than the protection of information, and is advanced through many other statutory, judicial, and constitutional means.

All national legislation is based on a strikingly similar set of "fair information principles" designed to minimize intrusiveness in the collection of personal information; to maximize fairness in its use; and to provide reasonable and enforceable expectations of confidentiality with regard to its transmittal. The major data-protection legislation at the federal level in the United States, and the main focus of this article, is the Privacy Act of 1974.[1]

So far, neither the personal data-protection question in general, nor the Privacy Act in particular, have received much attention from social scientists. The context of rapid technological change has produced a large body of technical, legalistic, and polemical writing that is reactive and transient rather than reflective or theoretical. More especially, there are few studies of data protection as a policy problem using the concepts and approaches of political science. Consequently, policy advocacy has progressed without a clear understanding of the tractability of the problem, and of the behavioral and structural variables that might impede effective policy implementation.

The aim of this article is to examine personal data protection as a policy problem, employing concepts and approaches from the field of political science. This task involves: (1) an analysis of issue emergence and problem definition; (2) a study of policy formation; (3) an assessment of oversight and enforcement; and (4) an identification of the various conceptual, structural, and motivational factors that have prevented data protection from becoming a fully effective component of American national information policy. The article concludes by discussing the prospects for American data-protection policy given the ten years' experience of implementing the Privacy Act.

It should be noted, however, that other constitutional, common law, and statutory controls play a role in national privacy policy. The First, Fourth, and Fifth Amendments all limit government intrusiveness in a variety of ways and thus pertain to the subject of privacy. Certain recently enacted statutes include specific safeguards for certain types of data: the Fair Credit Reporting Act of 1970 (credit reports); the

Family Educational Rights and Privacy Act of 1974 (education records); the Tax Reform Act of 1976 (tax information); the Right to Financial Privacy Act of 1978 (private financial records); and the Privacy Protection Act of 1980 (press offices and files). The Brooks Act of 1965, the Paperwork Reduction Act of 1980, and the Federal Managers' Financial Integrity Act of 1982 established federal agency roles for managing automated systems. In October 1984, Congress enacted the Counterfeit Access Device and Computer Fraud and Abuse Act which imposes criminal penalties for certain computer-related crimes. All states also now have a variety of privacy laws for both public and private sectors. While we do not address state law here, it should be noted that the protections afforded at the state level are becoming increasingly extensive.

However, while U.S. privacy law is derived from a variety of sources, the centerpiece remains the Privacy Act of 1974. The experience of this legislation exposes the major problems of implementing personal data-protection policy and of trying to protect personal information in a climate of rapid technological change and competing information values. Further, to the American, government (rather than the private sector) has always been regarded as the major threat to privacy rights. Unlike in most European countries, the private sector remains largely unregulated at the federal level. There are some statutory controls mainly related to credit, banking, and insurance records. The Privacy Protection Study Commission recommended the extension of controls on a sectoral basis to other record-keeping relationships. Overall, however, the private sector in the United States is expected to act voluntarily.

This is not so with the public sector. The fear of information technology in the hands of government, as expressed in the Privacy Act, reflects a cultural belief that government is the primary potential threat and the most likely structure to misuse or abuse the enormous power of information technology. In this respect too it is fitting to regard the Privacy Act as the cornerstone of American privacy policy, the successful implementation of which is crucial if personal privacy is to play a meaningful role in national information policy.

Problem Definition and Issue Emergence

There is no generally accepted definition of privacy. A variety of cross-cutting values and interests intrude upon its very broad and amorphous range. The classic definition is the "right to be let alone,"

originally presented by Judge Cooley and later elaborated in a famous article by Warren and Brandeis.[2] As the concept developed throughout the twentieth century, it became applied to a wide variety of social relationships and modes of behavior. In 1960, William Prosser tried to clarify the case law and found a complex of four torts: (1) intrusions upon the plaintiff's seclusion or solitude or into his private affairs; (2) public disclosure of embarrassing private facts; (3) publicity that places the plaintiff in a false light; and (4) appropriation for the defendant's advantage of the plaintiff's name or likeness.[3] As the concept was granted constitutional status in 1965, as existing in the "penumbras" of the Constitution, so its span and application widened.[4]

Privacy as a problem of public policy, however, really arose with the development and spread of computer technology in the 1960s and especially with its application to government. Of particular importance was the abortive attempt to establish a "National Data Center" of all basic statistical data originating in federal agencies. Although this center was intended for aggregate statistical analysis and not for administrative decision-making about individuals, the proposal floundered when subjected to Congressional scrutiny.

Simultaneously, privacy came to be regarded more as a policy problem than something that can be protected in the face of rapid technological change by case law. The necessity for a more synoptic public-policy solution arose "partly because judicial policies and constitutional interpretation failed to promote legal recognition of and protection for individuals' claims that their right of privacy entails safeguards against abuse of personal information collected, maintained and utilized by the government."[5] Henceforth the right to "information privacy" was distinguished from other behavioral aspects of privacy (such as physical intrusion and surveillance) and granted its own separate distinction as an issue of public policy.

Two books, *Privacy and Freedom,*[6] a study commissioned by the Association of the Bar of the City of New York and authored by Alan Westin, and Arthur Miller's *The Assault on Privacy*[7] helped sensitize public and elite opinion to the problem and played a critical role in defining that problem. For both, information privacy meant giving individuals "the ability to control the circulation of information"[8] relating to them or "to determine for themselves when, how and to what extent information about them is communicated to others."[9] Personal information emerged from the debates in the late 1960s as *property* which could not be taken or misused by government without due process of law. Later the idea was refined into a set of principles of "fair

information practice" to ensure minimal intrusiveness, maximum fairness, and legitimate expectations of confidentiality.

