UIC Law Review

Volume 10 | Issue 3 Article 3

Spring 1977

Agency Implementation of the Privacy Act and the Freedom of Information Act: Impact on the Government's Collection. Maintenance and Dissemination of Personally Identifiable Information, 10 J. Marshall J. Prac. & Proc. 465 (1977)

Robert R. Belair

AGENCY IMPLEMENTATION OF THE PRIVACY ACT AND THE FREEDOM OF INFORMATION ACT: IMPACT ON THE GOVERNMENT'S COLLECTION, MAINTENANCE AND DISSEMINATION OF PERSONALLY IDENTIFIABLE INFORMATION

by ROBERT R. BELAIR*

INTRODUTION

Purpose and Methodology of the Study

This article is based on a study conducted for the Commission on Federal Paperwork.[1] The study was developed through an interview approach, the purpose of which was to identify and analyze agency information practices for the collection, maintenance and dissemination of personal data which had been affected by the Privacy Act[2] and the amended Freedom of Information Act.[3]

The research focused on changes in agency practices within three categories of information management.[4] First, I sought to

---

* Robert R. Belair is an attorney with the firm of Hill, Christopher and Phillips in Washington, D.C. Mr. Belair was formerly Acting General Counsel of the Committee on the Right of Privacy, Office of the President. He has served as a consumer attorney for the Federal Trade Commission and as a staff member for the National Academy of Sciences Project on Computer Data Banks.

He is a graduate of Kalamazoo College and Columbia Law School and a member of the District of Columbia Bar, the American Bar Association and the Federal Bar Association Committee on Government Information and Privacy.

Mr. Belair recently served as a consultant to the Commission on Federal Paperwork for privacy and freedom of information issues.

1. The Commission on Federal Paperwork was created by the Congress in December of 1974 to "study and investigate statutes, policies, rules, regulations, procedures, and practices of the Federal Government relating to information gathering, processing, and dissemination, and the management and control of these information activities." 44 U.S.C. § 3501 (Supp. V 1975). The Commission has a two year life; however, because of initial delays in appointing members, the Commission will not expire until October of 1977. This article is based primarily on research done for the Commission on Paperwork. However, the article is not a Commission report and the author is solely responsible for its content.

2. 5 U.S.C. § 552a (Supp. V 1975).

3. 5 U.S.C. § 552 (1970 & Supp. V 1975).

4. The study has its limitations which should be underlined at the outset. First, the equivalent of only twenty working days could be devoted to research. In all, approximately thirty-five individuals were interviewed including officials at ten agencies, congressional staffers, members of the press and representatives of oversight and guardian groups.

determine whether the Acts had changed the *character* of the personal information collected or the *collection methods* used. Second, I tried to discover whether agencies had changed their *system of handling* personal information as a consequence of the Acts. Were different amounts or types of personal information maintained? Was the information organized, audited, or secured in a different manner? Finally, I attempted to identify the way in which the requirements of the Privacy Act and the amendments to the Freedom of Information Act had affected agency *disclosure* of personal information.[5]

Even a brief methodology should make it clear that this article presents a broadly gauged and somewhat impressionistic overview of the effects of agency compliance with the Privacy Act and the amended Freedom of Information Act. In the Spring of 1977 the Privacy Protection Study Commission will publish the results of an exhaustive analysis of agency compliance with the Privacy Act.[6] At that point a large body of empirical information will be available against which to view the conclusions of this article.

Because this article concerns agency practices for the management of personal information, it focuses primarily on the Privacy Act. The Freedom of Information Act's disclosure provisions, however, have a theoretical impact on many aspects of personal information practices and hence the article deals with both Acts.

Background of the Freedom of Information Act and Privacy Act

Personal Data in Federal Files

The executive branch of the federal government collects, maintains and disseminates a staggering amount of personal information. Agency reports submitted in compliance with Privacy Act requirements indicate that the executive branch has 6,723 systems of records that are accessed by personal identifiers,

5. The article uses the term "disclosure" in its broadest sense to mean any sharing of information by the agency possessing the data including inter- (but not intra-) agency transfers, subject access and public dissemination.

6. Interview with Arthur Bushkin, Program Director Privacy Act Implementation Study, Privacy Protection Study Commission, in Washington, D.C. (Nov. 29, 1976). One section of the Privacy Act as passed, Pub. L. No. 93-579 § 5, created the Privacy Protection Study Commission. Simply stated, the Act directs the Commission to investigate, among other things, the handling of personal information by the private sector and recommend to the President and the Congress whether the principles in the Privacy Act should be extended to private organizations.

that is, identified by information personal to the subject.[7] The first set of system descriptions consumed over 3,000 pages of small print in the *Federal Register*. At last count federal data systems were estimated to contain more than 3.8 billion records about individuals.[8] It is impossible to estimate the amount of additional personal information held by federal agencies in systems that are not accessed by personal identifiers and hence need not be reported.[9]

For those systems about which agencies are required to publish reports, fifty-eight percent are maintained by three agencies: the Department of Defense; the Department of the Treasury; and the Department of Health, Education and Welfare.[10] Sixty-eight percent of this data is compiled in administrative systems defined as data banks that deal with internal agency operations such as personnel records, travel records, or parking permit records. Thirteen percent of the government's personal records are in domestic assistance program systems defined as data banks that deal with the operation of federal assistance or benefit programs. Eighteen percent of the information is contained in other data systems, including law enforcement, intelligence and financial systems.[11] The Privacy Act and exemptions six and seven in the Freedom of Information Act are, in large measure, a response to what the Congress perceived as a threat to personal privacy posed by federal collection and use of such vast aggregations of personal information.

The Freedom of Information Act

Unless the information falls within one of the statute's nine exemptions, the Freedom of Information Act requires written information possessed by federal agencies to be actively disseminated or promptly made available to any individual who requests it. The requesting party, however, must reasonably describe the material sought and comply with published agency rules concerning time, place and fees for disclosure. Exemption six permits agencies to withhold "personnel and medical files and similar

7. The phrase "accessed by personal identifiers" means information which is "retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5) (Supp. V 1975).

8. *See* OFFICE OF MANAGEMENT AND BUDGET, FEDERAL PERSONAL DATA SYSTEMS SUBJECT TO THE PRIVACY ACT OF 1974, FIRST ANNUAL REPORT TO THE PRESIDENT at 2 (1975) [hereinafter cited as OMB REPORT].

9. The Privacy Act requires agencies to publish reports on "systems of records," 5 U.S.C. § 552a(e)(4) (Supp. V 1975). That term is defined in the Act to include only those records accessed by personal identifiers. *Id.* § 552a(a)(5).

10. OMB REPORT, *supra* note 8, at 3.

11. *Id.* at 4.

files, the disclosure of which would constitute a clearly unwarranted invasion of privacy."[12] The impact of exemption six has been increased by the broad application it has been given by the courts.[13] The "medical, personnel and similar file" language has been largely disregarded in favor of a functional approach which extends the exemption to almost any information if its disclosure would constitute a "clearly unwarranted invasion of privacy."[14]

The Privacy Act

At roughly the same time that the 93rd Congress overrode President Ford's veto and enacted legislation strengthening the procedural aspects of the disclosure provisions contained in the Freedom of Information Act, the Privacy Act was passed. The Privacy Act sets detailed standards for the collection, maintenance, use and disclosure of personal information. Agencies are admonished to "collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs."[15] This provision reflects a basic tenet of privacy and fair information practice—that an individual should be aware that the government is collecting information about him.[16] The Act further requires an agency to inform the subject individual of its authority to collect such data, the purpose for collection, the routine uses, if any, for the data and the consequences, if any, of refusing to provide the data.[17]

---

12. 5 U.S.C. § 552(b)(6) (1970 & Supp. V 1975).

13. *See* Ditlow v. Shultz, 517 F.2d 166 (D.C. Cir. 1975); Wine Hobby USA v. IRS, 502 F.2d 133 (3d Cir. 1974); Rural Hous. Alliance v. Department of Agriculture, 498 F.2d 73 (D.C. Cir. 1974); Robbles v. EPA, 484 F.2d 843 (4th Cir. 1973); Getman v. NLRB, 450 F.2d 670 (D.C. Cir. 1971).

14. 5 U.S.C. § 552(b)(6) (1970 & Supp. V 1975). It should also be noted that other FOIA exemptions may affect the handling of personal information. For example, the (b)(3) exemption permits agencies to withhold information specifically exempted from disclosure by statute. At last count, some 60 federal statutes are reached by (b)(3) including several that limit the release of personal information. For instance, 26 U.S.C. § 6103 (1970) makes tax return information confidential. FOIA exemption (b)(7) which limits public access to federal investigatory records compiled for law enforcement purposes, also influences information practices for personal data. It exempts disclosures from federal investigatory records where release would "constitute an unwarranted invasion of personal privacy."

15. 5 U.S.C. § 552a(e)(2) (Supp. V 1975).

16. Limiting the application of this standard in the way that the Privacy Act does to collection of information that can be used to make adverse determinations probably makes little sense from either a conceptual or practical standpoint.

17. 5 U.S.C. § 552a(e)(3) (Supp. V 1975). Office of Management and Budget Guidelines issued pursuant to the Privacy Act interpret this section to apply only to subject individuals, but a good argument can be made that it was meant to apply to third party sources as well. 40 Fed. Reg. 28,948 (1975) [hereinafter cited as OMB Guidelines].

The statute boasts a variety of provisions designed to regulate agency organization and maintenance of personal data. Agencies must identify systems of records that are accessed by personal identifiers[18] and must publish an annual notice in the *Federal Register* describing system subjects, the kind of material on file, its routine uses and access instructions.[19] Agencies are also required to establish rules of conduct for persons involved in the design, development, operation and maintenance of systems,[20] and to establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of personal information.[21]

In addition to establishing procedural requirements for the maintenance of personal data, the Privacy Act sets substantive standards which govern the nature of personal information that federal agencies can maintain. Only personal data that is relevant and necessary to accomplish a lawful purpose can be maintained.[22] Agencies cannot maintain a record concerning an individual's exercise of first amendment rights unless they do so pursuant to statute, subject consent or an authorized law enforcement activity.[23] Furthermore, if an agency uses information from a system to make judgments about an individual, it must maintain that information with a degree of accuracy, relevance, timeliness and completeness reasonably necessary to assure a fair decision.[24]

The Privacy Act also has extensive disclosure provisions. Unlike the Freedom of Information Act which does not distinguish between disclosure to third parties and disclosure to the subject individual, the Privacy Act sets substantive standards for subject access to his records. The Privacy Act prohibits agencies from relying on the exemptions in the Freedom of Information Act to block disclosure of personal information to the subject[25] and affirmatively requires agencies to allow individuals to review their files upon request.[26] However, the Act makes blanket exceptions for access to records maintained by the Central Intelli-

18. 5 U.S.C. § 552a(a)(4)-(5) (Supp. V 1975).
19. *Id.* § 552a(e)(4)(A)-(I).
20. *Id.* § 552a(e)(9).
21. *Id.* § 552a(e)(10).
22. *Id.* § 552a(e)(1). The word "maintain" is defined to include "maintain, collect, use, or disseminate." *Id.* § 552a(a)(3). Therefore, it should be emphasized that this and other provisions that use the word "maintain" can also be considered collection standards. For a good discussion of this point, see Project, *Government Information and the Rights of Citizens*, 73 MICH. L. REV. 971, 1303 (1975).
23. 5 U.S.C. § 552a(e)(7) (Supp. V 1975).
24. *Id.* § 552a(e)(5).
25. *Id.*
26. *Id.* § 552a(d)(1).

gence Agency (CIA) and criminal law enforcement agencies.[27] It further permits any agency to withhold subject access to systems of records that contain classified data, other investigatory records compiled for law enforcement purposes, data maintained to safeguard the President, data required by statute to be used as statistical records, personnel investigatory material where disclosure would identify a source who furnished information under an express promise of confidentiality and, under various circumstances, evaluative material used to make appointment or promotion decisions in the federal service and promotion decisions in the armed services.[28]

Two additional provisions in the Act place specific limitations on a subject's access to his records. One provides that nothing in the access section shall permit an individual to see information compiled in reasonable anticipation of a civil proceeding.[29] Another provision permits agencies to establish special procedures for access to medical information including psychological records.[30]

In addition to subject access rights and limitations, the Privacy Act also permits an individual to request an agency to amend its records about him, to appeal any denials of that request and after final administrative denial, to add his own rebuttal statement to the record.[31]

As to third party disclosure, the Privacy Act's restrictions in this area necessarily interact with the Freedom of Information Act. First, the language of the two Acts must be compared. The Freedom of Information Act *requires disclosure* to the public of all information held by the government except where that information falls within one of the Act's exemptions. The Privacy Act, on the other hand, *prohibits disclosure* except where the type of disclosure sought falls within one of the Act's exemptions.[32] Exemption two in the Privacy Act permits disclosure where it is *required* under the Freedom of Information Act.[33]

Personal information will fall within the Freedom of Information Act's exemption six if its disclosure would constitute an unwarranted invasion of privacy. This determination is made by the agency itself. However, under the Freedom of Information Act, agencies have discretion to release information even if

27. *Id.* § 552a(j)(1)-(2).
28. *Id.* § 552a(k)(1)-(7).
29. *Id.* § 552a(d)(5).
30. *Id.* § 552a(f)(3).
31. *Id.* § 552a(d)(2)-(3).
32. *Id.* § 552a(b)(1)-(11).
33. *Id.* § 552a(b)(2).

it qualifies for protection under one of the exemptions. Because the Privacy Act permits third party disclosure under the Freedom of Information Act only if the Freedom of Information Act *compels* disclosure, the effect of the Privacy Act is to extinguish agencies' discretionary disclosure powers to release information under the Freedom of Information Act once such release is determined to be a clearly unwarranted invasion of privacy.

