Washington University Law Review

Volume 1976 | Issue 4

January 1976

The Privacy Act of 1974: An Overview and Critique

THE PRIVACY ACT OF 1974: AN OVERVIEW AND CRITIQUE

CONTENTS

I. INTRODUCTION 668
II. COMPUTERS AND PRIVACY 669
III. THE PRIVACY ACT—A GENERAL ASSESSMENT 678
A. *Legislative History* 679
B. *Recognition of Individual Interests* 679
1. *Collection* 680
2. *Maintenance of Files* 681
3. *Disclosure of Records* 683
C. *Restrictions on Federal Agencies* 685
1. *Collection of New Data* 687
2. *Maintenance of Files* 689
3. *Disclosure and Dissemination* 690
D. *Civil Remedies* 692
IV. THE PRIVACY ACT AND THE SOCIAL NEED FOR INFORMATION 695
A. *The Law Enforcement Exemptions* 695
B. *Privacy and the Public's Right to Know* 700
1. *The FOIA Exemptions* 701
2. *The Agencies as Guardians of Privacy* 708
3. *Interaction Between the FOIA and the Privacy Act* 713
V. CONCLUSION 718

> As every man goes through life he fills in a number of forms for the record, each containing a number of questions. . . . There are thus hundreds of little threads radiating from every man, millions of threads in all. If these threads were suddenly to become visible, the whole sky would look like a spider's web, and if they materialized as rubber bands, buses, trams, and even people would lose the ability to move. . . . They are not visible, they are not material, but every man is constantly aware of their existence. . . . Each man, permanently aware of his own invisible threads, naturally develops a respect for the people who manipulate the threads.
>
> Alexander Solzhenitsyn,
> *Cancer Ward*[1]

1. A. SOLZHENITSYN, CANCER WARD (1968), *quoted in* DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE, RECORDS COMPUTERS AND THE RIGHTS OF CITIZENS 31 (1973) [hereinafter cited as HEW REPORT].

I. INTRODUCTION

Most of us have an intuitive sense of the meaning and value of privacy. As a legal matter, however, the term "privacy" has proved remarkably elusive,[2] and the dispute over what it means, what rights it encompasses, and the degree of legal protection it deserves, rages unabated. The few Supreme Court efforts to find a constitutional footing for privacy have been cautious, tentative, and confined to an examination of the individual's right to engage in activities intensely affecting his person.[3] The Court has yet to consider the constitutional status of informational privacy—the individual's interest in controlling the flow of personal information about him.[4]

Neither the paucity of case law nor the inability to define its contours precisely can diminish the importance of informational privacy to modern American society. Today, information is power; the development of the computer has enabled a person or institution acquiring information about an individual to increase its control over that individual in proportion to the data collected.[5] The decrease in individual freedom that necessarily accompanies this increase in external control is repugnant to the goals of a democratic society.[6] Underlying the debate over privacy is a consensus that the loss of informational privacy presents an unprecedented threat to the integrity of the individual—and, that the government has an affirmative duty to protect each citizen from unwarranted external control as part of its general duty to promote individual freedom. The best evidence of this consensus is the congressional decision to enact the Privacy Act of 1974 (Privacy Act).[7]

This Note is about the Privacy Act. Part II will discuss how the computer created a massive threat to individual privacy, rendered existing legal protection wholly inadequate, and left no alternative to the enact-

2. A. WESTIN, PRIVACY AND FREEDOM 7 (1967).

3. *See* note 40 *infra.*

4. For discussion of the constitutional bases of informational privacy, see Note, *Informational Privacy: Constitutional Challenges to the Collection and Dissemination of Personal Information by Government Agencies,* 3 HASTINGS CONST. L.Q. 229 (1976).

5. *See* notes 14-22 *infra* and accompanying text.

6. *See, e.g.,* S. REP. No. 93-1183, 93d Cong., 2d Sess. 7 (1974): "In the past, dictatorships have always come with hobnailed boots and tanks, and machine guns, but a dictatorship of dossiers, a dictatorship of data banks can be just as repressive, just as chilling, and just as debilitating on our constitutional protections."

7. 5 U.S.C. § 552a (Supp. V 1975).

ment of federal privacy legislation.[8] Part III will analyze the means by which the Privacy Act attempts to recognize and ensure the vitality of the individual's right to informational privacy.[9] Finally, Part IV will examine the manner in which the Privacy Act strives to accommodate privacy with two of the many societal interests with which it conflicts: effective law enforcement and the public's right to know.[10]

The conclusions of this Note are not optimistic. The Privacy Act is conceptually sound, but practically unenforceable. Additionally, the attempts to resolve the conflicts between privacy and interests with which it competes are wholly unsatisfactory. Nevertheless, the recognition that the Privacy Act is merely a first step dictates the conclusion that it is a monumental step.