Academic treatments gave way to empirical analyses as concern for the issue grew. Westin followed up his earlier work with a project for the National Academy of Sciences entitled *Databanks in a Free Society.*[10] In addition, a 1973 study entitled *Records, Computers and the Rights of Citizens*[11] by the Department of Health, Education, and Welfare's Advisory Committee on Automated Personal Data Systems called "attention to issues of record-keeping practice in the computer age that may have profound significance for us all." As the then Secretary of Health, Education and Welfare, Caspar Weinberger, wrote in its forward, it represented "the views of an unusual mixture of experts and lawyers."[12]

Kingdon, in *Agendas, Alternatives and Public Policies,* contends that policy is made in America when "the separate streams of problems, policies and politics come together at certain critical times. Solutions become joined to problems, and both of them are joined to favorable political forces."[13] In this case, the "solution" of fair information practices became linked to the "problem" of information privacy. Both were connected to the "favorable political forces" of Watergate. With its many and various cases of political bribery, corruption, malpractice, intrusiveness, and abuse of personal data, this crisis provided the propitious climate for the construction of a comprehensive data-protection policy.

Kingdon also suggests that this "coupling of the streams" is often facilitated by "policy entrepreneurs" defined as "advocates who are willing to invest their resources....to promote a position in return for anticipated future gain in the form of material, purposive or solidary benefits."[14] In the case of information privacy, the policy entrepreneur was Senator Samuel J. Ervin, Jr. (Democrat, North Carolina), who had been a staunch campaigner for protective legislation since the late 1960s. Ervin's central role as the chairman of the Senate investigative committee which held televised hearings into the Watergate affair, enhanced his stature. The passage of the Privacy Act in the final hours of the 93rd Congress, therefore, was a solution to a long-standing problem, a legislative response to the presidential abuse of power and a personal tribute to Ervin in his final term.

Policy Content

While privacy invasions in general had been a subject of Congressional interest since the mid-1960s, the idea of legislating a set of fair

information principles to protect the right to information privacy was motivated principally by the long-term efforts of Senator Samuel J. Ervin. In the House, the efforts of then Congressmen Edward I. Koch (Democrat, New York) and Barry Goldwater, Jr. (Republican, California) were instrumental in fostering broad bipartisan agreement on the basic content of the law.

The first principle in the act is that agencies shall not disclose personal information contained in a system of records without the "prior consent of the individual to whom the record pertains."[15] There are a number of controversial exemptions to this rule. Disclosure is permitted without consent to those within the agency who have a "need for the record in the performance of their duties"; to other agencies in connection with "routine uses," in other words for purposes "compatible with the purposes for which it was collected"; and to an agency engaged in "civil or criminal law enforcement activity." Agencies are also expected to keep an accurate accounting of all disclosures and ensure that corrections made are transmitted "down the line."

Second, the Privacy Act requires agencies to allow the individual access to "information pertaining to him" which is contained in a "system of records." A very similar right had existed since 1967 in the more widely drawn Freedom of Information Act (FOIA). Unlike FOIA, however, the Privacy Act grants the individual the concomitant right to correct any portion of that record which is not "accurate, relevant, timely or complete."[16]

The third principle concerns collection limitation. Agencies should only maintain those records that are "relevant and necessary to accomplish the purpose of the agency."[17] Records should be composed of information gleaned "to the greatest extent practicable directly from the subject individual." Data subjects should be informed of the authority for collection, the agencies to which the information may be transmitted, and the "routine uses" to which the information may be put.

Fourth, record systems should be public. Agencies are required to publish in the *Federal Register* at least once a year a notice of the existence and nature of each system of records containing details of the categories of individuals maintained therein, the type of information stored, and the practices of the agency regarding storage, retrievability, access, retention, and disposal. These systems notices are also sent to the Office of Management and Budget (OMB) and Congress for review.

The Privacy Act (unlike some of its European equivalents) applies to both manual and automated record-keeping systems and provides for both civil remedies and criminal penalties in the event of violation. It

was hoped that the implementation of these principles would restore the correct balance between the citizen and the record-keeping agency. To the extent that an American data-protection policy existed, it was reflected in a general consensus among privacy advocates that the dangers of information technology to individual rights could be minimized by the implementation of these principles by the federal agencies. A balance could be struck between the legitimate information needs of government and the constitutionally recognized privacy rights of the citizen.

The major controversy centered not on questions of principle but on methods of implementation. From an early stage in the debate, privacy advocates agreed that the most effective way to establish fair information practice would be through an independent commission. Advocates differed, however, over the size of such a body and over whether it should be granted the authority to enforce its regulations (thus making it in effect a regulatory body). As Regan demonstrates, the question of implementation came to dominate the policy discussions during which bureaucratic interests in maintaining maximum autonomy over personal information systems surfaced and eventually prevailed. This exposes the dilemma of trying to decide implementation questions during policy formation: "When implementation questions are left unresolved in policy design, bureaucratic concerns will dominate the implementation stage, but when implementation questions are resolved in policy design, bureaucratic concerns will dominate the formulation stage."[18]

Arguments about the need for an independent agency centered on the primary Senate bill[19] introduced by Senator Ervin. In contrast to the House bill,[20] Ervin's bill provided for a Federal Privacy Board with oversight and advisory responsibilities. A number of pressing factors forced Ervin to abandon this notion in the final days of the 93rd Congress: irreconcilable differences between House and Senate under severe time pressures; the overwhelming desire to provide some legislative response (however imperfect or symbolic) to the Watergate scandal; and the fear of a presidential veto if the bill contained provision for an independent and permanent privacy commission.

This backdown resulted in two compromises. First the Federal Privacy Board was transformed into a Privacy Protection *Study* Commission (PPSC) to investigate the issue and make recommendations to the president and Congress for action. The commission was given subpoena power and the power to swear witnesses. Two members were appointed by the president of the Senate, two by the speaker of the

House, and three by the president. The commission devoted the next two years to examining record-keeping practices in both the public and private sectors.