After a determination is made that disclosure of personal information to third parties is not compelled by the Freedom of Information Act, the Privacy Act and its exemptions control disclosure. Several specific types of disclosure are regulated by the Privacy Act's exemptions. For example, the Act authorizes disclosure under compelling circumstances affecting an individual's health or safety, for statistical research, to the Bureau of Census, to the National Archives, to a law enforcement agency pursuant to written request, to either House of Congress and in some circumstances its committees, and pursuant to court order.[34]

Two additional disclosure provisions deserve special mention. The Act provides for disclosure "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties."[35] Coupled with the very broad definition of an agency,[36] this provision permits agencies to share personal information within their agency virtually free of substantive or procedural checks.[37]

But perhaps the most controversial and difficult disclosure provision in the Act is the exemption which authorizes disclosure for a "routine use."[38] The Act defines a "routine use" as a use that is compatible with the purpose for which the record was collected. The legislative history indicates that the Congress settled upon the routine use formulation in an attempt to insure that the government's vital exchanges of information would continue to occur.[39] Critics have charged that as a disclosure "safety valve," the routine use has exceeded Congress' wildest dreams. It has been dubbed by many as a "routine abuse" and this report discusses its operation at length.[40]

---

34. *Id.* § 552a(b)(4)-(11).
35. *Id.* § 552a(b)(1).
36. *Id.* § 552a(a)(1).
37. Some authorities suggest that the intra-agency transfer provision is limited by standards in subsection (e)(10) which, among other things, requires agencies to establish appropriate administrative safeguards to insure the confidentiality of records.
38. 5 U.S.C. § 552a(b)(3). "Routine use" is defined in subsection (a)(7) and is required to be published under subsection (e).
39. 120 CONG. REC. H10,962 (daily ed. Nov. 21, 1974); *id.* S21,816 (daily ed. Dec. 17, 1974); *id.* H12,244 (daily ed. Dec. 18, 1974).
40. *See* text accompanying notes 159-64 *infra.*

Before concluding this background review, a few final comments need to be made about the Privacy Act's disclosure provisions. First, under the Privacy Act, disclosure of personal information even where authorized is always permissive, never mandatory. Guidelines issued by the Office of Management and Budget (OMB) properly stress this point.[41] Agencies can never directly rely on the Privacy Act as authority for a mandatory disclosure of personal information to a third party. Second, the Act requires agencies to maintain an accounting or audit log of disclosures except for intra-agency disclosures or disclosures mandated by the Freedom of Information Act.[42] Thus, individuals who wish to learn the identity of at least some of the parties that have seen their records can inspect all audit logs except for accountings of disclosures made pursuant to the Act's law enforcement disclosure exemption.[43] Furthermore, third parties who have received disclosures for which an audit trail is maintained must also receive notice of corrections or dispute notations made in a record.[44]

FINDINGS OF THE STUDY

Agency Collection of Personal Information

One of Congress' principal purposes in passing the Privacy Act was to reduce the amount of personal information collected by the executive branch. The *OMB Guidelines* emphasize the Act's collection restriction mandate.

> A key objective of the Act is to reduce the amount of personal information collected by federal agencies to reduce the risk of intentionally or inadvertently improper use of personal data. In simplest terms information not collected about an individual cannot be misused. The Act recognizes, however, that agencies need to maintain information about individuals to discharge their responsibilities effectively.[45]

But this objective does not appear to have imposed an active or voluntary change upon agencies' information collection prac-

41. Section 6 of the Privacy Act as passed, Pub. L. No. 93-579 § 6, directs the Office of Management and Budget in the Executive Office of the President to develop guidelines and regulations for agency compliance and provide continuing implementation oversight. From the outset, OMB has been reluctant to commit staff or resources to this effort. Furthermore, OMB takes a modest view of their authority to issue binding regulations for agency compliance. In the context of these restraints, most observers agreed that OMB has done an outstanding job. OMB created a temporary inter-agency task force initially to review agency Privacy Act rules; it has issued two formal sets of guidelines, published the first annual report and is presently compiling a cost report.

42. 5 U.S.C. § 552a(c) (Supp. V 1975).

43. *Id.* § 552a(c)(3).

44. *Id.* § 552a(c)(4).

45. OMB Guidelines, *supra* note 17.

tices. Instead, most officials interviewed agreed that the Privacy Act has "grandfathered in" collection activities that were underway in 1974 and 1975.

Because of the "relatively short time available to meet the requirements of the Act" many agencies simply adopted existing record systems and identified and reaffirmed collection and maintenance levels, reserving a reevaluation of their systems for a later time.[46] Although this study found few examples of actual voluntary discontinuance of significant information collection programs,[47] several agencies have purged some personal data systems and many have at least reviewed their information collection activities.

Personnel Suitability and Security Clearance Investigations

The Act has, however, had an impact in certain areas of information collection. The most frequently cited example of decreased information collection activities concerns federal personnel suitability and security clearance investigations. The alleged change in collection practices was by no means the result of a volitional determination by investigating agencies that as a result of the Privacy Act they should reduce the amount of information collected. Instead, changes were purportedly the result of restrictions imposed by the Privacy Act.

Perhaps, the Department of Defense has been the most vociferous critic of the impact of the Act in this area. One member of the Defense Privacy Board charged that,

> the impact of the Privacy Act provisions on security clearance investigations has been severe. The 'pledge of confidentiality' no longer prevails. For this reason the information submitted during security clearance investigations is less subjective in nature. The problem is of sufficient magnitude that a change in investigative techniques may result.[48]

---

46. The OMB REPORT, *supra* note 8, was helpful in evaluating some of the information gathered in this study. Although the report does not specifically address the issue of information collection, it does consider the effect of the Act upon the magnitude of personal record keeping in the executive branch. Here, as elsewhere, the line separating collection and maintenance of information is a thin one. If agencies maintain less personal information, there should be both a direct and indirect impact upon agency collection practices as reflected in the consistency between the developments reported by the Office of Management and Budget and the findings of this study.

47. The OMB REPORT indicates that 18 of the 85 agencies surveyed had reviewed and reduced the amount and nature of information retained on individuals in existing systems although they had not eliminated any system in its entirety. Eight agencies indicated that they had eliminated "information and duplicate files." Furthermore, "agencies indicated that data collection forms are being reviewed more closely to assure that only the minimum information necessary is requested." OMB REPORT, *supra* note 8, at 12.

48. Interview with Defense Privacy Board, in Washington, D.C. (July

Representatives of the Defense Investigative Service maintain that because federal investigators must now inform sources that the contents of personnel suitability and security clearance interviews are available for the subject's inspection, the quantity and quality of the information collected in these interviews have deteriorated. This development has allegedly occurred notwithstanding the fact that the Privacy Act permits agencies to deny the subject access to information that would reveal the identity of confidential sources.[49] Defense Investigative Service spokesmen admit, however, that they do not have data to document their charge and that there is no evidence that the amount of time devoted to personnel investigations has either decreased (presumably because agents are receiving fewer leads) or increased (presumably because agents must interview more sources to obtain the same amount of information).[50]

Sources at the Defense Investigative Service also claim that a growing number of sources are requesting confidential treatment of their identity.[51] A spokesman described an investigation of a nineteen year old serviceman who allegedly had a severe drug problem. Eight sources confirmed the subject's drug problem but all requested confidential treatment. Spokesmen explained that because witnesses know that the subject may gain access to his file "there is a general reluctance to be a public source."[52]

The Defense Investigative Service also experienced a mild decrease in the amount of information collected in its personnel

---

27, 1976) (by Messrs. Horton, Vargas and Brown of the Commission on Federal Paperwork). The Defense Privacy Board is an intra-agency Department of Defense organization with policy and adjudicative responsibility for administration of the Privacy Act.

49. The head of an agency may promulgate rules to exempt a system from access if the system of records is:

> investigative material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence . . . .

5 U.S.C. § 552a(k)(5) (Supp. V 1975).

50. Interview with William Cavaney, Executive Secretary, Defense Privacy Board; Colonel Aurelio Nepa, staff director, Defense Privacy Board; Robert Kelly, Director, Information Control Division, Office of the Secretary of Defense, and representatives of the Defense Investigative Service, in Washington, D.C. (Nov. 30, 1976) [hereinafter cited as Cavaney Interview]. Defense Investigative Service representatives point out that they have not attempted to collect data to document their argument.

51. The OMB Guidelines, *supra* note 17, rightfully discourage agencies from giving witnesses a promise of confidentiality. Confidential treatment of data frustrates the access provisions in the Act and substantially diminishes the utility of the interview.

52. Cavaney Interview, *supra* note 50.

and security clearance investigations and a mild increase in the number of witnesses who requested confidential treatment.[53] Defense Investigative Service District Commander Reports show, for example, that the Raytheon Corporation, among many others, now requests confidential treatment for its reports that contain derogatory or adverse employment information. One field report related that:

> [a] greater number of sources either declined to furnish information or request to be a confidential informant. During the first month of implementation of the [Privacy Act], most every agency, employer, etc. required extensive briefings before continuing to furnish information. Some declined completely, others reduced the amount of information to which they would permit access.[54]

In general, however, concerns expressed at the Department of Defense about the Privacy Act's effect on personnel investigations were not shared by officials at other investigative agencies. The prevailing view is that the Act has created few problems for those conducting investigations and examples of difficulties appear to be the exception rather than the rule.

A spokesman for the Central Intelligence Agency (CIA) noted that his agency has had little difficulty in collecting personal information and has not experienced an increase in the number of witnesses who request confidential status.[55] Although some CIA intelligence operatives apparently have complained that a few of the agency's confidential sources are more reticent since the passage of the Privacy Act and the amendment of the Freedom of Information Act, CIA sources caution that there is no way of determining if this alleged reticence is a result of the Acts or the unprecedented public scrutiny that has recently been directed at the Agency. In any event, the CIA does not have significant data pointing to a decrease in information collection activities.[56]

---

53. *E.g.*, District Commander Field Report to the Defense Investigative Service (March 16, 1976).

54. *Id.* Several field reports said that some state and local governments and private organizations initially misunderstood the applicability of the Privacy Act. They labored under the impression that they were somehow covered by the Privacy Act. Therefore, some organizations refused to disclose personal data to the federal government that they had previously supplied.

55. Interview with Gene Wilson, Privacy Act and Freedom of Information Act Coordinator, Central Intelligence Agency, in Washington, D.C. (Nov. 4, 1976) [hereinafter cited as Wilson Interview].