II. COMPUTERS AND PRIVACY

Unfortunately, the massive threat to privacy that gave rise to the Privacy Act emerged in large part from the government itself. Although governments have kept records for thousands of years,[11] only recently has the threat become epidemic. In the United States, the quantity of information gathered about individuals increased steadily throughout the twentieth century as it became apparent that large quantities of information were necessary for intelligent public decisions.[12] Privacy was not seriously threatened, however, because individuals were mobile and information was stored in manual files that could not easily be transported, consolidated, analyzed, or retrieved. Technological limitations and simple inefficiency preserved a reasonable balance between the individual seeking various benefits without sacrificing privacy, and the

8. *See* notes 11-53 *infra* and accompanying text.

9. *See* notes 54-156 *infra* and accompanying text.

10. *See* notes 157-273 *infra* and accompanying text.

11. For an outstanding discussion of the history of government record keeping from Egyptian times to the present, see *Federal Data Banks, Computers and the Bill of Rights: Hearings Before the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 92d Cong., 1st Sess. 836-46 (1971) (statement of A. Westin) [hereinafter cited as *Data Bank Hearings*].

12. *See* A. WESTIN, *supra* note 2, at 321-23. Professor Westin maintains that the marked increase in data collection stems from the rejection of the theory that rational governmental action could be based on limited facts and the acceptance of a behavioral-predictive theory of information. *See also* HEW REPORT, *supra* note 1, at 34-35; Project, *Government Information and the Rights of Citizens*, 73 MICH. L. REV. 971, 1222 (1975).

government, which needed, and could compel the surrender of, vast amounts of personal data.[13]

Recent technological advances enabled government employees to shatter that balance. With the advent of the computer, the government's ability to compile, retrieve, manipulate, analyze, and disseminate information has increased exponentially. A 1974 study of fifty-four federal agencies disclosed 858 computerized data banks containing 1.25 billion records on individual citizens.[14] The FBI's National Crime Information Center alone contained over 1.7 million files and 195 million sets of fingerprints.[15] Twenty-nine data banks, used exclusively to maintain "black lists," contained damaging information about thousands of law-abiding citizens.[16] One commentator estimates that the average American citizen is the subject of at least twenty records.[17]

---

13. *See Data Bank Hearings, supra* note 11, at 69 (statement of J. Rosenberg). *See also* Miller, *Computers, Data Banks and Individual Privacy: An Overview*, 4 COLUM. HUMAN RIGHTS L. REV. 1 (1972); Ruggles, Pemberton & Miller, *Symposium: Computers, Data Banks, and Individual Privacy*, 53 MINN. L. REV. 211, 223, 228 (1968).

14. *See* STAFF OF THE SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 93D CONG., 2D SESS., FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS IV (1974) [hereinafter cited as DATA BANK STUDY]; Project, *supra* note 12, at 1223-24.

15. *See* Countryman, *The Diminishing Right of Privacy: The Personal Dossier & the Computer*, 49 TEX. L. REV. 837, 853 (1971). *See also* HEW REPORT, *supra* note 1, at 13-15; Miller, *supra* note 13, at 5.

16. *See* DATA BANK STUDY, *supra* note 14, at xxxix (summary of findings). Most of these files were compiled and computerized by the Army, HUD, and the FCC. Perhaps most shocking was the revelation that the Army "had been systematically keeping watch on the *lawful* political activity of a number of groups and preparing *incident* reports and dossiers on individuals engaged in a wide range of legal protests." Miller, *supra* note 13, at 4. *See* Countryman, *supra* note 15, at 857. For a collection of press articles documenting the public uproar upon discovery of the Army's activities, see *Data Bank Hearings, supra* note 11, pt. II, at 1607-09.

17. *See* Project, *supra* note 12, at 1224 (citing *Records Maintained by Government Agencies, Hearings on H.R. 9527 and Related Bills Before a Subcomm. of the House Comm. on Government Operations*, 92d Cong., 2d Sess. 22 (1972) (statement of Representative Patten)). *See also* DATA BANK STUDY, *supra* note 14, at iv; Karst, *"The Files": Legal Controls Over the Accuracy and Accessibility of Stored Personal Data*, 31 LAW & CONTEMP. PROB. 342, 343-44 (1966). Individuals are generally unaware of the multitude of ways in which personal information is collected. For example,

> [w]hether he knows it or not, whenever an American travels on a commercial airline, reserves a room at one of the national hotel chains, rents a car, he is likely to leave distinctive electronic tracks in the memory of a computer that can tell a great deal about his activities,—his movements, his habits and associations.

Data Bank Hearings, supra note 11, at 9 (statement of A. Miller).