Second, the oversight function was given to the Office of Management and Budget. Inserted right at the end of the statute is a stipulation that: "The Office of Management and Budget shall—1) develop guidelines and regulations for the use of agencies...and 2) provide continuing assistance to and oversight of the implementation of the provisions."[21]

Enforcement and Oversight

The Privacy Act stipulates that responsibility for implementation lies principally with the agencies themselves. But two institutions were given specific oversight responsibilities—the OMB and the Subcommittee on Government Information of the House Government Operations Committee. The courts, and of course the individual "data subject," are also critical players in the complex enforcement scheme. We shall analyze the response of each of these players under the assumption that effective implementation (defined as bureaucratic compliance) requires constant monitoring by outside forces.

Oversight of the Privacy Act by the Office of Management and Budget

From the start, there was disagreement about the role that Congress expected OMB to perform. Congressional intent is obscure, with no clarification of the words "develop guidelines and regulations" and "provide continuing assistance and oversight." We shall evaluate OMB's performance according to three criteria: the issuance of guidelines; the compilation and presentation of the annual report; and the provision of assistance and oversight.

The first and major effort to issue guidelines took place in the first six months of 1975 prior to the promulgation of the *Privacy Act Implementation Guidelines*[22] in July, ten weeks before the act became effective. While this circular contained a comprehensive section by section analysis of the act, there was little comment or interpretation. No additional formal guidance of consequence was issued until 1979 when, amid controversy surrounding the "Project Match" at the Department of Health, Education and Welfare, OMB developed comprehensive guidelines on the conduct of computer matching programs. This refers to the running of one computer tape against another to selectively identify those illegally receiving benefits, draft evaders, or others presumed guilty of cheating, tax evasion, or more serious criminal acts.

Since its inception, computer matching has been controversial, with many questions raised about its constitutionality (primarily under the Fourth Amendment), its cost-effectiveness (when so much follow-up effort is required), and also about its legality under the Privacy Act.[23]

An examination of the legislative history of the Privacy Act reveals that few people anticipated the possibility of computer matching. Virtually nobody foresaw the legal difficulties. Controversy centers on whether the transferral of tapes of personal data from one agency to another for matching purposes is a "routine use" and is therefore exempt from the consent requirements of the Privacy Act. The OMB guidelines of 1979 do not sufficiently clarify this issue. The House Government Information Subcommittee concluded that the guidelines were "largely procedural and intended to finesse some of the difficult legal questions."[24] Apart from a 1983 memorandum addressing the relationship between the Privacy Act and the newly passed Debt Collection Act,[25] no further guidance has been issued. On the question of guidance, it appears that 1975 was the "high water mark of Privacy Act activity in OMB."[26]

Analysis of the second function, the provision of the annual reports, is also revealing. That covering calendar year 1975 was 424 pages long, in two volumes, and included a complete inventory of federal personal data systems.[27] The second,[28] third,[29] and fourth[30] reports covered the same scope within single volumes. In 1980, the inventory of personal-data systems was dropped. Details are still published in the *Federal Register* but they are no longer compiled in a convenient form. The fifth,[31] sixth,[32] and seventh[33] reports are consequently a lot slimmer (no more than twenty pages) and concentrate on the barest reporting requirements of the law. Some observers have considered the latter two deficient in this regard.[34]

Finally, the provision of "assistance to" and "oversight of" agency implementation has not been interpreted in an aggressive way. OMB staff review the information system notices before they go to the *Federal Register* to ensure that they accurately describe: the categories of records stored; the "routine uses"; the information management practices of the agency; and the extent of the record subject's rights. They also review the fewer and more controversial proposals for exempt systems (mainly dealing with security or law enforcement matters). Figures on the number of exempt systems per agency are specifically required to be published in the annual reports.

In addition, they regularly answer questions from agencies in relation to the interpretation of the Privacy Act. In general, however, the

role is reactive rather than aggressive. OMB fulfills the first half of its responsibilities under Section 6 (2)—it provides "assistance." Apparently it does not provide "oversight," in the sense of actively ensuring that agencies comply with the fair information principles. As the 1983 House hearings revealed: "OMB's Privacy Act oversight efforts have been restricted to responding when issues and problems are presented to it. In the absence of a proposed system notice, OMB will not raise a question, start an investigation, or otherwise monitor Privacy Act compliance."[35]

Congressional Oversight of the Privacy Act

With the realization in 1974 that a separate Privacy Commission would not be created, Senator Ervin noted that "it will require aggressive oversight by the Committee on Government Operations" for the Privacy Act to be effective. Ogul draws the distinction between "formal" and "latent" oversight, arguing that those who just examine the written investigative committee record may be overlooking the more informal and routine process of monitoring that goes on away from public and media attention.[36] We shall make the same distinction in analyzing the Congressional response to the Privacy Act.

From the standpoint of formal oversight, the number of days directly devoted to hearings on the Privacy Act alone is low, specifically three. In June 1975, before the act had come into force, the Government Information and Individual Rights subcommittee conducted a day's hearings to ensure that agencies were preparing to meet their obligations. The committee found that, with the exception of the Department of Defense (which had decided to set up a separate operational unit to administer the act on account of the large number of record-keeping systems in the department), OMB and agency efforts were less than enthusiastic.[37]

It was another eight years before the next formal investigation by the Government Information Subcommittee of the House Government Operations Committee. Two days of hearings were held in November 1983, at which written and oral testimony were received from a number of officials, interest group leaders, and "privacy experts."[38] The hearings had symbolic significance as well as an investigative purpose: there had been no general oversight hearings since enactment; the literary significance of *"1984"* had brought the questions of surveillance by the "Big Brother" state to public attention; and the growing volume of international data traffic had increasingly exposed the incompatibility of the stronger and more comprehensive European laws, causing anx-

iety abroad that legal protections in the United States were inadequate to protect personal information sent to this country for data processing.