56. *Id.* As a single example of reduced collection, a CIA spokesman reported that some foreign intelligence agencies have informed the CIA that they are now reluctant to supply the Agency with information, including personal information, for fear that it might somehow become part of the public domain. *Id.*

At the Federal Bureau of Investigation (FBI), sources did not think that the Bureau's collection activities in personnel investigations have been affected by the collection restraints in the Privacy Act or by the disclosure provisions in the Freedom of Information Act.[57] One FBI source, however, gave an example of the Act's impact on information collection. According to the source, the FBI had made arrangements with an American businessman to attend a trade meeting allegedly organized by the Russian KGB. The FBI's informant backed out at the last minute, citing the Freedom of Information Act as his reason. The informant allegedly feared discovery of his identity because he felt that the FBI would not be able to protect the data that he would collect.

Similarly, officials at the Civil Service Commission, which performs the largest number of civilian personnel and security clearance investigations in the executive branch, do not feel that the Privacy Act affects the amount or character of information obtained in these investigations.[58] In the months immediately following the effective date of the Privacy Act, officials at Civil Service Commission headquarters received numerous complaints from field investigators that the Privacy Act restrained them from collecting sensitive and derogatory information. Headquarters review of the interview reports, however, has convinced officials that there has been no such effect. They speculate that most witnesses do not understand the Privacy Act or its consequences and therefore it is not surprising that the Act has not changed the nature of their responses.[59]

Effect on Other Information Collection Programs

Other than the alleged limited impact that the Acts may have on federal personnel and security clearance investigations, sources interviewed at a number of agencies could provide only a few examples of collection impact on other programs. At the Department of Health, Education and Welfare it was reported that officials in HEW's vocational rehabilitation programs complain they now receive less information from state provider agen-

57. Interview with Dick Dennis, FBI Special Agent, FOIA/Privacy Unit, in Washington, D.C. (Nov. 8, 1976) [hereinafter cited as Dennis Interview].

58. Interview with Robert J. Drummond, Jr., Director, Bureau of Personnel Investigations, Civil Service Commission; Walter Waldrop, Deputy Director; and Joseph Durrand, Staff Member, in Washington, D.C. (Nov. 1, 1976) [hereinafter cited as Drummond Interview].

59. *Id.* It is unwise to draw conclusions from a comparison of the Defense Investigative Service with other agencies such as the Civil Service Commission because each of these agencies conducts a separate and somewhat unique investigative program.

cies because of the Privacy Act. Many vocational rehabilitation patients receive Social Security Administration disability payments. Officials of state provider agencies have a responsibility to inform the Social Security Administration of the continuing extent of the subject's disability after the subject's completion of the state-operated rehabilitation program. Social Security Administration officials complain that because state officials know that their patients can use the Privacy Act to obtain their files, state officials are reluctant to provide information that might result in the termination or reduction of the patients' benefits.[60]

Effect on Collection from Subject

There had been some speculation that subjects themselves might be less inclined to provide agencies with information because the Act requires that they be given an explanation of the agency's authority for collecting the data and its uses for the information. The *OMB Report* states, however, that no agency reported any change attributable to this provision.

> The Act requires that individuals from whom information about themselves is solicited be apprised of the purposes for which the information is sought so that they can make an informed judgment as to whether to provide it. No agencies reported any measurable change in the willingness of individuals to provide non-mandatory information . . . .[61]

Agency sources surveyed for this study corroborated the *OMB Report* and cited only a few rather quixotic examples that suggest that individuals are now in fact more reluctant to provide information as a result of the Act's notice provisions.[62]

The study also looked for voluntary actions taken by agencies to reduce the amount of personal information that they collect. No significant examples were found. Sources at many agencies did say that the agencies have adopted a policy to reduce the amount of personal information collected. However, when pressed, they usually added that their agency had not as yet adopted any concrete or formal procedures to review the present level of information collected or to make reductions.

---

60. Interview with Edward Gleiman, Director of Fair Information Practices Staff, Department of Health, Education and Welfare, in Washington, D.C. (Nov. 3, 1976) [hereinafter Gleiman Interview].

61. OMB REPORT, *supra* note 8, at 14.

62. Interview with Robert Ellis Smith, Editor of the Privacy Journal, in Washington, D.C. (Nov. 9, 1976) [hereinafter cited as Smith Interview]. In its decennial Census test runs, the Census Bureau, for example, apparently has had difficulty with its Privacy Act disclosure notices. The Bureau has discovered that if it informs individuals as it must under the Privacy Act, that failure to reply to its questions may result in penalties, including jail, respondents are so unsettled or angry that they may refuse to answer.

Methods of Collecting Personal Information

By and large agencies have not changed their *methods* of collecting personal information. Despite the Privacy Act's prescription that information should be collected to the greatest extent practicable directly from the subject, no source was able to provide any evidence that his agency had changed its collection practices to focus more specifically upon the individual. Many of those interviewed pointed out, however, that their agency already collected the vast bulk of its personal information directly from the subject. This view of agency collection practice is shared by most expert observers.[63]

The notice requirements of the Privacy Act have had some impact upon agency collection methods. The collection notice provisions in section (e)(3) of the Act require each agency maintaining a system of records to:

> inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual—
>
> (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;
>
> (B) the principal purpose or purposes for which the information is intended to be used;
>
> (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and
>
> (D) the effects on him, if any, of not providing all or any part of the requested information . . . .[64]

The (e)(3) notice has been subject to two major criticisms. First, agency officials complain that production of (e)(3) notice forms has been expensive and burdensome. They point out that the Act, if read literally, requires Privacy Act notices even for the most inconsequential collection activities. The effect of this provision from a paperwork standpoint has been considerable. For example, at the Department of Defense, 15,000 forms require the Privacy Act's (e)(3) statement.[65] The Department of Defense decided that pending depletion of its existing stock of forms, the (e)(3) notice should be placed on a separate sheet of paper distributed with or attached to data collection forms.

---

63. Interview with Louise Becker, Analyst in Information Services, Congressional Research Service, Library of Congress, in Washington, D.C. (Nov. 18, 1976).

64. 5 U.S.C. § 552a(e)(3) (Supp. V 1975).

65. Briefing Presentation by the Defense Privacy Board to the Privacy Protection Study Commission at 15 (Jan. 16, 1976) [hereinafter cited as DPB Briefing].

Other agencies, including HEW, have adopted a similar approach.[66]

Second, agency sources charge that most subjects ignore the (e) (3) notices although those interviewed did provide a few examples of instances where subjects appeared to pay attention to the (e) (3) notice. For example, the Social Security Administration claims that the (e) (3) notice causes interviewees who are entitled to benefits to take a longer period of time to answer questions and they in turn now raise a greater number of questions.[67]

Effect on New Information Collection Programs

While agencies have not appreciably changed *existing* collection activities to comply with the Privacy Act or the amended Freedom of Information Act, there is some reason to suspect that the Acts have discouraged agencies from developing *new* information collection programs. Admittedly, it is difficult to prove this impact because there is no way to determine what new collection programs agencies would have instituted had not the Privacy Act been passed or the Freedom of Information Act strengthened. Nevertheless there are a few indications that the Privacy Act in particular has an impact on new information collection programs. Subsection o, "Report on New Systems," of the Privacy Act requires

> [e]ach agency [to] provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.[68]

OMB's *Guidelines* state that the subsection is intended to assure that proposals to establish or modify systems of records are made known in advance so that OMB and the Congress will have a

66. Interview with Edward Gleiman, Director of Fair Information Practices Staff, Department of Health, Education and Welfare, in Washington, D.C. (Dec. 13, 1976).

67. Interview with Franklin Reeder, Office of Management and Budget, in Washington, D.C. (Nov. 2, 1976) [hereinafter cited as Reeder Interview]. Mr. Reeder has been directly responsible for OMB's Privacy Act oversight activities. The Social Security Administration has been unable to document this claim. The (e) (3) notice has also caused problems at naval medical facilities. The (e) (3) notice used at these facilities was written in such a way that it created the impression that if individuals refused to sign the "acknowledgement of receipt of notice," they would not receive medical care. This misunderstanding created an uproar and the notice was subsequently reworded.

68. 5 U.S.C. § 552a(o) (Supp. V 1975).

basis for monitoring the development or expansion of record keeping activities and the Privacy Protection Study Commission will be able to review trends in the collection of personal information.[69]

As a practical matter, the new system notice requirement puts agencies on the alert that new information collection activities may be subject to close scrutiny. As such, the Act establishes a disincentive to create new systems. Sources at the Office of Management and Budget estimate that since the effective date of the Privacy Act, September 27, 1975, agencies have published approximately two hundred new system notices.[70] When this figure is compared with the nearly 7,000 initial system notices, it suggests that there is a reluctance to initiate new collection activities because of a desire to avoid the scrutinization of collection methods that the publication of new system notices might bring. An OMB official, for example, reported that the Navy had planned to conduct an extensive attitudinal study of personnel who were slated to be sent overseas. The Navy now plans to scale down the program, primarily because of external scrutiny but at least in part out of concern that collection of extensive data in this fashion would require publication of new system notices.[71]

A similar development was reported at the FBI. The Bureau has apparently considered establishing a new record system which would consist of information on known or alleged terrorists. Some of this data is already available in other FBI files, but much would have to be obtained from new collection activities. Those activities are not underway at least partly because the FBI is reluctant to create a new system of records and thereby trigger the new system notice requirements.[72]

Sources at other agencies, however, have denied that they have altered information collection plans to avoid the new system notice requirement. A CIA official stated that the Agency has fifty-seven record systems and is not reluctant to publish new system notices. According to this official, the CIA's mission and its record keeping activities are simply too important to permit essentially tangential considerations to control. Nevertheless the CIA has yet to publish a new system notice.[73]

In view of the fact that the Privacy Act places direct requirements on agency collection practices, it is surprising that it has

69. OMB Guidelines, *supra* note 17, at 28,977.
70. Reeder Interview, *supra* note 67.
71. *Id.*
72. Dennis Interview, *supra* note 57.
73. Wilson Interview, *supra* note 55.

had little impact in this area. Research indicates that agencies continue to collect the same kind and quantity of personal information; that agencies have not altered their procedures for personal information collection nor given much attention to developing plans for review of their information collection activities. Indeed, no agency official was able to produce one document that contained a program for review or restructuring of collection activities. Agencies that have changed their collection procedures as a result of the Privacy Act have limited the changes to mechanical alterations specifically required for compliance such as the (e) (3) notice.

On the other hand, the study does suggest that the Privacy Act and to a lesser extent the amended Freedom of Information Act have had two general effects on agency information collection practices. First, most agency sources were quick to emphasize that their agency has become more thoughtful about its personal data collection practices. Most officials stated that their agency was committed to an early review and reform of information collection practices. Second, this new information consciousness, when coupled with Privacy Act system notice requirements, may work to discourage initiation of new information collection programs.

Agency Handling of Information

In addition to discovering the impact of the Privacy Act and the amended Freedom of Information Act on agency collection habits, one of the principal goals of this study was to look at the impact of the Acts on the manner in which agencies *handle* personal information. At the outset it is important to clarify the scope of this discussion. The ability to define its information needs, to set priorities for data, and to use information effectively determines the success that an agency will have in achieving its goals. Naturally, I did not attempt to evaluate the ability of executive branch agencies to discharge their responsibilities or otherwise perform critical governmental functions. Rather, I looked at factors that pertain to the impact of the Privacy Act and the Freedom of Information Act on agency maintenance of personal information.

I sought to determine first, whether agencies had changed the *organization* or *content* of their files. Second, I investigated whether agencies had adopted *new and different audit procedures* in an effort to assure that their files met standards prescribed by the Acts. Third, I tried to discover whether agencies had implemented *new security procedures* for the handling of personal information. Finally, I sought to determine whether

agencies had instituted *new personnel rules and/or training programs* for the handling of personal information.

Impact of Title 44

By way of background, it is worth noting that the executive branch's maintenance of personal information is affected not only by the Privacy Act and the Freedom of Information Act, but also by a number of other statutes and sources of policy. One of the most important is title 44 of the *United States Code*. Section 3101 of that title authorizes the heads of federal agencies to compile and maintain such information as is adequate to document the agency's functions, policies and essential transactions.[74] Section 3102 requires agency heads to establish record management programs that assure effective control over the creation, maintenance, and use of records.[75] Title 44 contains, therefore, the basic statutory authority for executive agency information maintenance and retention programs.