For several reasons, the exponential increase in governmental recordkeeping ability poses a unique threat to personal privacy. The most obvious danger is the computer's ability to combine scattered bits of data into a comprehensive personal dossier.[18] This capacity permits government agents to make far more effective, and consequently more intrusive, use of information already in government files.[19]

Second, the increased capacity to handle information creates strong pressures to acquire more of it. Using either legal compulsion or subtle

18. The crux of the problem is that the computer has enabled government to collect "too much data." The mere compilation of vast personal dossiers offends privacy by creating a "potential 'record-prison' for millions of Americans, as past mistakes, omissions, or misunderstood events become permanent evidence . . . ." A. WESTIN, *supra* note 2, at 160. *See* HEW REPORT, *supra* note 1, at 12-15; Countryman, *supra* note 15, at 868; Miller, *supra* note 13, at 1-3. Professor Countryman maintains that our continued worship of efficiency and failure to discard the misconception that whatever is efficient is desirable will result in the destruction of privacy. Countryman, *supra*, at 869. He argues that "we have not, in this country, permitted efficiency to be the determining factor when individual liberty is jeopardized." *Id.* at 870. Countryman somberly concludes that the computer cannot be controlled and that "[t]he only hope for substantial protection of privacy against the computerized dossiers . . . is that they not exist—at least . . . not exist on their present scale." *Id.* at 869.

19. For example, standardized computer languages and remote access to computer terminals allow the instantaneous transfer of information between data banks or from a data bank to any person with access to a computer terminal. Recently there has been a movement to centralize all information about an individual in one data bank. As Alan Westin has noted:

> Compared to manual files, computers offer greater storage capacity for data; greater speed of processing; lower processing cost per item of information; greater capacity for complex logical operation; simultaneous access to multiple records; ability to link data on the same person, place, or thing from different files; remote access to central facilities for input and output; and the ability to exchange information with other computer systems.

Data Bank Hearings, supra note 11, at 838. *See also* Countryman, *supra* note 15, at 863; Miller, *Personal Privacy in the Computer Age: The Challenge of a New Technology in an Information-Oriented Society*, 67 MICH. L. REV. 1089, 1093-1103 (1969); Comment, *The Computer Data Bank-Privacy Controversy Revisited: An Analysis and an Administrative Proposal*, 22 CATH. U. L. REV. 628, 635 (1973).

Public reaction to the computer-based privacy invasion, initially slow to develop, erupted upon disclosure of formal proposals for a National Data Center, which would have consolidated information held by all government agencies. For a discussion of the trend towards centralization and the National Data Center, see DATA BANK STUDY, *supra* note 14, at XV-XVIII; Meldman, *Centralized Information Systems and the Legal Right to Privacy*, 52 MARQ. L. REV. 335 (1969); Miller, *supra*, at 1131-40; Note, *Privacy and Efficient Government: Proposals for a National Data Center*, 82 HARV. L. REV. 400, 406 (1968).

Although the proposal for a National Data Center was defeated, the "vast numbers of personal dossiers already assembled by private and official compilers have effectively created a 'National Data Bank' now." Countryman, *supra* at 863.

coercion,[20] federal agencies quickly seized the opportunity to acquire huge quantities of personal information,[21] much of it irrelevant to any legitimate government duty.[22] Moreover, unqualified investigators often solicited data from third parties and compiled dossiers replete with information that was inaccurate, biased, or simply fabricated by the investigator.[23] Few persons know the importance of, or even the existence of, such personal records. Until 1974, individuals aware of these records could not inspect them, challenge their accuracy, or restrict their use.[24]

Finally, the computer's own fallibility poses a significant threat to personal privacy. Contrary to popular belief, computers do err.[25] The advent of remote terminals and universal computer language makes possible inter-data bank transfers, both authorized and unauthorized. The latter constitute simple theft, to which computer records are more vulnerable than manual records.[26] Authorized information transfers raise the prospect of contextual inaccuracy.[27] Information supplied to

---

20. *See* Miller, *supra* note 19, at 1137.

21. "The inevitable result of using computers is that the investigator acquires two or three times as much personal information . . . as was ever collected before because of the physical or cost limitations of acquisition." A. WESTIN, *supra* note 2, at 160. *See* Ruggles, Pemberton & Miller, *supra* note 13, at 229.

22. *Data Bank Hearings, supra* note 11, at 11 (statement of A. Miller); Address by Senator Ervin, Spring Joint Computer Conference (May 20, 1971), *reprinted in Data Bank Hearings, supra* note 11, pt. II, at 1552; Ruggles, Pemberton & Miller, *supra* note 13, at 229. *See also* S. REP. No. 93-1183, *supra* note 6, at 11.

23. *See* Countryman, *supra* note 15, at 839-43; Miller, *supra* note 19, at 1141-42.

24. *See* Countryman, *supra* note 15, at 844. Professor Countryman argues that even in those rare instances when an individual realizes that constant credit or employment rejections are attributable to a damaging record, he is unable to secure access to the record, and thus relief is impossible.

25. *See* Miller, *supra* note 19, at 1109-18. Accidental disclosures, dust, and related mechanical failures can also be extremely damaging to personal privacy.

26. *See Data Bank Hearings, supra* note 11, at 470-73 (statement of R. Henderson) (discussing security developments); Grenier, *Computers and Privacy: A Proposal for Self-Regulation*, 1970 DUKE L.J. 495, 496; Miller, *supra* note 19, at 1109-14; Comment, *Public Access to Government-Held Computerized Information*, 68 NW. U.L. REV. 433 (1973).