The result of these hearings was a report entitled *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress.* This report indicated that interest in privacy issues had steadily diminished. Simultaneously, Congressman Glenn English, the chairman of the Government Information Subcommittee, introduced a bill to establish a permanent Privacy Protection Commission.[39] Nothing particularly original surfaced from this oversight effort, mainly because other investigative bodies had already exposed the major shortcomings. For instance, the Privacy Protection Study Commission issued an incisive analysis of the Privacy Act as an appendix to its 654-page report *Personal Privacy in an Information Society.*[40] As early as 1977, it was apparent that "the difficulty with the current law does not appear to arise from the flexibility of implementation it allows, but rather from the fact that agencies have taken advantage of that flexibility to contravene its spirit."[41] The act also received criticism from the General Accounting Office,[42] and from other congressional committees that had been looking into related issues: the privacy of medical records,[43] international data flow,[44] and computer matching.[45] Hence, the 1983 hearings and report on general Privacy Act oversight served to put on the official record what most observers knew already.

Ogul further suggests that most members of Congress prefer more informal methods of oversight, and that "formal methods are seen as an indication of the breakdown of informal efforts."[46] This is probably what happened here, although there is some evidence that the continuous efforts of the staff of the Government Information Subcommittee over the years have yielded modest results in some respects.

Congress is specifically granted two oversight mechanisms in the Privacy Act. The first is the annual report which—as already demonstrated—has been little used. The second is the requirement that agencies give prior notice of the creation or alteration of any system of records. To the extent that latent oversight exists, it centers on the examination of these system notices by the staff of the subcommittee on government information. It is estimated that around 20 percent of these reports are found to require follow-up enquiry, either by a telephone call or, in more serious cases, by a letter from the congressman. Most controversy seems to stem from the claiming of new "routine uses" for personal information.[47]

The committee staff over the years has gained considerable expertise in reviewing these system notices and in detecting irregularities. Insofar as these formal descriptions reflect the actual personal information practices of an agency, the staff has a fairly comprehensive view. On the other hand, they are aware that a massive activity such as the collection, use, and disclosure of billions of personal records can only be reflected to a very limited extent in a system notice.

Enforcement through the Courts

The case law under the Privacy Act is underdeveloped because of the restrictive remedial scheme. The act stipulates that damages can only be awarded if it can be demonstrated that the plaintiff has suffered actual injury from an intentional agency action. This is virtually impossible to prove, given the intangible and speculative nature of the harm that might result from the unfair collection, use, and transmittal of personal information. Injunctive relief is available only to force access to and amendment of records. Most litigation relates to the interpretation of the exemptions to access and to their relationship with those under the related FOIA.[48]

Furthermore, the courts have not broadly recognized a right of privacy for information held by third parties. In *U.S.* v. *Miller*[49] the Supreme Court held that an individual has no Fourth or Fifth Amendment interest to assert when government demands access to the records an organization maintains about him (in this case, bank records). An individual's expectation of privacy for records held by any third party is neither legitimate, warranted, nor enforceable under the Constitution. The Privacy Protection Study Commission described this as a "fateful day for personal privacy."[50] While it should be noted that subsequently Congress enacted the Right of Financial Privacy Act of 1980 to protect the confidentiality of bank records, the Miller decision also meant that Privacy Act implementation was a matter for legislative and executive oversight rather than judicial enforcement.

The Role of the Individual Data Subject

The importance of the rights of individual access and correction in the overall implementation scheme is also not as great as many expected. There is little retrievable under the Privacy Act which cannot also be obtained through the FOIA. Consequently, as the PPSC found, "the number of Privacy Act access requests (i.e., requests specifically citing the Privacy Act) has not been great and most have come from agency employees or former employees."[51] The last time comprehensive

figures were compiled (for calendar year 1978) OMB reported nearly 750,000 access requests to federal agencies for personal records. Of these, 96 percent were granted in whole or in part. Some 43 percent of requests went to the Department of Defense (which has the highest number of record systems). Over 90 percent were received by five agencies—Defense, Veterans Administration, HEW, Justice, and Transportation.[52]

These data should be treated with considerable caution as it is not clear how much of this participation is the direct result of the Privacy Act. Most agencies operating public-assistance programs already had procedures to allow record subjects access to their files as part of the eligibility verification process. And since 1967, access to personal records could be gained through the FOIA. Moreover, there are major problems of definition and quantification. The majority of requesters do not cite the Privacy Act let alone a specific system of records. Some cite both the FOIA and the Privacy Act (as the civil liberties groups advise). Most just ask to see "their file on...."

Although there are no pre-1974 figures on access requests, it is unlikely that the Privacy Act ushered in a completely new spirit of openness. The OMB has concluded that the main result of the access right "has been to give the agencies a uniform set of procedures for handling requests for record subjects...even when the requests do not cite a specific Act."[53]

The Barriers to Successful Implementation

The impact of the Privacy Act is difficult, if not impossible, to assess in any specific way. The policy goals are not defined in terms of achieving tangible results (such as distributing or redistributing a public good). The resource to be regulated is an elusive one. Violation of fair information practice is only visible in a tiny minority of circumstances. Hence, wrongful collection, storage, and dissemination of personal information (while in violation of the Privacy Act) may not expose actual harm to the individual concerned. There are no firmly established or measurable standards of evaluation. Our assessment of impact relies more on impressionistic and anecdotal evidence from those with the direct experience of implementation.

The Privacy Act codified an important set of principles that have had a significant impact on the way agencies think about and treat personal information. The major effort at compliance, which took place from 1975 to 1976, succeeded in establishing the extent and nature of personal record-keeping practice in the federal government. Privacy

Act officers were appointed in each agency. Standard operating procedures were instituted for the collection, use, and dissemination of personal data. Compared to the time prior to 1974, the act appears a major force for change. But there remain serious weaknesses and limitations which will now be explored in greater detail.

Explanations of the inadequacy of the Privacy Act offered in the past have been predominantly legal. Inherent statutory weaknesses and inconsistencies have produced ambiguous guidelines, a weak implementation framework, and allowed officials to take advantage of the wide latitude and vague prescriptions. While statutory weaknesses are important there are other limitations relating to the tractability of the problem, the structure of the implementing institutions, and the incentives of the implementing officials.