Furthermore, title 44 authorizes the Administrator of the General Services Administration (GSA) to monitor and review executive branch information management practices. Specifically, the Administrator is directed to make surveys of record and record management practices, promote and improve the use of information, and report to the Congress and the Office of Management and Budget.[76] Section 2906 permits the General Services Administration to inspect records maintained by federal agencies.[77]

Title 44 also sets standards for information disposal pursuant to GSA coordination. Agencies are required to identify information in their possession that is no longer needed in the transaction of their business or that does not otherwise warrant preservation. Under title 44 agencies are required to submit a destruction schedule to GSA for information falling within either of those two categories.[78] The Administrator submits these schedules to Congress' Joint Committee on Printing. If the Committee has no objection, GSA then authorizes the agency to adopt the record disposal plan. Under emergency circumstances, GSA unilaterally can authorize an agency to destroy information where that data constitutes an immediate menace to health, life, or property.[79] Agencies are prohibited from disposing of any written document except pursuant to these procedures.[80]

74. 44 U.S.C. § 3104 (1970).
75. *Id.* § 3102.
76. *Id.* § 2904.
77. *Id.* § 2906.
78. *Id.* § 3302-3303.
79. *Id.* § 3310.
80. *Id.* § 3309.

Impact of Privacy Act and Freedom of Information Act

However controlling title 44 is, there is much in both the Privacy Act and the Freedom of Information Act which should have an enormous impact on agency handling of personal information. From the fact that the Freedom of Information Act makes information held in federal files public, many felt that the statute would have influence on the manner in which agencies maintain information. More specifically, because the amended Freedom of Information Act requires agencies to segregate information so that public information can be disclosed and nonpublic information appropriately protected,[81] observers believed that agencies would organize their files to reflect the public and nonpublic distinction.

At the same time, the Privacy Act contains specific directions concerning the handling of personal information. The statute requires agencies to: identify and describe systems of records that are accessed by personal identifiers; establish rules of conduct for persons involved in the operation and maintenance of the records; establish technical and physical safeguards to insure the security of the information; maintain only personal data that is relevant and necessary to accomplish a lawful purpose; and, in most circumstances, exclude from personal files information concerning that individual's exercise of his first amendment rights.[82]

Annual System Notices

The Privacy Act requires every agency to identify annually its record systems that are accessed by personal identifiers and to publish system notices in the *Federal Register* that describe the subjects in the file, the kind of material, its routine uses, and the procedures a subject can use to gain access to his record.[83] Agencies had approximately nine months from the time that the Act was passed until its effective date to undertake a comprehensive review of their personal information record keeping. Many observers hoped that a high degree of agency awareness and understanding of their record management practices would emerge from this process. Observers also thought that agencies would make significant changes in their record management practices, well beyond the specific requirements of the Privacy Act. Instead, this study suggests that agencies emerged from

81. 5 U.S.C. § 552(b) (1970 & Supp. V 1975). FOIA case law has long made it clear that agencies should segregate public and nonpublic information.
82. 5 U.S.C. § 552a(e)(4) (Supp. V 1975).
83. *Id.* § 552a(e)(4), (11).

their nine-month review period without a well defined sense of how record management practices could be reformed to improve efficiency and effectiveness or to better meet the objectives of the Privacy Act. The nine-month review process was described by sources as something of a "blitzkrieg." Officials attempted to make sense of what they perceived to be a vague and abstruse statute and a baffling amount of personal information and to describe it in system notices—all under severe time and manpower restraints. Not surprisingly, it appears that most agencies did little to change their methods of handling personal information beyond the minimum necessary for compliance with the Privacy Act.

Organization of Agency Files

Most agency sources reported that their agency had not changed its manner of organizing record systems accessed by personal identifiers. OMB officials emphasized this point after many months of reviewing agency system notices and advising agencies on implementation questions.[84]

Perhaps one reason why agencies have not reorganized their files in light of the Freedom of Information Act and the Privacy Act is that most simply have not received enough access requests to make it worth their while to do so. For example, subsection (f)(3) of the Privacy Act permits the establishment of special procedures for subject access to medical information. Most agencies have interpreted this provision to permit them to disclose medical information to a subject's physician but not to the subject directly. Therefore it would be reasonable to expect that many agencies would change their files, segregating medical information to permit subject inspection without the subject seeing the medical data. Instead, most agencies have continued to handle medical information exactly as they did prior to enactment of the Privacy Act, probably because they have received a limited number of access requests or because in some instances medical data is already segregated. It is more cost efficient to audit a file and remove medical data on an individual access basis than to initiate a wholesale reorganization of the system.

Although some agencies are faced with numerous requests from individuals interested in viewing their files, they have found it unnecessary to reorganize their systems. Sources at a number of agencies, particularly those in the intelligence and criminal justice communities, said that files in their agencies have always been carefully organized according to proper record

84. Reeder Interview, *supra* note 67.

management procedures and agency needs, so that there has been no need to reorganize the files.[85] Furthermore, officials point out that under the Act their files can be exempted from many requirements such as relevance, timeliness, etc., that would logically lead an agency to consider restructuring its files.

Minor Changes

The findings of the study show that a few agencies have made minor changes in the organization of their files in a constructive attempt to meet the requirements of the Acts. The Civil Service Commission has altered the form of investigative reports used in personnel and security clearance investigations. Because the Privacy Act permits witnesses to request confidential treatment of any information that would reveal their identity, the Commission restructured its reports so that witness identification information could not be viewed by the subject. Prior to enactment of the Privacy Act, investigative reports were organized to commingle the witness' evaluation of the subject with the witness' biographical data. Reports have now been reorganized so that one section is devoted exclusively to an identification of the witness and a second section is devoted exclusively to subject evaluation.[86]

Similarly, other agencies segregate files to separate public and nonpublic information. In particular, agencies that collect substantial amounts of business data and are therefore subject to frequent requests pursuant to the Freedom of Information Act, have adopted filing schemes under which information is classed and filed as public or nonpublic at the point of collection.[87] The Federal Trade Commission and the Food and Drug Administration have adopted variants of this filing system. The Office of Civil Rights at HEW and the Justice Department reportedly use this approach to a limited extent.[88] A few sources

85. Interviews with officials at the CIA, FBI and Defense Investigative Service, *supra* notes 55, 57 and 50 respectively.

86. Drummond Interview, *supra* note 58, and interview with Phillip Schneider, Associate Director for Manpower Information, Civil Service Commission, in Washington, D.C. (Nov. 5, 1976) [hereinafter cited as Schneider Interview].

87. Interview with Jack Schwartz, Staff Attorney, Office of the General Counsel, Federal Trade Commission, in Washington, D.C. (Dec. 8, 1976) [hereinafter cited as Schwartz Interview]; interview with Jeffrey Edelstein, formerly an attorney in the General Counsel's Office at the Federal Trade Commission and now the Chairman of the Federal Bar Association's Committee on Government Information and Privacy, in Washington, D.C. (Dec. 3, 1976); interview with Thomas Susman, Chief Counsel, Subcommittee on Administrative Practice and Procedure, Senate Committee on the Judiciary, in Washington, D.C. (Nov. 8, 1976) [hereinafter cited as Susman Interview].

88. *See* note 87 *supra*; Smith Interview, *supra* note 62.

speculated that the organization of information to accommodate access requests (such as segregating medical information, third party data, confidential source data, removing irrelevant or untimely data, etc.) was the intelligent approach and one which eventually many agencies would surely adopt.

Purge of Systems

Many observers had great expectations that the Privacy Act and the amended Freedom of Information Act would induce agencies to purge existing systems. The *OMB Report* suggests that, although most agencies have not significantly reduced the amount of personal information that they maintain, at least some have eliminated a few personal record systems.[89] In addition, sources at many agencies said that the Privacy Act has encouraged their agency to destroy information. Agency officials, however, could not point to anything substantial to document this claim. It was noted that although the Act does give agencies an incentive to reduce the amount of personal data in their files, natural bureaucratic instincts to maintain data, coupled with the provisions in title 44, make it extremely difficult for an agency to destroy information.[90]

A couple of officials reported that their agency had recently applied to and received approval from the Archives for new and shorter purge schedules. Officials at the Defense Investigative Service reported that a new purge schedule had been adopted with shorter time periods for the destruction of personal information.[91] The FBI has also apparently changed its purge schedule. The Bureau now destroys misdemeanor information after ten years and felony conviction information after twenty years. Previously the FBI had maintained such data indefinitely. Whether this change is a consequence of the Privacy Act, the FBI's recent public exposure, or a combination of both, is difficult to determine.[92] The FBI, as well as the CIA and the IRS have testified that they would like to purge a number of record systems including several containing especially sensitive political and first amendment data, collected as a part of their COINTELPRO CHAOS and SPECIAL SERVICES PROJECTS, respectively.[93]

---

89. OMB REPORT, *supra* note 8, at 12.
90. Interview with Mary Lawton, Deputy Assistant Attorney General, Office of Legal Counsel, Department of Justice, in Washington, D.C. (Nov. 3, 1976) [hereinafter cited as Lawton Interview].
91. Cavaney Interview, *supra* note 50.
92. Dennis Interview, *supra* note 57.
93. Congress placed a moratorium on the destruction of these records pending further evaluation of the data banks.

The Civil Service Commission reportedly purged a few record systems containing personal data systems in anticipation of the effective date of the Privacy Act.[94] For example, prior to enactment of the Privacy Act, the Commission maintained a file of newspaper clippings on selected individuals. This file system has now been eliminated. The Civil Service Commission also previously maintained a system with information that appraised the promotion or potential of selected employees. This system was likewise destroyed and such data is reportedly no longer developed by the Commission.[95]

Changes to Circumvent Acts

Some agencies have reorganized their files in an effort to subvert or avoid Privacy Act requirements. It has been reported that particular organizations no longer file certain sensitive information in record systems that are identified by personal information. Record systems which are not identified by data personal to the subject are not covered by the Privacy Act. Instead the Act covers information about an individual maintained in a system of records that is *accessed* by personal identifiers. Critics point out that permitting the Act to be turned on and off by the method of access is an open invitation to agencies to circumvent the Act.[96]

Another device used by agencies to avoid Privacy Act requirements is the creation of temporary or informal files. Material that should be placed in permanent files (and that was previously contained in such files) is now maintained informally and/or temporarily to avoid the creation of files subject to Privacy Act regulation. The Department of Justice, for example, no longer has a file for attorney applicants. Instead, resumes and related correspondence are maintained in an informal manner, shuffled from desk to desk and then destroyed when no longer needed.[97]

---

94. Schneider Interview, *supra* note 86.
95. *Id.*
96. Lawton Interview, *supra* note 90. Most sources were naturally reluctant to identify specific examples of personal information that had been hidden in systems not accessed by personal identifiers. Nevertheless, there are reports, for example, that merit promotion files at the Civil Service Commission are now maintained in systems that are not accessed by personal identifiers. Another example is the Department of Justice's access request log, which contains the names of individuals who have accessed information in files that are covered by the Act. The access request log is organized so as not to be accessed by personal identifiers.
97. *Id.* The Privacy Act does not make an exception for temporary or informal files except to the extent that such a file is not "under the control" of the agency. 5 U.S.C. § 552a(a)(5) (Supp. V 1975).

Observers further charge that law enforcement agencies are keeping information in open investigatory files after an investigation is terminated. This practice avoids the disclosure requirements of the Freedom of Information Act because an exception permits agencies to withhold information in investigatory files where disclosure would compromise an enforcement proceeding.[98] There has also been an alleged increase in agency use of oral communication. Agencies may be using oral communications to exchange some information that would previously have been exchanged and memorialized either exclusively or additionally in written form. The Department of Labor has reportedly instructed its Office of Safety and Health Administration to communicate orally with the subjects of its investigations when possible.[99] According to one source, the Federal Deposit Insurance Corporation recently distributed a memorandum to its employees advising them that they should attempt, where possible, to communicate on the telephone instead of in written form.[100] Although the memorandum did not say so, one reason for this recommendation may have been to avoid the creation of written information that would be subject to the requirements of both the Privacy Act and the Freedom of Information Act.[101]

One of the most interesting examples of potential changes in agency handling of information is the formation of so-called "data havens." There is some reason to believe that federal agencies may "hide" data, including personal information, in systems maintained by organizations that are not subject to the Privacy Act or the Freedom of Information Act. In many instances this information would have been maintained by the agency itself prior to enactment of the statutes. For example, it is reported that HEW personnel no longer accept possession of copies of General Accounting Office audits, but instead travel to the offices of the General Accounting Office (an arm of the Congress not covered by the Acts) to look at information that HEW normally would have maintained in-house.[102] The extent of the "data-haven" development could not be documented in this study, but insofar as the executive branch is subject to standards that are more rigorous than those applied to other organizations, agencies have an incentive to look for such havens.