27. For example, where an individual is listed as a felon on a computerized record, but the offense, civil disobedience, is not recorded, the party receiving the data is likely to misinterpret it. Other frequent examples of contextual inaccuracy arise when employment ratings are transmitted to users who do not have access to the rating criterion. *See, e.g.*, HEW REPORT, *supra* note 1, at 19; Miller, *supra* note 19, at 1115-17; Ruggles, Pemberton & Miller, *supra* note 13, at 230; Comment, *supra* note 19, at 636-37.

one agency for one purpose is often transmitted to other agencies for wholly unrelated purposes.[28] Deprived of its contextual background, the data may be misinterpreted, often to the disadvantage of the person whom it concerns.

These technological forces have had a devastating impact on personal privacy. Increasingly, almost all that we do, and particularly the mistakes we make, are recorded in government files. Neither the passage of time nor departure to a new community can erase these blemishes on our records,[29] records that are consulted with increasing frequency whenever we apply for employment, credit, insurance, or other important benefits. We live in what one commentator calls a "record prison."[30] Almost all of us have committed some act at some time that would seriously jeopardize our chances in life if recorded, retained indefinitely, and disclosed on a regular basis.[31] The technological breakthroughs in information handling may deprive people of the opportunity for a fresh start in life, a disastrous result because

> [i]f we want man to be self-realized . . . [w]e have got to give him opportunities to fall on his face, to blunder occasionally, to make mistakes. We are human, and possess frailties . . . [i]f we put another wall or barrier up, or some kind of fear in front of people, they can become very reluctant to experiment and life will be very disappointing and confining for many.[32]

Moreover, data derived from a computer carries an impact disproportionate to its actual value. Too often, those who consult computerized records assume the accuracy of the data presented and rarely consider that personalized information in such files may be irrelevant to their needs, factually or contextually inaccurate, dated, or incompelete.[33] The

28. The computer has made it too easy for too many people to gain access to personal files. *See* HEW REPORT, *supra* note 1, at 13; Karst, *supra* note 17, at 342-43; Miller, *supra* note 13, at 230; Comment, *supra* note 26, at 433.

29. *See Data Bank Hearings, supra* note 11, pt. I, at 31 (remarks of S. Ervin): "[A] computer has marvelous gifts of memory far beyond any human being . . . and at the same time it lacks virtues of human beings, such as the virtue of compassion and the willingness to forget and forgive some of our offenses."

30. A. WESTIN, *supra* note 2, at 160. *See* note 18 *supra.*

31. *See* A. WESTIN, *supra* note 2, at 160; *Data Bank Hearings, supra* note 11, pt. I, at 31 (remarks of S. Ervin); Comment, *supra* note 19, at 638-39.

32. *Data Bank Hearings, supra* note 11, at 83 (statement of J. Rosenberg).

33. *See* A. WESTIN, *supra* note 2, at 160; Miller, *supra* note 19, at 1116; *cf.* Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890) (discussing nineteenth century tendency to rely excessively on printed words).

innocent subject of the unreliable record, however, is usually either ignorant of its existence or incapable of correcting it.[34]

Finally, the mere capacity to acquire such records may seriously injure the human interests that the concept of privacy protects. The mere collection and retention of sensitive or personal information creates a state of severe psychological insecurity.[35] As people begin to feel they are under constant surveillance, they will begin to evaluate themselves and regulate their conduct with reference to what is, or may be, contained in their computerized records.[36]

None of these threats to individual freedom and dignity was planned or even foreseen. Each has arisen as the inadvertent by-product of information techniques essential to the solution of pressing social needs. Striking a balance between the individual interest in privacy and the government interest in social progress is an extraordinarily difficult task. What makes that task urgent is the speed and completeness with which the computer has destroyed the balance that previously existed.[37]

Prior to the Privacy Act of 1974, the law afforded little protection from the dangers of extensive recordkeeping systems.[38] In both

34. *See Data Bank Hearings, supra* note 11, at 17 (statement of A. Miller); Countryman, *supra* note 15, at 844.

35. *See* DATA BANK STUDY, *supra* note 14, at xviii (statement of A. Miller): "It is not essential that dossiers, files, surveillance, actually are used to repress people. If these activities give the appearance of repression that in itself has a chilling effect on the precious rights guaranteed . . . by the Constitution . . . ."

36. *See* A. WESTIN, *supra* note 2, at 323; *Data Bank Hearings, supra* note 11, at 10 (statement of A. Miller); Miller, *supra* note 13, at 6 (discussing impact of computers on exercise of first amendment rights); Note, *supra* note 19, at 637-39.