Inherent Statutory Weaknesses

The inherent weaknesses of the Privacy Act have been well documented. Several have been alluded to earlier. Sabatier and Mazmanian, presenting their framework for implementation analysis, argue that "original policy makers can substantially affect the attainment of legal objectives by utilizing the levers of power to coherently structure the implementation process."[54] Several conditions need to be met.

Most crucially, the statute must contain "clear and consistent objectives." The Privacy Act is deficient in this regard as the language is at times vague or contradictory. For instance, "each agency...shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency."[55] The words "relevant and necessary" are interpreted by the agencies themselves and normally given an expansive definition.

In addition, agencies should not disclose personal information contained within a system of records without the "prior consent of the individual to whom the record contains."[56] This general principle, however, is qualified by ten different exemptions. Most controversially, disclosure is permitted if for a "routine use," that is for purposes "compatible with the purposes for which it was collected." Agencies have found some broad definitions of "compatible," particularly in relation to the process of computer matching to detect waste and fraud. For example, in 1980, the Office of Personnel Management (OPM) released some of its records to help the Veterans Administration check the accreditation of its hospital employees. OPM claimed that the disclosure constituted a "routine use" of its data because the agency believed "that an integral part of the reason that these records are

maintained is to protect the legitimate interests of government and, therefore, such a disclosure is compatible with the purposes for maintaining these records."[57]

The notion of information privacy may be incompatible with laws and procedures requiring openness and disclosure. The values underlying the Freedom of Information Act,[58] for example, may be viewed as opposed to those upon which the Privacy Act is based. Many argue that in fact they are two sides of the same coin; both attempt to check governmental power by placing constraints on an agency's control of information. At the level of statutory language, however, the competing values of disclosure and confidentiality are at times in conflict. Interpretation of the two laws continues to provide dilemmas for both the courts and the agency information officers (who are often responsible for both statutes).

As mentioned earlier, the Privacy Act does not provide an effective process for the recovery of damages: "The vast number of systems involved, the need to establish willful or intentional behavior on the part of the agency, and the cost and time involved in bringing a lawsuit, often make enforcement by the individual impractical."[59] In most cases, an individual has to show actual injury as a result of unlawful collection, use, or disclosure of his/her personal information. Because this is virtually impossible to prove, the Privacy Protection Study Commission recommended that a suit for punitive damages should be permitted in the absence of a demonstration of actual injury to the individual.

The Tractability of the Problem

It is clear that some social problems are much easier to deal with than others. Some are more technical and some require the alteration of behavior by large and diffuse target groups. In this case, the difficulty stems more from the extent of behavioral change required by the regulated body—namely the federal bureaucracy.

Agencies are expected to alter long-standing practices regarding the treatment of personal information. All information is a vital resource for the agency's internal decision-making processes as well as important in its relation to the external environment. The capacity to manipulate information has increased exponentially with the introduction of information technology. As Regan argues: "Information in general is a resource that contributes to bureaucratic autonomy in terms of stability, predictability and competency over its functions and goals; the value of personal information is no different."[60] Federal agencies under the Privacy Act are expected to surrender their monopoly of control over a

vital resource. They face limitations on the collection, storage, retrieval, and transmittal of that resource. Such counterpressures may explain why the federal bureaucracy has often taken advantage of the flexibility of the Privacy Act to, in effect, contravene its spirit.

There is a qualitative difference between expecting a public agency to alter its standard operating procedures to distribute or redistribute goods and services, or to regulate an outside activity, and expecting it to submit to regulation itself. Privacy policy shares with other attempts to "open up" government (such as freedom of information or sunshine laws), the somewhat peculiar characteristic that the target group is the bureaucracy, and that the "impact" is defined and evaluated in terms of reducing bureaucratic power.

Structural and Resource-Related Factors

In earlier years the conventional wisdom saw administration as the neutral instrument of the Congress and executive branch with effective control established through certain simple principles of organization: strong managerial leadership, clear lines of authority, meritocratic promotion, etc. It was assumed that controlling bureaucracy was an objective desired by both Congress and president but which was impeded by a wide range of structural and resource-related factors. The problem was one of means rather than will.

Congress appropriated no additional funds for the act's implementation. The individual agencies and the OMB, therefore, have had to comply with a complex and innovative set of statutory expectations within the limits of existing resources. Most agencies appointed Privacy Act officers, most of whom have other responsibilities (such as for FOIA) and who may not be highly placed in the agency hierarchy. They often have little ability to voice privacy interests in the face of more politically important agency tasks.

Until 1980, responsibility for Privacy Act oversight at OMB was in the hands of one or two persons in the Information Systems Policy Division. After that date, with the reorganization pursuant to the passage of the Paperwork Reduction Act, responsibility became diffused within the newly created Office of Information and Regulatory Affairs (OIRA). Each OIRA desk officer is responsible for all the information resources management activities of his or her agency. These include: forms clearance, checking for onerous regulations, the establishment of automatic data processing systems, as well as privacy matters.

The former administrator of OIRA claimed that "this has meant a strengthening and enlargement of the scope of our review. An agency's

Privacy Act activities are examined within the context of other relevant information resources management activities."[61] Conversely, the organizational reform has meant that no one person in OMB has responsibility for Privacy Act oversight. Privacy questions have been subsumed by the programmatic goal of reducing federal regulations and paperwork under the Paperwork Reduction Act. While this goal is compatible with the aim of the Privacy Act to limit information collection to that which is "relevant and necessary," the net effect of this combination of functional responsibilities has been to make the Privacy Act less effective.

In this capacity the act has contributed to some reduction in unnecessary information collection, in the elimination of a large amount of information from existing systems, and in the consolidation of a number of duplicate record-keeping systems. The Privacy Act has been described as a "records management statute" rather than a mechanism to protect individual rights. The fact that the act provides for administrative responsibilities to be added to the already heavy OMB workload is no doubt a contributory factor.