---

98. 5 U.S.C. § 552(b)(7)(A) (1970 & Supp. V 1975).
99. Susman Interview, *supra* note 87.
100. *Id.*
101. Interestingly, the disclosure provisions in the Privacy Act cover any method of communication. 5 U.S.C. § 552a(b) (Supp. V 1975).
102. DOMESTIC COUNCIL COMMITTEE ON THE RIGHT OF PRIVACY, NATIONAL INFORMATION POLICY: REPORT TO THE PRESIDENT at 51-52 (1976).

Auditing of Files

Neither the Privacy Act nor the Freedom of Information Act specifically requires agencies to audit files containing personal information. Nevertheless, along with the reorganization of files, many observers expected agencies to implement audit programs to help insure that their personal information systems met standards in the Acts. It appears, however, that no such development has occurred.[103]

The consequence of failing to audit files properly was recently brought to the attention of two executive branch agencies. Six Fort Riley soldiers have brought suit against the Department of Defense for its alleged failure to maintain their personal records with the accuracy, relevance, timeliness and completeness necessary to insure that fair decisions can be made.[104] In *Emory v. Laise*, an aggrieved subject has instituted suit against the Department of State, charging that files maintained on the plaintiff contained "erroneous and scandalous matererial in violation of the Privacy Act."[105]

Only a few officials reported that their agency had adopted any new audit procedures as a result of the Act. The Civil Service Commission has undertaken a comprehensive audit program to expunge information in its files concerning subject exercise of first amendment rights. However, the program only applies to "archival" files from which information is about to be used. The opinion of the Civil Service Commission's General Counsel describes the scope of the program:

> Finally, we concur in your proposal to screen investigative files assembled before the effective date of the Privacy Act for impermissible information at the time they are released rather than immediately. Technically speaking, these old files are 'maintained' by the Commission. However, they are maintained as archives and not as current files in an active operating system. To the extent that they are inactive or purely archival, there is no real need to screen them, until such time as they are released or reactivated for some purpose other than archival.
>
> Because these files are in storage and not used, i.e., not 'maintained for active use,' there is little or no chance that the information contained in them will be misused. The potential of such misuse is the actual basis for the Act's embargo on 'maintaining' First Amendment related information. We recommend then, that a procedure be established to systematically screen all investigative files retrieved from the Commission's storage banks and to expurgate all proscribed information from those files.[106]

---

103. Reeder Interview, *supra* note 67.
104. Topeka Kansas Journal, April, 1976.
105. 421 F. Supp. 91 (D.D.C. 1976).
106. Memorandum from Carl F. Goodman, General Counsel to Robert

The Civil Service Commission has requested a $500,000 authorization in the Commission's budget to conduct this audit program.[107] According to staff sources, even this kind of limited audit involves the commitment of substantial manpower by executive level employees.[108]

The Department of Defense has added Privacy Act criteria to its Inspector General's audit program. The Inspector General's office performs an annual audit of Department of Defense performance and, since 1975, the review has included a determination of whether information in systems covered by the Act, is timely, accurate and relevant. Inspector General evaluations are conducted once a year on a spot check basis and Department of Defense spokesmen do not claim that these investigations constitute an in-depth evaluation of the Department's compliance with the Privacy Act.[109]

In general, the study discovered that auditing is given a low priority by federal agencies. Possibly, the absence of specific audit requirements in the Acts makes it difficult for agencies to commit resources to the effort. It may also be that the Act's requirement that files be maintained with a degree of accuracy, relevance and timeliness requisite to the making of a fair decision, is a standard simply too vague and subjective to mean much to agency record keepers. In any event, at present it appears that agencies only audit files (if at all) immediately prior to access by the subject or release to third parties.

Security

One of the Privacy Act's primary considerations for the handling of personal information is the physical, administrative and technical security of the system. If "confidentiality" is the promise to keep personal information from falling into the public domain, then security is an organization's ability to keep that confidentiality promise. Subsection (e) (10) of the Privacy Act requires agencies to "establish appropriate administrative, technical and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could

---

J. Drummond, Jr., Director, Bureau of Personnel Investigations on Protection of First Amendment Rights Under the Privacy Act (Nov. 7, 1975).

107. Reeder Interview, *supra* note 67.

108. Drummond Interview, *supra* note 58. Approximately one-half of the time of the Director and Deputy Director of the Bureau of Personnel Investigation at the Civil Service Commission is devoted to Privacy Act matters, a substantial part of which includes the first amendment audit program.

109. Cavaney Interview, *supra* note 50.

result in substantial harm, embarrassment, inconvenience or unfairness to any individual on whom information is maintained."[110]

In view of this specific mandate, together with the increased awareness of the sensitivity of personal information, the fact that many systems are protected by such simplistic physical security measures as locked filing cabinets and doors, and the government's failure to use sophisticated, technical means to safeguard computer data,[111] many observers expected wholesale changes in agency security procedures. Here too, it appears that compliance efforts have fallen short. In general, sources believed that prior to the enactment of the Privacy Act, security procedures for systems containing personal information were already more than adequate. The *OMB Report* describes the feeling of most agency officials:

> Agency reports indicate that they have been able to develop physical and administrative safeguards for systems subject to the Act. Eight agencies indicated that no new safeguards were necessary beyond giving specialized instructions to personnel. Fifty-five agencies outlined security procedures, although not all identified them as new procedures established in response to the Act. For example, many agencies cited security measures such as bolting, guards, lockable rooms and cabinets and limited access to records, safeguards which in many cases were in existence before September 27, 1975. Most agencies apparently concluded that security safeguards already in place augmented by increased staff awareness of the need for safeguarding personal information are adequate to meet the requirements of the Privacy Act for the majority of systems which they maintain.[112]

Consequently, little has been done to improve security and most agencies apparently did not closely review security systems prior to making the determination that they were adequate.

A few agencies, however, have taken specific action to implement the Privacy Act's security standards. The Department of Defense has reworked its procedures, making changes in security measures for new automated systems.[113] HEW has also done work in this area, establishing a task force to examine security questions for all systems containing personal information, focusing initially on automated systems.[114] For the moment, however, it appears that security procedures have changed little since the passage of the Privacy Act.

---

110. 5 U.S.C. § 552a(e)(10) (Supp. V 1975).
111. OMB REPORT, *supra* note 8, at 16. *See also* Turn, *Privacy and Security in Centralized Versus Decentralized Databank Systems*, 7 POL'Y. SCI. 17 (1976).
112. OMB REPORT, *supra* note 8, at 15.
113. DPB Briefing, *supra* note 65, at 18.
114. Gleiman Interview, *supra* note 60.

Personnel Rules

If the executive branch in fact altered significantly its method of collecting, handling or disseminating personal information, it was believed that the change would manifest itself in new personnel rules and training programs. The Privacy Act, subsection (e) (9), requires agencies to:

> establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or maintaining any record, and instruct each such person with respect to such rules and requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance.[115]

Pursuant to this directive, the Civil Service Commission revised the *Federal Personnel Manual* to include changes in personnel record keeping practices required by the Privacy Act.[116] Additionally, it has issued regulations governing personnel security investigations under the Privacy Act,[117] has conducted a training course on the Privacy Act for federal employees and specific personnel and has developed a two-day general course that is available to most federal agencies.[118]

The Department of Defense has also undertaken a major effort to meet the concerns of subsection (e) (9). It has budgeted $2.4 million to train personnel over a period of twelve to eighteen months[119] and has issued Training Reg. 5400.11 which sets out the substance of the training program.[120]

Other than the Department of Defense and the Civil Service Commission, however, it appears that few agencies have implemented new personnel rules or programs to govern employees who handle personal information.[121] It is worth noting that the Department of Justice which enforces the Freedom of Information Act has done little to encourage the implementation of training programs to effectuate compliance with the Act. Indeed, the Attorney General's Freedom of Information Act implementation memoranda in 1967 and 1974 are viewed by many

---

115. 5 U.S.C. § 552a(e)(9) (Supp. V 1975).
116. 40 Fed. Reg. 45,904 (1976).
117. 40 Fed. Reg. 56,651 (1976).
118. OMB REPORT, *supra* note 8, at 10-11; Schneider Interview, *supra* note 86.
119. Interview with William Cavaney, Executive Secretary, Defense Privacy Board, in Washington, D.C. (Dec. 9, 1976) [hereinafter cited as Cavaney Interview #2].
120. For an early discussion of this training program, see DPB Briefing, *supra* note 65, at 13-25.
121. The FBI claims that it has changed its internal training program to emphasize Privacy Act concerns, but no written evidence was supplied.

observers as negative and unhelpful statements that in fact discourage agency compliance.[122]

Access to and Dissemination of Government-held Personally Identifiable Information

There is no information policy issue more significant than that of public access to government-held personally identifiable information. Decisions controlling access to such information shape the relationship of individual and government. Today there is general agreement that increased public access to *most* kinds of government-held information develops a well-informed electorate, promotes trust in government, and improves governmental responsiveness and integrity. There is also general agreement that personal information should be treated as an exception to an open door policy of public access. But once beyond affirmation of such vague principles, there is sharp disagreement over the extent to which personal information should be available to the public.

The dissemination and access issues are discussed under four headings: (1) the Privacy Act's system notice requirement; (2) access requests; (3) intra- and inter-agency transfers of information within the federal government; and (4) the flow of information to and from state and local governments and private sector organizations.

System Notices

The Privacy Act requires agencies to publish annually a notice of the existence and character of their record systems.[123] System notices are descriptions of each record system that an agency maintains detailing, for instance, the categories of individuals covered by the system, its purposes and its routine uses.[124] The public notice requirement is crucial to the primary purposes of the Act—elimination of *secret* record systems containing personal information and agency accountability through a system of public scrutiny.[125]

The annual system notice requirement constitutes an impressive and perhaps the major paperwork burden placed upon agencies by the Privacy Act. The first batch of annual notices, pub-

122. Interview with Harold Reylea, Freedom of Information Act Specialist at the Congressional Research Service, in Washington, D.C. (Nov. 18, 1976).
123. 5 U.S.C. § 552a(e)(4)(A)-(I) (Supp. V 1975).
124. For examples of system notices see the Department of the Treasury's notice publication in 40 Fed. Reg. 37,602-37,910 (1974).
125. 40 Fed. Reg. 28,948 (1975).

lished for the most part in August and September of 1975, consumed over 3,200 pages of small print in the *Federal Register.*

Unfortunately, however, the system notice requirement has been relatively ineffective. There is widespread belief throughout the federal bureaucracy that members of the public neither read nor have general access to the *Federal Register.* Apparently, therefore, individuals who make access requests seldom, if ever, base their requests upon information obtained from the *Federal Register.* The CIA, for example, reported that out of almost 5,000 access requests, only nine used system notice or request format information found in the *Federal Register* to make the request.[126]

Perhaps because of the public's unfamiliarity with the *Federal Register*, one "information entrepreneur" recently established a Privacy Act access request service. For $15.00, Freedom of Information Services, Inc., will file an access request and follow-up request with any one of about a dozen federal agencies.[127]

Access Requests

Role of the Freedom of Information Act

Despite the apparent lack of interest in or knowledge of system notices, there is no doubt that since the adoption of the Privacy Act and the amendment to the Freedom of Information Act, the number of access requests received by federal agencies has increased dramatically. The Freedom of Information Act provides that written information that cannot be sheltered from distribution by one of the Act's nine exemptions must be made available to *any* individual who requests it, provided that the requesting party reasonably describes the material and complies with published rules concerning time, place and fees for the disclosure.