37. As Professor Miller has noted:

> The computer is a many-splendored animal. It is myopic to think of it as little more than a high speed calculator with a gland condition . . . .
>
> . . . .
>
> We must recognize that we are dealing with a new technology, whose applications are just beginning to be perceived and whose capacity to deprive us of our privacy simply cannot be measured in terms of existing systems . . . .

Ruggles, Pemberton & Miller, *supra* note 13, at 225-27.

38. Commentators unanimously agreed that the existing legal structure was totally incapable of coping with the threats posed by computers. *See, e.g.*, HEW REPORT, *supra* note 1, at 34-35; Beaney, *The Right to Privacy and American Law*, 31 LAW & CONTEMP. PROB. 253, 258-59 (1966); Countryman, *supra* note 15, at 864; Kalven, *Privacy in Tort Law—Were Warren and Brandeis Wrong?*, 31 LAW & CONTEMP. PROB. 326, 327 (1966); Karst, *supra* note 17, at 350; Meldman, *supra* note 19, at 352; Miller, *supra* note 19, at 1207; Sills, *Automated Data Processing and the Issue of Privacy*, 1 SETON HALL L. REV. 7, 19 (1970). *See also* Shibley v. Time, 40 Ohio Misc. 51, 321 N.E.2d 791

constitutional and common law interpretation, courts have awkwardly followed in the footsteps of technology while attempting to construct a legal framework to protect the right of privacy.[39] Although the Supreme Court has enunciated a constitutional right of privacy which emanates from penumbras of the Bill of Rights and is necessary to ensure the vitality of specific guarantees,[40] the Court has yet to directly address informational privacy as a constitutional right.[41] The common law provides little more protection.[42]

The common law of informational privacy was designed primarily to compensate a victim for injuries inflicted by the mass media.[43] To recover on a cause of action for invasion of privacy, an individual must ordinarily prove *public disclosure* of *intimate facts.*[44] Most injuries arising from misuse of records involve neither. The law of privacy is intertwined with the law of defamation, so that communications subject to a qualified privilege under defamation law are not actionable in a suit for invasion of privacy.[45] In the majority of cases, disclosures made for employment or credit determinations are qualifiedly privileged. Traditionally, consent was a defense in a privacy suit, and courts applied it liberally when information voluntarily surrendered for a spe-

(Ct. C.P. 1974) (holding sale of names not an actionable invasion of privacy and apologizing to plaintiff for the pitiful state of the law).

39. For discussion of the development of the right to privacy, see HEW REPORT, *supra* note 1, at 34-35; Long, *The Right to Privacy: The Case Against the Government,* 10 ST. LOUIS U.L.J. 1 (1965); Sills, *supra* note 38, at 10-17.

40. *See* Griswold v. Connecticut, 381 U.S. 479 (1965) (right to privacy in penumbras of first eight amendments protects interest of married persons in using contraceptives). *See also* Roe v. Wade, 410 U.S. 113 (1973) (right to privacy encompasses woman's interest in having an abortion); Stanley v. Georgia, 394 U.S. 557 (1969) (right to privacy embodied in first amendment protects individual's interest in viewing pornography at home); Katz v. United States, 389 U.S. 347 (1967) (right to privacy found in fourth amendment protects individuals against warrantless wiretap); Beaney, *supra* note 38, at 253 (1966); Gross, *The Concept of Privacy,* 42 N.Y.U. L. REV. 34 (1967).

41. For a discussion of the constitutional dimensions of informational privacy, see Note, *supra* note 4.

42. *See* notes 43-47 *infra.*

43. *See* Meldman, *supra* note 19, at 340-48; *Data Bank Hearings, supra* note 11, at 17 (statement of A. Miller); Miller, *supra* note 19, at 1156-60.

44. *See* note 43 *supra*; Karst, *supra* note 17, at 346. Accordingly, if accurate information is disclosed, an individual cannot recover absent publication to a large number of people. False disclosures will often be subject to a qualified privilege. *Id. See* note 45 *infra.*

45. The qualified privilege covers both communications that are made in good faith and those in which the communicator has an interest. *See* Karst, *supra* note 17, at 346-47; Miller, *supra* note 19, at 1158-62; Note, *supra* note 19, at 631-32.

cific reason is used for totally unrelated purposes.[46] Law suits are costly and time consuming; damages are difficult to determine and frequently inadequate.[47] Finally, and perhaps most importantly, the victim is often unaware that a computerized record containing damaging information is the cause of his injury.

On a more fundamental level, it is wholly unreasonable to expect courts alone to protect personal privacy because there is no adequate definition of the concept.[48] Several leading commentators have urged

46. *See* Project, *supra* note 12, at 1241-42 (discussing recent developments). Consent may be express or implied. Courts have upheld the defense notwithstanding the use of coercion to obtain the information. *See* Meldman, *supra* note 19, at 349; Miller, *supra* note 19, at 1170-73 (noting inappropriate applications of the defense as well as countervailing tendency of courts to scrutinize carefully claims that consent was given).