Congress is also faced with considerable structural and resource-related obstacles. The PPSC noted that the Subcommittee on Government Information has neither the "staff nor the consolidated expertise necessary to evaluate each report submitted. Furthermore there is no agreement on how to assess the potential impact of a proposed system change along the lines called for in the Act."[62] The Privacy Act, because of its comprehensive application to the entire federal bureaucracy, is virtually impossible to monitor by one congressional subcommittee whatever the staffing level. The information practices of agencies differ widely. Staff cannot hope to become expert in the wide range of public policies for which personal information is collected and used. They cannot build ties with all the agency personnel responsible for implementing data-protection policy. The comprehensive scope of the act, cutting across all policy sectors, many of which require huge and complex information systems, presents the major structural dilemma to Congress.

Motivational and Incentive Explanations

As our understanding of the behavior of politicians and bureaucrats has become more thorough, so structural and resource approaches to bureaucratic control have been supplemented, and in some cases replaced, by those stressing motivations and incentives. The literature reveals a progressive shift away from the conceptualization of static institutional relationships toward models which emphasize more

dynamic, reciprocal processes of mutual adaptation between policymakers and implementers. This more complex understanding has led political scientists to realize that "controlling," "monitoring," or "overseeing" the bureaucracy can only arise through a thorough understanding of the "realpolitik" of the policy process and of the federal agency's central and political role in that process. More directly, the problem becomes not what oversight of the Privacy Act Congress and OMB *can* perform but what they *want* to perform.

From the outset, commentators recognized that the location of Privacy Act responsibility in OMB would provide few incentives for aggressive oversight. OMB's primary mission as coordinator of the president's budget and fiscal watchdog may be incompatible with many of the programmatic goals of data-protection policy. Interviews with officials in OMB revealed that the implementation of the Privacy Act has been monitored to the extent that it provides statutory support for OMB's emphasis on economy and efficiency in government. Hence the stress on limiting the collection of irrelevant material and eliminating duplicate information systems. The major provisions of the act (the use and disclosure restrictions, and the access and correction principles), however, impose direct manpower costs. Accordingly, OMB has monitored these provisions with less force than it has its primary functions.

The congressional incentives to monitor bureaucratic compliance are correspondingly low in the sense that personal data-protection policy requires comprehensive and coordinated control. Fiorina argues that "Congress has no electoral incentive to work toward coordinated control. Quite the opposite is the case. Congress is making increasing use of instruments that keep the bureaucracy more closely tied to decentralized Congressional control."[63] The splintering and decentralizing trends in Congress in recent years have occurred to allow members increased influence over segments of the bureaucracy of concern to them and their constituents. Control of the parts is achieved at the expense of control of the whole. Congress maintains the type of bureaucracy that makes it permeable to legislative influence. By doing so it facilitates the type of work most beneficial to the individual legislator: securing distributive benefits and casework.

Hence, when a policy like data protection arises, demanding congressional oversight of the implementation of a policy protecting a diffuse value in the entire federal bureaucracy on behalf of the whole citizenry, the motivations are going to be low. This is especially so at a time when the issues of efficiency and economy in government are politically attractive. Given the prevailing climate, it appears that con-

gressional interest will remain low until some outrage—maybe the Three Mile Island equivalent of privacy—involving a massive abuse of personal data, serves as a catalyst for public and legislative attention.

Conclusion: Prospects for Privacy in the Information Society

As we have shown, the Privacy Act has some important flaws—particularly the expansive and flexible nature of the "routine use" exemption and the inadequacy of the remedial scheme. It also suffers from the inherent programmatic goals which may require a reduction in bureaucratic information control and power. In this regard the delegatory pattern of policy-making (where Congress has ordered the bureaucracy to keep its own house in order) is likely to fail especially given the absence of an outside institutional force with the incentive and means to monitor and regulate the public use of personal information.

Moreover, these institutional failings have occurred in a climate of rapid technological development. As the "information revolution" continues to produce staggering advances in miniaturization, desktop storage capacity, computing speed and instantaneous retrieval, so the networking of information systems has been facilitated, and data have become far easier to transmit and retrieve. A recent study by the General Services Administration of the federal government's purchase of small computers found that agencies bought 37,277 such units in fiscal year 1984 at a cost of $137 million. The equivalent figures in 1983 were 8000 units at a cost of $34 million. It is estimated that federal agencies may acquire a half-million small computers by 1990.[64] These developments could raise the same normative questions about the overintrusive state that were debated back in the 1960s and 1970s. The imperative of balancing the legitimate needs of government with the personal rights of the citizen is as great as ever.

This context of rapid change, together with the observed inadequacies of existing institutional mechanisms, has led observers to renew the call for a permanent and independent privacy commission similar to that proposed in the original Senate version of the Privacy Act. Such a body should have oversight, advisory, and analytical responsibilities. This was an important recommendation of the Privacy Protection Study Commission.

Yet the same factors have also prompted others to argue that such a reform would not only be politically impossible but ultimately irrelevant. This school of thought holds that a privacy commission without a privacy constituency could be the reverse of the progressive step

intended. Once created, such a body could present the illusion of protection and at the same time be susceptible to interference by those with goals and interests which conflict with privacy. The necessary check on bureaucratic power will not arise if a coalition of interests does not perceive the value at stake and organize itself to address the important issue. So efforts should be directed toward building such a constituency while lobbying for a strengthening of the law to allow effective remedies through the courts.

The difficulty for privacy advocates in deciding upon a lobbying strategy is that "privacy" is a very complex issue which is not easy to frame in general terms. It is closely related to other issues (such as confidentiality, secrecy, and computer security). In some respects, such as free speech and other First Amendment concerns, it directly challenges other interests advanced by the civil liberties lobby. Privacy invasions are specific and context-related. The harm to be remedied is variable because the value of personal information changes from time to time, from person to person, and from organization to organization. The issue and the policy problem are perceived and evaluated subjectively. The statutory protections are only seen to be of value when specific harm is demonstrated. For these reasons a "privacy constituency" is not likely to emerge. The Privacy Act was passed not because of pressure from such a constituency, but because of the enormous and transcendant significance of the events surrounding the Watergate crisis.