Short and strict time limits govern agency response to access requests. The government must determine whether to comply with the request within ten working days and must promptly notify the requesting party of its determination. If an application is rejected, the individual has the right to one administrative appeal which must be determined within twenty working days.[128] Under unusual circumstances, agencies may extend

126. Wilson Interview, *supra* note 55.
127. *See Use Abuse of Freedom of Information Act*, Washington Post, July 27, 1976.
128. 5 U.S.C. § 552(a)(6)(A)(i)-(ii) (1970 & Supp. V 1975).

the ten and twenty day time limits, but in no event may the delay exceed ten additional days.[129]

Information may be withheld only if the data comes within one of the Freedom of Information Act's nine exemptions. No other legal grounds exist upon which to base a refusal.[130] But the exemptions are permissive, and therefore, unless otherwise restrained, agencies are free to ignore the availability of an exemption and to release the data.[131] Cases reflect this discretion in holding that the exemptions must be narrowly construed and ambiguities resolved in favor of disclosure.[132] Critics, however, charge that agencies tend to withhold information mechanically where an exemption will apply without determining if there is any particular reason why that information should be withheld *despite* the availability of the exemption.[133]

Freedom of Information Act applicants whose requests are rejected on administrative appeal may seek a district court order compelling the production of the documents. Unless given additional time by the court, agencies must answer Freedom of Information Act complaints within thirty days. Courts look at the requests de novo and the burden is squarely upon the government to justify nondisclosure.[134] If the court finds for the complainant, it can award court costs and attorney's fees.[135] Moreover, if the court finds that agency personnel acted arbitrarily or capriciously in withholding the information, it can direct the Civil Service Commission to initiate an investigation to determine whether disciplinary action is warranted.[136] To date, however, neither the courts nor the Civil Service Commission have shown much enthusiasm in exercising this disciplinary authority.[137]

---

129. *Id.* § 552(a)(6)(B).

130. *See* Rabbitt v. Department of the Air Force, 383 F. Supp. 1065 (S.D.N.Y. 1974). There is much debate among legal scholars concerning the availability of the executive privilege doctrine as a discrete authority for withholding documents.

131. Moore McCormack Lines, Inc. v. I.T.O. Corp., 508 F.2d 945 (4th Cir. 1974).

132. Literally dozens of decisions have adopted this interpretation. *See, e.g.*, Ditlow v. Shultz, 517 F.2d 166 (D.C. Cir. 1975); Cuneo v. Schlesinger, 484 F.2d 1086 (D.C. Cir. 1973); Soucie v. David, 448 F.2d 1067 (D.C. Cir. 1971); Sears, Roebuck & Co. v. GSA, 384 F. Supp. 996 (D.D.C. 1974), *aff'd*, 509 F.2d 527 (D.C. Cir. 1974).

133. Interview with Mark Lynch, Attorney for Freedom of Information Clearinghouse, in Washington, D.C. (Dec. 14, 1976) (by Phillip Vargas of the Commission on Federal Paperwork) [hereinafter cited as Lynch Interview].

134. *See* Seafarers International Union AFL-CIO v. Baldovin, 508 F.2d 125 (5th Cir. 1975); Washington Research Project v. HEW, 504 F.2d 238 (D.C. Cir. 1974), *cert. denied*, 421 U.S. 963 (1975).

135. 5 U.S.C. § 552(a)(4)(E) (1970 & Supp. V 1975).

136. *Id.* § 552(a)(4)(F).

137. Lynch Interview, *supra* note 133.

Role of the Privacy Act

As noted in the background section, the Privacy Act prohibits disclosure of personal information except to the subject individual or with the subject's written consent or where the disclosure falls within one of the Act's exemptions. Since one exemption permits disclosure when it is required by the Freedom of Information Act, access request procedures found in that statute may be followed. Additionally, some of the Privacy Act exemptions set forth minimal access request procedures for disclosure to third parties. For instance, disclosures to a government agency for a civil or criminal law enforcement activity must be pursuant to written requests specifying the particular portion of the record that is needed.[138]

However, the Privacy Act's access request procedures are most detailed with regard to subject individual requests. The Privacy Act provides that each agency that maintains a system of records shall:

> upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.[139]

The Act provides civil remedies for a wrongful refusal to comply with a subject individual's access request and empowers the courts to enjoin the agencies from withholding the requested information. In such a case the court is to consider the request de novo and in camera to determine whether there are grounds in the Act for withholding the record or portions of it from the subject individual. Attorney's fees and other reasonable litigation costs may be recovered when the complainant prevails in such a suit.[140]

The Act also provides specific procedures to be followed for subject individual requests to amend the record and insert rebuttal statements. Agency review and civil remedies are available to the subject individual for the wrongful refusal to comply with such requests.[141]

---

138. 5 U.S.C. § 552a(b)(7) (Supp. V 1975).
139. *Id.* § 552a(d)(1).
140. *Id.* § 552a(g)(3)(A)-(B).
141. *Id.* § 552a(d)(2)-(3), (g)(1).

Individual Deluge of Access Requests

By the effective date of the Privacy Act, many agencies, particularly those in the criminal justice, intelligence and regulatory communities, were inundated with access requests from private individuals. An initial wave of access requests overwhelmed some agencies and created grave processing difficulties for many others. During 1975, for example, the CIA received 6,609 access requests.[142] The Justice Department received 30,000 requests of which 14,478 were addressed to the FBI.[143] The Department of Treasury, including the IRS received another 30,000 requests.[144] By summer of 1976, the CIA had a backlog of 2,400 requests. At the FBI, the backlog ran as high as 8,400 requests and created processing delays of nine months.[145]

The Justice Department, in its Freedom of Information Act report to the Congress, complained that the deluge of access requests threatened to compromise the Department's ability to perform its substantive missions.

> In reviewing all of the data submitted herewith, I must state that much of it is disturbing to me and others interested and involved in FOIA matters. The receipt of over 30,000 requests for access, a number far in excess of what anyone had anticipated, has transformed this into a major area of departmental operations. Over 120,000 manhours are reported as having been expended, the majority by attorneys and supervisors, and these constitute only a partial accounting for the total personnel effort within the Department. These figures demonstrate the adverse impact on this Department's ability to carry out its traditional substantive missions during the past year. Moreover, the figures for the first two months of 1976 offer no indication that the tide is ebbing. Through March 5, for example, the Federal Bureau of Investigation has received in excess of 2,500 new requests for access to its records.[146]

Number of Access Requests Declining

By the fall of 1976 interviews conducted for this study indicated that the number of requests had decreased at both the CIA

142. *Freedom of Information Act: Burdensome, Costly, Much Used,* Washington Post, July 25, 1976. Most agencies do not distinguish FOIA and Privacy Act access requests. The requestor is given the greatest amount of information that he is entitled to under both Acts.

143. *Id.*

144. FOIA ANNUAL REPORT (1976).

145. *Id. See also FBI Slow to Free Information,* Washington Post. July 30, 1976; *Demands of FOIA and Privacy Act on the FBI: Hearings of the Civil and Constitutional Rights Subcommittee of the House Committee on the Judiciary,* 94th Cong., 2nd Sess. 2 (1976) (statement of James M. Powers).

146. Letter from Harold R. Tyler, Jr., Deputy Attorney General, Department of Justice to Bella S. Abzug, Chairwoman, Government Information and Individual Rights Subcommittee of the House Committee on Government Operations (March 15, 1976).

as well as the FBI. At the CIA, access requests that had been running as high as 100 per day had dropped to an average of ten per day by November of 1976.[147] The FBI reported a somewhat smaller decline. Unlike officials at the CIA, FBI sources, however, are not optimistic about the future curve for access requests.[148] The FBI also reports that its access request load is extremely sensitive to publicity. For instance, shortly after CBS Network News featured a Freedom of Information Act story, the FBI received 1,042 access requests in a single day.

Agencies outside the criminal justice and intelligence communities generally report that they are able to process their access request load with little difficulty. For example, both the Department of Defense, with an estimated 44,400 access requests in 1975, and the Civil Service Commission, which is currently averaging ten access requests per day, indicate that they are well able to process this flow.[149] Indeed, in some agencies, the number of access requests has been almost disturbingly small. The *OMB Report* describes the typical agency experience:

> most agencies have not reported a substantial number of requests. Those agencies which have reported perceptible increases in requests for access to records are for the most part engaged in law enforcement/investigative activities (*e.g.*, IRS and FBI). They have been unable, however, to segregate requests for access as a result of the Privacy Act from those resulting from the Freedom of Information Act. Agencies' reports other than those from the law enforcement agencies indicate that most requests for access were being made by Federal employees. This tends to support the assertion that the public at large was not aware of mechanisms established by the Act during the first months after it became effective, and that Federal employees are more informed as a result of extensive training given them incident to implementing the Act.[150]

Agencies that attempt to distinguish Freedom of Information Act and Privacy Act requests find that the number of requests pur-

147. Wilson Interview, *supra* note 55.

148. Many observers believe the Department of Justice and particularly the FBI have a degree of concern, if not hostility, for the Privacy Act not found at other agencies. However, in fairness to the Bureau it should be pointed out that congressional staff members responsible for FBI oversight argue that the Bureau's recent efforts to comply with FOIA and the Privacy Act have been sincere and effective. Interview with Alan Parker, Chief Counsel, Subcommittee on Civil and Constitutional Rights, House Committee on the Judiciary, in Washington, D.C. (Jan. 21, 1977). Publicly and privately, Justice officials complain that the Acts cause interference, frustration and loss of morale within the Bureau. They cite, for example, the celebrated FOIA request for access to the Rosenberg spy case files. Compliance with the request cost the Bureau over $261,000. To date the Rosenberg children have not bothered to inspect the documents. Dennis Interview, *supra* note 57; Lawton Interview, *supra* note 90.

149. Cavaney Interview #2, *supra* note 119; Drummond Interview, *supra* note 58; Schneider Interview, *supra* note 86.

150. OMB REPORT, *supra* note 8, at 15.

suant to the Privacy Act in particular has been low. For example, the FTC reports that it has processed only 200 Privacy Act requests since the effective date of the Act, almost all of which were from employees and were handled promptly and amicably.[151]

Agency Overreaction

Passage of the Privacy Act and the amendment to the Freedom of Information Act undoubtedly permits individuals to obtain more personal information from their federal files. It is unclear, however, if the Acts have changed the nature or the amount of personal information that executive agencies release to the public generally.[152] Initially, in an attempt to avoid violations of the Act, agencies relied upon withholding provisions under both statutes and may have released less information in certain areas than they normally do.

During 1975, executive branch agencies relied on the privacy exemption in the Freedom of Information Act 3,856 times to withhold personal information.[153] Observers report that the Department of Justice is reluctant to discourage agencies from using Freedom of Information Act exemptions for fear that agencies will complain to Congress.[154]

In addition to reliance on the Freedom of Information Act's exemption to withhold personal information, some agencies, particularly in the first months after enactment of the Privacy Act, may have relied improperly upon the Privacy Act to deny individuals access to information that previously had been public. The *OMB Report* describes this phenomenon:

> Another key objective of the Act is to assure that personal information is not used for purposes other than those for which the information was collected without the consent of the individual to whom the information pertains. This provision and the complex set of criteria under which information may be released

151. Schwartz Interview, *supra* note 87.

152. A fear expressed by critics is that under the crunch of access requests agencies will inevitably release sensitive information that ought to be protected. So far only one such occurrence has been documented. The IRS apparently improperly released over 90 pages of law enforcement investigatory documents to an indicted Chicago lawyer allegedly involved in a $700,000 tax evasion scheme. *See Too Much FOIA at IRS*, Washington Post, July 28, 1976. In a related phenomenon, FBI officials point out that over 10% of their access requests come from inmates in various penal institutions. They fear that one result of providing this data to inmates is that inmates may discover the Bureau's *modus operandi* in investigating criminal cases.

153. *See* Harold C. Reylea, The Administration of the Freedom of Information Act: A Brief Overview of Executive Branch Annual Reports for 1975 (Sep. 2, 1976).

154. Lynch Interview, *supra* note 133.

> without the consent of the individual initially caused substantial confusion and operational problems.[155]

A newspaper story carried by the Washington Bureau News Service illustrates the initial overreaction to the Privacy Act.