47. *See* Meldman, *supra* note 19, at 352; Comment, *supra* note 19, at 631-32. *See also* Karst, *supra* note 17, at 351. "Restitution in any literal sense is simply impossible in the context of disclosures of sensitive data; once made, a disclosure can never be erased." *Id.*

48. *See* A. WESTIN, *supra* note 2, at 7: "Few values so fundamental to society as privacy have been left so undefined in social theory or have been the subject of such vague and confusing writing by social scientists." *See also* Sills, *supra* note 38, at 11.

Commentators have argued intensely over whether there is in fact an independent right to privacy. Dean Prosser maintained that the right to privacy was merely an expedient legal device employed by courts to protect several independent interests "which are tied together by a common name but otherwise have almost nothing in common." W. PROSSER, HANDBOOK OF THE LAW OF TORTS § 117, at 804 (4th ed. 1971). *See also* Sills, *supra* note 38, at 11; Note, *supra* note 19, at 406.

Professor Bloustein, Prosser's leading critic, urged that privacy is a truly independent interest that protects individual dignity and integrity. *See* Bloustein, *Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser*, 39 N.Y.U.L. REV. 962, 971 (1964). For criticism of both Prosser and Bloustein, see Gross, *supra* note 40; *cf.* Kalven, *supra* note 38, at 327 (tort law should not protect privacy at all). The debate is significant, since only Bloustein's thesis is broad enough to allow the erection of new principles capable of averting the computer based threat to privacy. *See* Bloustein, *supra*, at 1006; Project, *supra* note 12, at 1232-39. Specifically, Dean Prosser's theory of privacy is merely a method derived from existing case law, designed to provide sensible resolutions to problems caused by mass-media disclosure of extremely personal information. It cannot be adapted to cope with the computer-based privacy invasion.

Professor Bloustein's theory, under which privacy is defined broadly as the interest in protecting individual dignity, is more readily adaptable. The advantage of the Bloustein thesis is that it can accomodate the regulation of any kind of threat to individual dignity and assures that "new techniques could not outflank the law." The problem with the Bloustein thesis is that it provides absolutely no guide to aid in determining what constitutes an actionable invasion of privacy. If privacy is defined in such broad terms it will ultimately be necessary to delineate the scope of legal protection against the misuse of computers with rules comparable to those developed by Dean Prosser. Thus, it does not matter if privacy is defined narrowly with reference to a specific

that privacy is the "right to determine when, how, and to what extent information is . . . communicated to others."[49] A control-oriented definition of privacy will permit elimination of some of the grosser abuses by records custodians. This definition alone can never guide the courts to a reasonable approach to privacy, however, because it does not facilitate a quantitative assessment of the right to privacy.[50] Yet such quantification is essential because the amorphous nature of information, its many uses, and the degree to which privacy conflicts with such other critical social interests as freedom of expression and law enforcement dictate that the right to privacy can never be absolute.[51]

Commentators recognized the judicial inability to resolve the problems created by the computer and directed their attention to Con-

threat, such as the computer, or broadly, with accompanying legal rules to cope with that threat. The crucial point is that the legal system must recognize the need for flexibility so that the law can adapt to new technological threats. We can no more expect to transfer rules adopted today to cope with the problems of tomorrow than we can "attempt a literal transfer of rules that were framed for a vanished environment." *Data Bank Hearings, supra* note 11, at 835 (statement of A. Westin). Thus, the legal framework must be agreed upon before the law can proceed to struggle with the problems posed by computers.

49. A. WESTIN, *supra* note 2, at 7. Professor Westin maintains that protection of privacy is crucial to a free society because: (1) it fosters self-reliant citizens; (2) it allows experimentation and innovation by private parties; and, (3) it stifles government tendencies toward totalitarianism. *See Data Bank Hearings, supra* note 11, at 835 (statement of A. Westin). Arthur Miller asserts that although privacy is impossible to define, it has begun to be seen as an "individual's ability to control the flow of information concerning or describing him." Miller, *supra* note 19, at 1107. Miller and Westin had a strong influence on the Senate subcommittee investigating computerized data banks. The committee combined the Miller and Westin conceptions and defined privacy as "the capacity . . . to determine what information about the individual will be collected and disseminated to others. Privacy also involves a subjective sense of self-determination and control over personal information." DATA BANK STUDY, *supra* note 14, at ix. For additional proposed definitions of privacy, see Beaney, *supra* note 38, at 254; Gross, *supra* note 40, at 34; Jourard, *Some Psychological Aspects of Privacy*, 31 LAW & CONTEMP. PROB. 307 (1966); Project, *supra* note 12, at 224-26; Comment, *supra* note 19, at 630-31. *See* Warden v. Hayden, 387 U.S. 294, 323 (1967) (Douglas, J., dissenting).

Several commentators have urged that individuals should have a property right in all information pertaining to them "with all the restraints on interference by public or private authorities and due process guarantees that our law of property has been so skillful at devising." Miller, *supra* note 19, at 1223-28.

50. *See* note 48 *supra*.