Hence we reach the dilemma of implementing data-protection policy in the federal bureaucracy. Without a supportive privacy constituency it is rendered subordinate to other policy interests. The policy sits uneasily within the dominant style of American policy-making: a fragmented system in which "subgovernments" or "issue networks" interact within more or less clearly defined policy sectors to convey tangible governmental benefits to subsidized individuals, groups, and corporations.[65] While a permanent privacy commission would provide a more specialized and expert focus for concern, it would have to operate without the support of a clientele (other than civil liberties and consumer protection groups) that would derive recognizable benefits from its work.

These dilemmas have persuaded more recent commentators that privacy issues cannot continue to be viewed in individualistic terms. While opinion polls[66] continue to show that a majority of the American people are concerned about personal privacy, this concern has not been effectively translated into either the use of access and correction rights,

widespread litigation, or political lobbying and protest. It is argued that, as privacy is becoming inextricably linked with other information policy issues (such as computer crime, data security, and international data flow), it could be more advantageous to view privacy as just one social problem among many which are emerging in the information society. If an independent federal body is established, it should be given the responsibility to address the whole array of national and international issues associated with all types of sophisticated computer and communications equipment.

Each of the three approaches outlined earlier share the same rationalistic faith in man's ability to control the adverse effects of technology. The solution does not lie in a Luddite restriction of technological progress. The computer is a human creation. There is nothing inherent in the technology that cannot be incorporated into our existing system of legal and institutional controls. The computer has created a temporary imbalance between the individual and the modern complex organization. Privacy policy rests on a theoretical assumption that balance can be restored by the successful application of these rationally conceived principles of fair information practice. The goals of the Privacy Act are laudable; the problem so far lies in its full implementation.

Others see the situation differently, questioning the premise that organizations require more and more accurate personal information for effective operation in the first place. Taken to its extreme, this argument could lead to the conclusion that privacy is immediately lost once a record-keeping system is established, and vast quantities of personal data are collected and stored. Under these assumptions, personal privacy can only be regained by a dismantling of such systems and by developing a looser, less discriminating relationship between the individual and the modern complex organization.

The final prospect stems from the belief that as social change is driven by technology, law and public policy can only have at best a tangential influence on these inexorable processes. The theory is normally called "technological determinism" and is most closely associated with Ellul's *The Technological Society*.[67] The force behind social change has been the drive for improved "techniques." This force has overwhelmed political and legal controls and has progressively shaped social institutions according to the exigencies of the latest technology. More specifically, information technology has been regarded as the primary force behind the change from industrial to "post-industrial" or "technetronic" society—a society "shaped culturally, psychologically, socially, and economically by the impact of technology and electronics, particularly in the area of computers and communications."[68]

We do not need to embrace this theory wholeheartedly to see that the prescription to dismantle information systems is unrealistic. The post-industrial society is an information society. The vastly expanded capacity to collect, store, manipulate, and transmit data has irrevocably changed our lifestyles, workplaces, educational institutions, businesses, and political systems. In the post-industrial society, the individual has to expect a greater accumulation of information about him/her and the circulation of that information throughout society. Some aspects of privacy may be an inevitable sacrifice for the other advantages that information technology offers.

While the future of a comprehensive and enforceable personal data-protection policy is uncertain, the various scenarios may be becoming more clear. We can maintain the individualistic goals of the privacy issue and try to reconcile individual rights with the management needs of inherently hostile bureaucratic institutions. This may be achieved either through a new privacy-protection commission or more traditionally through case law. We can abandon those goals and treat privacy as one social problem among many in the information society. We can fight the information revolution to seek a looser, less efficient, and less discriminating relationship between the individual and the modern record-keeping organization. Or we can be philosophical and recognize that in a technologically driven society the advantages of information technology will inevitably conflict with our search for individual freedoms. What is certain, however, is that whatever direction national data-protection policy takes, privacy will still have a powerful emotive appeal within our political culture and will remain a central and cherished part of the system of individual freedoms in American society.

References

1. 5 U.S.C. 552a.

2. Warren, Samuel D., and Brandeis, Louis D. "The Right to Privacy." *Harvard Law Review* 4(Dec. 1893):193-220.

3. Prosser, William. "Privacy." *California Law Review* 48(Aug. 1960):383-423.

4. *Griswold* v. *Connecticut*, 381 U.S. 479 (1965).