> A State mental hospital official won't tell a worried son that his missing mother has been checked into the hospital. Sorry Privacy Act. A policeman won't tell a lawyer whether his client has been arrested. Sorry Privacy Act. A school official won't tell the local newspaper who plays the kazoo in the school band. Sorry Privacy Act. The Secret Service won't release the list they have compiled of public court actions. Sorry Privacy Act. All over the country the Privacy Act is being invoked by various officials in and out of government as a reason for not releasing information, information which has often formerly been available to the public.[156]

Another story carried by the wire services during this period described a State Department lawyer who delayed publication of the Department's biographical register of foreign service agents because he feared that disclosing directory information would violate the Privacy Act.[157]

Intra- and Inter-Agency Transfer of Information

Abuse of Routine Use Provision

Under the Privacy Act inter-agency transfers of sensitive personal information may be accomplished pursuant to a routine use notice. The routine use concept does not pertain to the frequency or normalcy of a transfer but rather looks to the compatibility of the use. Information falls within the Privacy Act's routine use exemption and may be exchanged by agencies if it is to be used for a purpose which is compatible with the purpose for which the information was first collected,[158] provided that the agency possessing the information has published an appropriate routine use notice. Under these circumstances a transfer may be made even though the subject has not consented to the transfer and even though the information, if disclosed to the public, would constitute a clearly unwarranted invasion of privacy. As such, the routine use concept represents a compromise. It attempts to reconcile agencies' need to share sensitive personal information with the Congress' desire to limit sharply the transfer of such information and, indeed, to give the individual subject control over such transfers.

---

155. OMB REPORT, *supra* note 8, at 12-13.
156. *Sorry, Privacy Act Standard Answer from Officials*, Oklahoma City, Oklahoman, March 28, 1976.
157. *Privacy Act provides bureaucratic field day*, Aberdeen South Dakota American News, Jan. 26, 1976.
158. 5 U.S.C. § 552a(b)(3), (a)(7).

> In discussing the final language of the Act, Senator Irvin and Congressman Moorhead in similar statements said that '[t]he compromise definition should serve as a caution to agencies to think out in advance what uses it will make of information. This Act is not intended to impose undue burdens on the transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to other persons or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.'[159]

Initially, overreaction and misunderstanding created problems for some agencies in implementing the routine use provision. The Civil Service Commission, for example, had difficulty persuading other agencies in the executive branch to send personnel files that it was *required* to obtain.[160]

Throughout the federal bureaucracy, however, there is agreement that the routine use requirement has not imposed a significant burden upon information exchanges. Interviews for this study suggest that the difficulty may have been alleviated in part, by the development of techniques designed specifically to circumvent the routine use restrictions. Many routine use notices authorize transfers of information for purposes which by no stretch of the imagination are compatible with the purpose for which the information was first collected.

On June 5, 1975, the Department of Justice sent a memorandum to heads of all executive departments and agencies requesting that each agency publish a routine use notice authorizing the transfer of information to a law enforcement agency where the information indicates a violation or potential violation of law.[161] In the same memorandum, the Attorney General encouraged agencies to publish routine use notices for the transfer of information to agencies conducting employment and security clearance investigations. Department of Justice sources readily admit that there is no way such uses, now adopted by almost every federal agency, comport with the Act's definition of a routine use.[162]

---

159. OMB Guidelines, *supra* note 17, at 28,953 (citing 120 CONG. REC. S21,816 (daily ed. Dec. 17, 1974); *id.* H12,244 (daily ed. Dec. 18, 1974)).

160. Schneider Interview, *supra* note 86.

161. *See* Memorandum from the Attorney General to the heads of all executive departments and agencies, Office of the Attorney General, Washington, D.C. on the Implementation of Privacy Act of 1974 Routine Uses of Information (June 5, 1975).

162. Lawton Interview, *supra* note 90.

Law enforcement transfers are by no means the only routine use notices that depart from the concept as defined in the Act. For instance, initially many agencies withheld personal information from congressional caseworkers who were seeking help for constituents. The Congress complained bitterly and in October of 1975, OMB advised agencies to regard disclosure to congressmen as a routine use permitted under the Act.[163] In reality, of course, there is no assurance that congressmen will use the information they receive from this transfer in a way that is compatible with the purpose for which the information was first collected.

Many agencies have also established routine use provisions for medical data that violate the Act's requirement. An informal survey by the Domestic Council Committee on the Right of Privacy found that many agencies make it a routine use to share medical information with law enforcement agencies, notwithstanding the fact that in almost all instances medical information was initially collected for reasons related to the subject's health care.

Another common routine use that is probably inconsistent with the Act's definition provides for the release of information to the news media. Like the Congress and law enforcement agencies, the news media has clout with most agencies and can effectively pressure agencies to treat as a routine use the release to the news media of information in their files.[164]

Laundering of Information

Perhaps the greatest potential for abuse of the Privacy Act's routine use provision flows from the statute's definition of an agency. That "definition" merely recites that the term "agency" includes "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government . . . or any independent regulatory agency."[165] Federal agencies, no matter how large or heterogenous, have taken advantage of this broad definition to define themselves as a single agency. Because transfers within a single agency are accomplished on a "need-to-know basis," without serious check or limitation, the routine use provision can be avoided altogether. Therefore, agen-

163. 40 Fed. Reg. 56,741-42 (1975).
164. *See* 40 Fed. Reg. 56,465 (1975).
165. 5 U.S.C. § 552(e) (1970 & Supp. V 1975). The Privacy Act, (a)(1), defines agency by incorporating the definition in the FOIA which refers the reader to section 551(1) of Title 5 for a full definition in addition to summarizing what the term agency includes.

cies as large as the Department of Health, Education and Welfare are able to trade sensitive personal information on a "need-to-know basis" among their own units as diverse as the Social Security Administration, the Student Loan Office, the Indian Health Service, the National Institute of Mental Health, and the Parent Locator Service. In a letter to Mr. John Ottina, Assistant Secretary for Administration and Management of HEW, OMB urged HEW to avoid transfers of personal information among its units unless made for compatible purposes.

> It is noted that HEW has elected to define agency for purposes of the Act as including all elements of the Department rather than treating elements within the Department as separate agencies. (HEW Rules, Section 5b.3(a)(b); FDA Rule § 7.3(f)). While this is not technically inconsistent with the Privacy Act, in the context of an agency as large and complex as HEW, this interpretation creates a possibility of abuse by permitting inappropriate free interchange among elements of the agency. Therefore, care should be taken to insure that this interpretation is not used in such a way as to evade the intent of the Act, i.e., the disclosure of information from a record should be on a need-to-know basis and only for a purpose compatible with that for which the information was originally gathered.[166]

It appears that OMB's admonition has been ignored. A prime example is the information "shell game" played by HEW's Parent Locator Service (PLS). The PLS is a small unit charged with locating absent parents whose children are receiving state or federal welfare benefits. Before its creation in 1974, and prior to enactment of the Privacy Act, state units that performed similar tracking functions were generally able to obtain parent locator information from HEW's Social Security Administration. After passage of the Privacy Act, the Social Security Administration decided that it was improper for it to continue transfers of this information, because the data would not be used by state locator services for purposes which were compatible with the reason for which the Social Security Administration had originally collected the data. This decision generated considerable controversy and eventually involved Secretary Matthew's office, the Congress, and the White House. At length, the Secretary decided that HEW's own Parent Locator Service should obtain the information from the Social Security Administration on an intra-agency need-to-know basis.[167] The federal PLS then

166. Letter from Office of Management and Budget to John Ottina (Dec. 15, 1975).

167. In their defense, Department of Health, Education and Welfare officials believed, in view of the Privacy Act's definitional latitude, that they had no real option but to define the agency as "one agency." Furthermore, the Social Security Administration gave notice of its intention to amend its regulations to permit the internal transfer of information to the Parent Locator Service. 44 Fed. Reg. 16,561 (1976).

published a routine use notice authorizing the transfer of parent locator information to state units.

Under even the most charitable interpretation, this scheme amounts to little more than an information "laundering" service by HEW's Parent Locator Service. HEW's PLS "collects" the information from the Social Security Administration for the purpose of tracking down the missing parents,[168] clearly not the reason for which the information was originally gathered. A literal interpretation of the Act's routine use provision then permits the PLS to transfer that information to state units which will use the data for the same tracking purpose. This study was unable to document whether other agencies take advantage of the ease of intra-agency transfers to "launder" information before transferring it pursuant to a routine use notice.

Some Transfers Discouraged

Despite the abuse of the Act's routine use provision, evidence that some inter-agency transfers have been discouraged by the Privacy Act was found. Transfers of information which is of little importance to an agency are likely to be discontinued if the transfer does not fit neatly within the routine use requirements. The Department of Justice, for instance, previously transferred information about applicants rejected for its attorney honors program to other agencies which might be interested in these applicants. After passage of the Privacy Act, the Department abandoned this practice because it was simply too much trouble.[169]

Other agencies have ceased or limited transfers, not because of obstacles posed by routine use requirements, but because they fear that the receiving agency may be unable to protect the information. The Air Force Office of Special Investigations (AFOSI) reports that it no longer shares detailed investigative information, but instead merely provides a summary to its consumer agencies. AFOSI claims that it does not want its full investigative files subjected to access requests from agencies that may be forced to disclose the information once it is in their possession because they are unable to take advantage of the law enforcement exemptions available to AFOSI.[170]

---

168. Query whether an organization such as the Parent Locator Service, which is not an agency for purposes of the Act, can nonetheless establish a new purpose for information use by receiving that information on a "need-to-know" basis.
169. Lawton Interview, *supra* note 90.
170. Cavaney Interview, *supra* note 50.

Accounting Requirement

Transfers made for a routine use, as well as most transfers authorized by the Privacy Act (except for transfers made pursuant to the Freedom of Information Act or intra-agency transfers), must be accounted for and recorded. Subsection c of the Privacy Act, "Accounting of Certain Disclosures," provides:

> each agency with respect to each system of records under its control, shall . . . keep an accurate accounting of (A) the date, nature and purpose of each disclosure of a record to any person or to another agency made under Subsection b of this Section, and (B) the name and address of the person or agency to whom the disclosure is made.[171]

The Act requires that agencies retain the accounting for at least five years or the life of the record, whichever is longer. Furthermore, with minor limitations, the agency must make the accounting available to the individual named in the record at that individual's request. This provision has a two-fold impact on agencies: first, agencies know that, if they are going to make a transfer, they have certain accounting and paperwork responsibilities; second, the subject of the disclosure will be able to learn of the nature of the transfer, if he so chooses.

A number of agencies have indicated that the accounting requirement is costly and burdensome. Sources reported that next to the system notice and (e) (3) collection of information notice provisions, the accounting requirements constitute the largest paperwork burden under the Act.[172]

The Department of Defense has indicated its concern with the burdensome accounting requirements.

> The requirement to account for all routine disclosures is extremely burdensome. For example, within DOD GAO routinely audits pay records on a daily basis and the entire system on a quarterly basis to determine if procedures are correct. Each disclosure under the Act requires an accounting and in this instance we question the value of such an accounting considering the immense costs involved. Likewise other routine accounting for disclosures to other governmental agencies is extremely burdensome and costly.[173]

The Guaranteed Student Loan Program at HEW has been unable to comply with the accounting provisions. As a consequence, HEW requires students who apply for guaranteed loans to "waive" their right to see the accounting of disclosures. The legality of this practice has been challenged by several student

---

171. 5 U.S.C. § 552a(c) (1) (A)-(B) (Supp. V 1975).
172. Schneider Interview, *supra* note 86.
173. DPB Briefing, *supra* note 65, at 24.

loan applicants in a suit pending in United States District Court.[174]

Transfer of Personal Information to State and Local Governments and Private Sector Organizations

There is a continuous flow of personal information from federal files to state and local government agencies and private organizations. In the months following the passage of the Privacy Act, in some instances the flow was interrupted or shut off altogether. In May of 1974, the Veterans Administration reinterpreted its own statute and interpreted the Privacy Act so strictly that it advised administrators of VA hospitals that they could no longer notify local police when patients with gun shot wounds were admitted, and local administrators were warned that they could not report cases of communicable diseases to state health departments. This strict interpretation of the Act provoked an outcry in the Congress and among state officials.[175] Congress subsequently amended the Veterans Administration's statute to make it clear that the VA could release communicable disease and gun shot wound information.[176]

Federal officials tell horror stories of the consequences that ensued when some federal agencies initially cut off information to state governments. One such story concerns an Oklahoma state trooper who was reportedly involved in a high speed chase that ultimately resulted in a collision. The suspect was rushed to a nearby VA hospital and subsequently identified by hospital officials. Despite pleas from the trooper and his superiors, the hospital refused to disclose the suspect's identity allegedly because they believed that the Privacy Act prohibited the disclosure. State police obtained a warrant for the information, but not before the suspect regained consciousness and checked himself out against medical advice.[177]

The OMB Report describes the initial overreaction of some agencies:

> Initially, agencies experienced some difficulty in determining whether certain types of disclosures are compatible with the purposes for which records are maintained and therefore, could be established as routine uses. Over the years, for example, units

174. Hettig v. Matthews, No. C-762697 (N.D. Calif. Dec. 2, 1976).
175. *See, e.g., Privacy For Shootings*, Des Moines, Iowa Register, Oct. 4, 1975; *Privacy Law and Public Health*, Los Angeles Times, Oct. 31, 1975.
176. 38 U.S.C. § 3301(a) (1970), as amended by Pub. L. No. 94-321 (1976).
177. Lawton Interview, *supra* note 90.