51. *See* HEW REPORT, *supra* note 1, at 38-40; A. WESTIN, *supra* note 2, at 7; Beaney, *supra* note 38, at 256; Miller, *supra* note 19, at 1162-70, 1193-1200; Comment, *supra* note 19, at 629; notes 157-273 *infra* and accompanying text. Additionally, total protection for privacy is neither possible nor desirable. *See* Meldman, *supra* note 19, at 352.

gress,[52] which responded by passing the Privacy Act of 1974.[53] The remainder of this Note will assess the degree to which the Act permits effective control of government abuses of personal records and adequate resolution of the conflict between individual privacy and social responsibility.

III. THE PRIVACY ACT—A GENERAL ASSESSMENT

The Privacy Act of 1974 has three broad goals—to recognize individuals' interests in government records concerning them, to regulate the information practices of federal agencies, and to strike an appropriate balance between the need of the "individual American for a maximum degree of privacy over personal information he furnishes his government, and . . . that of the government for information about the individual which it finds necessary to carry out its legitimate functions."[54] The first two goals of the Act are essentially similar: increasing the individual's control over his records necessarily restricts agency control. This section will discuss the mechanisms by which the Act seeks to achieve these two generally compatible goals.

The section will begin with a brief review of the Privacy Act's chaotic legislative history, a prerequisite to understanding its many inconsistencies. Next, it will discuss the individual interests recognized by the Act, analyzing them in terms of the Act's three conceptual focal points—collection of new information, maintenance of files, and disclosure of agency records to other persons or institutions. The third part of this section will employ the same analytic framework to assess the Act's restrictions on agency information practices. Finally, this section will discuss the civil remedies available to a citizen whose rights under the Act are ignored by a federal agency.

The conclusions reached are generally pessimistic. Although the Act is conceptually sound, the mechanisms used to implement these concepts are likely to prove ineffective. To enforce its substantive provisions, the Act relies primarily on individual initiative, yet provides citizens with neither the means to discover agency violations nor the

52. *See, e.g.*, HEW REPORT, *supra* note 1, at 34-35; Beaney, *supra* note 38, at 264; Meldman, *supra* note 19, at 352; Comment, *supra* note 19, at 635.

53. 5 U.S.C. § 552a (Supp. V 1975).

54. H.R. REP. No. 93-1416, 93d Cong., 2d Sess. 4 (1974). For a discussion of the Privacy Act, see Project, *supra* note 12, at 1303-40.

incentive to rectify them. In short, the Act is conceptually sound but pragmatically unenforceable.

A. *Legislative History*

The legislative history of the Privacy Act is both extraordinary and significant. The final enactment of the statute ended an outstanding demonstration of legislative chaos. The House of Representatives and the Senate originally passed separate, materially different privacy bills.[55] The Senate sent its bill to the House, which retained the Senate's enacting clause and substituted the House bill in its entirety thereafter.[56] Facing strong pressure to enact some type of privacy legislation before the end of the session, and lacking adequate time for a conference committee, House and Senate committee leaders held a series of informal meetings. These meetings ultimately produced a compromise bill derived in part from the original Senate bill, in part from the original House bill, and in part from entirely new amendments.[57]

The consequence of this hasty and haphazard legislative process is an internally inconsistent statute with no reliable indication of congressional intent. The original committee reports are of limited value in interpreting the final statute. The only reliable legislative history consists of a rather skimpy staff analysis of the compromise amendments appearing in the Congressional Record.[58] Consequently, courts are likely to have great difficulty interpreting the Act and vigorous enforcement may be impossible.

B. *Recognition of Individual Interests*

The Privacy Act explicitly assumes that informational privacy "is a personal and fundamental right protected by the Constitution,"[59] respect for which is essential to our government.[60] By various means, the

55. H.R. 16373, 93d Cong., 2d Sess. (1974); S. 3418, 93d Cong., 2d Sess. (1974).

56. *See* 120 CONG. REC. H11,661 (daily ed. Dec. 11, 1974).

57. *See* 120 CONG. REC. S21,811 (daily ed. Dec. 17, 1974).

58. *Analysis of House and Senate Compromise Amendments to the Federal Privacy Act, printed in* 120 CONG. REC. S21,817 (daily ed. Dec. 17, 1974) *and in* 120 CONG. REC. H12,243 (daily ed. Dec. 18, 1974).

59. Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(4), 88 Stat. 1897. *See* H.R. REP. No. 93-1416, *supra* note 54, at 9.

60. *See* S. REP. No. 93-1183, *supra* note 6, at 14 ("[t]he premise underlying this legislation is that good government and efficient management require that basic principles

Act attempts to enable individuals to limit the collection, maintenance, and dissemination of personal information about them.