5. O'Brien, David M. *Privacy, Law and Public Policy*. New York: Praeger, 1979, p. 203.

6. Westin, Alan F. *Privacy and Freedom*. New York: Atheneum, 1967.

7. Miller, Arthur R. *The Assault on Privacy*. Ann Arbor: University of Michigan Press, 1971.

8. Ibid., p. 40.

9. Westin, *Privacy and Freedom*, p. 7.

10. Westin, Alan F., and Baker, Michael A. *Databanks in a Free Society*. New York: Quadrangle, 1972.

11. U.S. Department of Health, Education and Welfare. *Records, Computers and the Rights of Citizens.* Washington, D.C.: HEW, 1973, p. vi.
12. Ibid.
13. Kingdon, John W. *Agendas, Alternatives, and Public Policies.* Boston: Little, Brown, 1984, p. 204.
14. Ibid., p. 188.
15. 5 U.S.C. 552a, sec. 3(b).
16. 5 U.S.C. 552a, sec. 3(d).
17. 5 U.S.C. 552a, sec. 3(e).
18. Regan, Priscilla M. "Personal Information Policies in the United States and Britain: The Dilemma of Implementation Considerations." *Journal of Public Policy* 4(Feb. 1984):36.
19. U.S. Congress, Senate. *A Bill to Establish a Federal Privacy Board,* S.3418, 93d Cong., 2d sess., 1974.
20. U.S. Congress, House. *A Bill to Amend Title 5 U.S.C., By Adding a Section 552a to Safeguard Individual Privacy from the Misuse of Federal Records.* H.R. 16373, 93d Cong., 2d sess., 1974.
21. 5 U.S.C. 552a, sec. 6 (PL 93-579).
22. 40 Fed. Reg. 28948.
23. See, U.S. Congress, Senate Committee on Government Affairs. *Oversight of Computer-Matching to Detect Fraud and Mismanagement in Governmental Programs,* 97th Cong., 2d sess., 1982; and Shattuck, John. "In the Shadow of *1984:* National Identification Systems, Computer Matching, and Privacy in the U.S." *Hastings Law Journal* 35(July 1984):991-1005.
24. U.S. Congress, House Committee on Government Operations. *Who Cares About Privacy? Oversight of the Privacy Act of 1974 by the Office of Management and Budget and by the Congress.* H. Rept. 455, 98th Cong., 1st sess., 1983:11.
25. 48 Fed. Reg. 15556.
26. U.S. Congress, House Committee on Government Operations, *Who Cares About Privacy?* p. 8.
27. U.S. Office of Management and Budget. *Federal Personal Data Systems Subject to the Privacy Act of 1974,* First Annual Report of the President. Washington, D.C.: OMB, 1976.
28. _____ . *Federal Personal Data Systems Subject to the Privacy Act of 1974,* Second Annual Report of the President. Washington, D.C.: OMB, 1977.
29. _____ . *Federal Personal Data Systems Subject to the Privacy Act of 1974,* Third Annual Report of the President. Washington, D.C.: OMB, 1978.
30. _____ . *Federal Personal Data Systems Subject to the Privacy Act of 1974,* Fourth Annual Report of the President. Washington, D.C.: OMB, 1979.
31. _____ . *Fifth Annual Report of the President on the Implementation of the Privacy Act of 1974.* Washington, D.C.: OMB, 1980.
32. _____ . *Sixth Annual Report of the President on the Implementation of the Privacy Act of 1974.* Washington, D.C.: OMB, 1981.
33. _____ . *Implementing the Privacy Act of 1974.* Washington, D.C.: OMB, 1982.
34. U.S. Congress, House Committee on Government Operations, *Who Cares About Privacy?,* p. 26.
35. Ibid., p. 24.
36. Ogul, Morris S. "Congressional Oversight: Structures and Incentives." In *Congress Reconsidered,* edited by Lawrence C. Dodd and Bruce I. Oppenheimer, pp. 317-31. Washington, D.C.: Congressional Quarterly, Inc., 1981.
37. U.S. Congress, House Committee on Government Operations. *Implementation of the Privacy Act of 1974: Data Banks (*Hearing before a subcommittee of the Committee on Government Operations), 94th Cong., 1st sess., 1975, pp. 1-33.

38. _____ . Committee on Government Operations. *Oversight of the Privacy Act of 1974* (Hearing before a subcommittee of the House Committee on Government Operations), 98th Cong., 1st sess., 1983.

39. _____ . *A Bill to Establish a Privacy Protection Commission* (H.R.3743), 98th Cong., 1st sess., 1983.

40. Privacy Protection Study Commission. *Personal Privacy in an Information Society*. Washington, D.C.: USGPO, 1977, appendix 4.

41. Ibid., appendix 4, preface.

42. U.S. General Accounting Office. *Agencies' Implementation of and Compliance with the Privacy Act can be Improved*. Washington, D.C.: GAO, 1978.

43. U.S. Congress, House Committee on Government Operations. *Privacy of Medical Records* (Hearings before a subcommittee of the House Committee on Government Operations on H.R. 3444), 96th Cong., 1st sess., 1979.

44. _____ . *International Data Flow* (Hearings before a subcommittee of the Committee on Government Operations), 96th Cong., 2d sess., 1980.

45. U.S. Senate, Committee on Governmental Affairs. *Oversight of Computer Matching*.

46. Ibid., p. 322.

47. U.S. Congress, House Committee on Government Operations, *Who Cares About Privacy?* p. 38.

48. Ehlke, Richard. *Litigation Trends Under the Privacy Act*. Washington, D.C.: Library of Congress, Congressional Research Service, 1983.

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

50. Ibid., p. 7.

51. Privacy Protection Study Commission, *Personal Privacy in an Information Society*, appendix 4, p. 83.

52. U.S. Office of Management and Budget, *Federal Personal Data Systems*, p. 15.

53. _____ . *Fifth Annual Report*, p. 12.

54. Mazmanian, Daniel A., and Sabatier, Paul A. *Implementation and Public Policy*. Glenview, Ill: Scott, Foresman, p. 25.

55. 5 U.S.C. 552a, sec. 3(e).

56. Ibid., sec. 3(b).

57. OPM statement, quoted in, Kirchner, Jake. "Privacy: A History of Computer Matching in the Federal Government." *Computerworld* 15(14 Dec. 1981):15.

58. 5 U.S.C. 552 (1967).

59. Privacy Protection Study Commission, *Personal Privacy in an Information Society*, appendix 4, pp. 103-04.

60. Regan, "Personal Information Policies," p. 23.

61. U.S. Congress, House Committee on Government Operations, *Hearings*, 1983, p. 70.

62. Privacy Protection Study Commission, *Personal Privacy in an Information Society*, p. 531.

63. Fiorina, Morris P. "Congressional Control of the Bureaucracy: A Mismatch of Incentives and Capabilities." In *Congress Reconsidered*, p. 341.

64. U.S. General Services Administration. *Purchase of Small Computers by the Federal Government in 1984*. Washington, D.C.: GSA, 1985.

65. Lowi, Theodore J. *The End of Liberalism*. New York: Norton, 1969.

66. Louis Harris and Associates. *The Road After 1984: The Impact of Technology on Society*. New Haven, Conn.: Southern New England Telephone, 1984.

67. Ellul, Jacques. *The Technological Society*. New York: Vintage Books, 1964.

68. Brzezinski, Zbigniew. *Between Two Ages: America's Role in the Technetronic Era*. New York: Viking Press, 1970, p. 9.