> of state and local government have become dependent on federal agencies for verifying entitlement to a variety of programs including food stamps, unemployment compensation and both federally and locally funded income maintenance and assistance programs. In many cases, initial implementation of the Act resulted in the denial of information needed for the conduct of these programs by state and local governments. In many of those cases appropriate, "routine uses" have been established to permit the disclosure of this information to units of state and local government without the consent of the individual. In those instances where it has been concluded that the written consent of the subject of a record is required (e.g. access to social security records for verifying eligibility for food stamps) statements authorizing access to agency records have been incorporated into state and local aid application forms.[178]

Overreaction Ends

Agency overreaction to the Privacy Act and consequent reduction of dissemination of personal information outside the federal government has ceased. In fact, some sources suspect that the very same pattern of abuse that marks inter-agency transfers now characterizes the transfer of personal information from the federal government to state or private recipients.[179]

The study indicates, however, that the Privacy Act continues to limit federal, state and local government and private sector transfers of personal information in some areas. Officials in state executive and legislative offices who perform the same kind of case work that the staffs of federal congressmen perform are without the benefit of the Congress' new routine use provision and consequently they claim their effectiveness has been compromised. One administrative aide to a governor stated that "while the purpose of the Act was admirable its practical effects were to increase the length of time and the amount of paperwork required to resolve citizens' problems with federal agencies, and possibly to leave the erroneous impression with constituents that the Governor was unresponsive to their problems."[180]

This article has already alluded to the impact that the Privacy Act has had on personal information that HEW shares

178. OMB REPORT, *supra* note 8, at 13.

179. Interview with James Davidson, Counsel, Subcommittee on Intergovernmental Relations, Senate Committee on Government Operations, in Washington, D.C. (Nov. 9, 1976). Carole Parsons, Executive Director of the Privacy Protection Study Commission, recently testified that her staff has found some evidence that transfers among federal, state and local agencies are an area of abuse. *See* S.3425, *A Bill to Increase an Authorization of Appropriations for the Privacy Protection Study Commission, Hearings by the Subcommittee on Government Information and Individual Rights of the House Committee on Government Operations*, 94th Cong., 2nd Sess. 34 (1976).

180. *New U.S. Privacy Law Creating Problems, Aide to Governor Declares*, Little Rock, Arkansas Gazette, Oct. 5, 1975.

with various state agencies. This information includes data collected by the Social Security Administration such as wage record data, supplementary insurance data, and information concerning eligibility for cash payment benefits. Despite pressure from the states, HEW has refused to establish routine uses for the transfer of some of this information. Therefore, some of these transfers must now be authorized by the subject, albeit that these authorizations generally take the form of blanket consents signed at the time of application. Nevertheless, even this perfunctory consent should help to acquaint the subject with the uses that will be made of the information and at least theoretically give the individual some control over that use.

Other agencies have also indicated that because of the Privacy Act, they have eliminated or reduced dissemination of personal information to non-federal organizations. The Department of Defense reports that it may stop providing labor unions with the same type of personal information that it did prior to the enactment of the Privacy Act.

> In some instances we have agreements with labor unions which require us to provide them with certain personal information relating to DOD personnel. This includes such material as civilian promotion files which contain evaluations and personal information about all candidates. This is to permit the union to make their own evaluation as to the merit promotion program. It is questionable whether or not such information can be provided under the "routine uses" of the Act. We are releasing that information which is releasable under the Freedom of Information Act but have not resolved the problem for that which would be a clearly unwarranted invasion of personal privacy.[181]

FBI officials feel that they are now unable to provide private sector organizations with as much information as was possible before the passage of the Privacy Act. As evidence, an FBI source described two recent incidents involving bank investigations. In one case the FBI suspected a bank employee of embezzling. Before the existence of the Privacy Act, the FBI would have informed the bank of its suspicions but here it did not. In another instance, FBI agents had three suspects under surveillance whom they suspected were planning to rob a bank. According to the interviewee, the agents did not inform the bank that it might be a target of a robbery, because they felt constrained by the Privacy Act.[182]

---

181. DPB Briefing, *supra* note 65, at 25.
182. Dennis Interview, *supra* note 57.

CONCLUSION

Analysis of Fair Information Practice Standards

This study, taken alone, does not provide a basis for final judgments about the information impact of agency compliance with the Privacy Act and the amended Freedom of Information Act. The Acts are relatively new and still developing. Furthermore, the "findings" of this study are of necessity dependent on anecdotal and impressionistic research. Nevertheless, the study is a warning signal of possible problem areas.

The trends revealed suggest that after a year and one-half of experience with the Privacy Act, there should be some doubt about the conceptual validity and practicability of the fair information practice principles upon which the Act rests. Federal policy makers have accepted fair information practice principles as gospel. This study suggests that some of that faith may have been misplaced.

The concept of fair information practice was best articulated in a report by HEW's Secretary's Advisory Committee on Automated Personal Data Systems.[183] The "fair information practice code" includes perhaps seven basic standards:

1. There should be no systems containing personal information whose very existence is secret.

2. Organizations should collect only personal information needed by the organization for a lawful purpose.

3. The subject of the information should have access to his records.

4. The subject should have the ability to correct and amend his records.[184]

5. Information obtained for one purpose should be used only for purposes compatible with that purpose (in effect, a confidentiality provision).

6. The organization maintaining personal information must take responsibility to ensure that the records are maintained with the degree of accuracy, relevance and timeliness needed to make a fair decision.

---

183. HEW SECRETARY'S ADVISORY COMMITTEE ON AUTOMATED PERSONAL DATA SYSTEMS, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS xxiii-xxxii (1973).

184. This study did not look in any depth at the subject's ability to correct and amend his records under the Privacy Act. As noted in the body of this article, few agencies reported any significant number of Privacy Act access requests. A fortiori, there was little reason to investigate the impact of challenge and correction rights. Agency sources queried on this point unanimously stated that the amendment provisions had not been used to any appreciable extent and had not had a significant impact on agency information practices.

7. The information must be maintained with a degree of security requisite to safeguard the data.

As implemented in the Privacy Act, these fair information principles take on something of a hollow ring. Publication in the *Federal Register* is an ineffective method for ensuring that a system of records is not secret. Initially, the very act of publishing descriptions of record systems may have an impact on agency record keepers and policymakers; however, in the absence of significant attention by subjects or by guardian groups in the government or the private sector, the effectiveness of publication may soon be diminished. Personal notice to the subject that information about him is maintained in the system—a provision debated by the Congress and discarded as too burdensome—may prove to be the only effective publication method.

Collection standards in the Privacy Act (including those standards couched in terms of "maintenance") may be too vague and too modest to have much impact on agency information practices. The Act permits agencies to continue to define their own collection needs (in keeping, of course, with applicable congressional and executive branch direction). Of course, it may well be that agency discretion for the collection of personal information should not be abridged by comprehensive privacy legislation. Critics argue that if you control an agency's information collection standards, you control the substantive standards and activities of that agency. The point to be drawn from this study is not necessarily that new, substantive collection standards must be established, but rather that we should be aware that the collection standard articulated as a part of fair information practice standards and more or less expressed in the Privacy Act—collect only information necessary for a lawful purpose—should not be relied on as a substitute for resolution of the debate over collection policy.

Perhaps the single finding from the study that can be advanced with near dogmatic confidence concerns the Act's routine use requirements. There is evidence that agencies ignore routine use requirements whenever officials believe that data exchanges must be made. Certainly the study indicates that the Privacy Act's dissemination concept as principally embodied in the routine use concept fails when it is subject to the wholesale exceptions (such as the "need-to-know" and "releasable under the Freedom of Information Act" standards) permitted by the Privacy Act. As a practical matter, the Act allows agencies to define for themselves the meaning and application of a routine use. The only review is publication in the *Federal Register.*

The adequacy of the routine use requirement is not only a

matter of practical implementation; it is also a question of conceptual validity. It may be that the principle—"personal information collected for one purpose should only be used for purposes compatible with that purpose"—is too simplistic. Perhaps transfer of *some kinds* of personal information held by the government (or, for that matter, held by other organizations), should be governed by different standards; standards that for some data would be strict and for other data would be flexible.[185] Indeed, many agency officials argue that the result of conscientious application of the routine use concept would be chaos. They claim that, had agencies taken the routine use requirement seriously, there would have been frightful inefficiency, duplication of collection, waste of resources and extraordinary operational costs.

Analysis of the findings of the study also indicates that the fair information practice principle—that personal information should be maintained with relevance, timeliness and accuracy and in a setting that guarantees reasonable security, at least in the form expressed in the Privacy Act—may be too vague a standard to be implemented. In a context of scarce resources and mission imperatives, many agencies ignored or downplayed these provisions.

Our notions about the beneficial effects of subject access to his record may also need some rethinking. There is tentative evidence that subjects are not interested in obtaining access to information about themselves held by the government, except that held by intelligence and criminal justice agencies. Ironically, the Privacy Act exempts most of the information maintained by those agencies from such access. This study suggests the need for a public education program and questions the wisdom of reliance on the threat of access to improve agency information practices. The old saw that the people get only as good as a system as they deserve was perhaps never more true than as regards the utility of access rights for an indifferent public.

Recommendations

This study and the foregoing discussion raise questions about reform of the Privacy Act and perhaps the Freedom of Informa-

185. For example, the Buckley Amendment, enacted as the Family Educational Rights and Privacy Act of 1974, 20 U.S.C. § 1232(a) (Supp. V 1975), Pub. L. No. 93-380, specifically defines 10 circumstances under which a school may release student record information without the consent of the student or his parents. Most observers claim that, despite a good deal of initial congressional confusion, the Buckley Amendment has worked well.

tion Act. A detailed analysis of possible amendments to the Privacy Act or reform of fair information practice standards, is beyond the scope of this article. It is appropriate, however, to identify, at least in capsule form, areas for discussion and potential reform.

*The definition section of the Privacy Act needs attention: including rewording of the definition of "agency" and the definition of systems of records covered by the Act.

*Collection standards: including the Act's prohibition on collection of first amendment information; and consideration of the identification of specific types of personal information that should be subject to collection standards.

*Maintenance standards: including consideration of the development of specific audit requirements, security requirements, personnel training and regulation requirements, and development of purging standards and schedules, and standards for timeliness, relevance and accuracy.

*Dissemination standards: including consideration of a more protective and specific definition of confidentiality; reform of the intra-agency "need-to-know" standard and reform of the routine use standard.

*Access rights: including consideration of a public education program, and a more effective notice system including personal notice requirements; reform of access exemptions for law enforcement, intelligence, civil investigative and medical information.

*Consideration of the creation of a centralized regulatory authority.

One general conclusion emerges from an analysis of the information gathered in this study. The Congress must reexamine and reform the federal government's standards for handling personal information as expressed in the Privacy Act. Although the nation has made remarkable progress in a relatively short period of time in recognizing and alleviating many of the problems caused by society's handling of personal information, there is more work to be done. Developing and implementing fair information practice standards for the collection, maintenance and use of personal information is a more difficult task than first imagined. Recent amendments to the Freedom of Information Act, and, more directly, enactment of the Privacy Act, are critical and difficult initial steps in the effective regulation of the nation's use of personal information. However, it is likely that they are only first steps in a lengthy process of establishing a conceptual and practicable framework within which to regulate society's use of personal information.

The John Marshall Journal Of Practice and Procedure

Volume 10 Spring, 1977 Number 3

Member, National Conference of Law Reviews