1. *Collection*

Subsection (e)[61] of the Privacy Act establishes specific collection regulations for each federal agency that maintains a system of records. Several of these restrictions implicitly recognize the individual's interest in limiting government acquisition of personal data about him. For example, subsection (e)(3)[62] attempts to ensure that an individual's decision to surrender information about himself to the government is intelligent and voluntary. Accordingly, agencies must disclose to persons from whom they seek information:

> (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 . . . .[63]

In theory this section permits individuals to resist disclosures that are not explicitly authorized by statute or executive order. In practice, however, the free choice granted by this section may be illusory if, as in the past, individuals must waive their right to withhold personal information when applying for a government job or benefit.[64]

Subsection (e)(7)[65] recognizes another important individual interest—that some personal information is ordinarily beyond the scope of any legitimate government inquiry.[66] This subsection prohibits agencies from collecting or maintaining any "record describing how any

---

of privacy, confidentiality and due process must apply to all personal information programs . . .").

61. 5 U.S.C. § 552a(e) (Supp. V 1975).

62. 5 U.S.C. § 552a(e)(3) (Supp. V 1975).

63. *Id.*

64. *See* note 20 *supra.*

65. 5 U.S.C. § 552a(e)(7) (Supp. V 1975).

66. This provision, like subsection e(1), *see* notes 115-20 *infra*, is "aimed particularly at preventing collection of protected information not immediately needed, about

individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or *unless pertinent to and within the scope of an authorized law enforcement activity.*"[67] The concept that some information belongs only to the individual is extremely important.[68] As one commentator has noted, however, Congress' decision to define this category of "untouchable information" in terms of the first amendment was unfortunate.[69] Moreover, the exemption for law enforcement activity opens a loophole that threatens to swallow the rule,[70] a problem that Section III of this Note will consider in detail.

2. *Maintenance of Files*

Subsection (d)[71] explicitly recognizes the individual's interest in gaining access to and correcting errors in personal records. Subsection (d)(1) provides: "Each agency that maintains a system of records

---

law-abiding Americans, on the off-chance that Government . . . might possibly have to deal with them in the future." S. REP. No. 93-1183, *supra* note 6, at 57. For discussion of the compromise amendment, see 120 CONG. REC. S21,816 (daily ed. Dec. 17, 1974).

67. 5 U.S.C. § 552a(e)(7) (Supp. V 1975) (emphasis added).

68. *See* note 49 *supra.*

69. *See* Project, *supra* note 12, at 1308-09 (criticizing subsection (e)(7) for failing to prohibit collection about other activities unprotected by the first amendment). *See also* Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Fed. Reg. 28,949 (1975) [hereinafter cited as OMB Guidelines]. The OMB Guidelines direct agencies to "apply the broadest reasonable interpretation" in determining whether or not a particular activity is protected by the first amendment. *Id.* at 28,965. Although the Guidlines structly limit the use of the subsection (e)(7) exception to acquisition expressly authorized by statute, they fail to provide adequate guidance for agencies attempting to determine if the collection of information concerning a suspect's first amendment rights would be "pertinent to and within the scope of an authorized law enforcement activity." *Id.*

70. The primary problem with this section is that the exception is overly broad. Although there are many instances in which law enforcement agencies require information pertaining to the exercise of a subject's first amendment rights, there is no way to assure that agencies will refrain from collecting such information "unless pertinent to and within the scope of an authorized law enforcement activity." The exemption may well perpetuate precisely those "fishing expeditions" that subsection (e)(7) is designed to preclude. *See* 120 CONG. REC. H10,892 (daily ed. Nov. 20, 1974) (purpose of the exemption is to assure that "political and religious activities are not used as a cover for illegal or subversive activities").

71. 5 U.S.C. § 552a(d) (Supp. V 1975).

shall—(1) upon request by any individual to gain access to his record or to any information pertaining to him . . . permit him . . . to review the record . . . ."[72] Subsections (d)(2)-(4)[73] enable the individual to object to the contents of a personal record, institute proceedings to correct it, and request that notice of the objection be sent to those who have previously received the record.[74] These provisions are the heart of the Privacy Act and constitute a major conceptual advance.[75] This subsection recognizes that an individual has a continuing interest in information about him collected by the government.[76] For the first time, an individual can examine his records and ensure their accuracy.

The access provisions in subsection (d) are also the key to enforcing the other provisions of the Privacy Act. The Act relies almost exclusively on individual initiative for enforcement.[77] Consequently, unless the individual has access to his files, he will lack both the knowledge and the incentive to challenge agency lapses. If an agency fails to maintain the list of disclosures required by subsection (c),[78] or retains stale and unreliable information in violation of subsections (e)(1) and (e)(5),[79] the individual can take corrective action only if he learns of the violation via the access provision of subsection (d).[80] The enforcement of the entire Act, therefore, depends on the efficacy of subsection (d) in granting individuals access to their files.

On this critical point, the Privacy Act's sound concepts are as a practical matter deficient. The original Senate bill required agencies to take affirmative action to notify every subject of the existence of a government file about him.[81] The abandonment of this provision

72. 5 U.S.C. § 552a(d)(1) (Supp. V 1975).

73. 5 U.S.C. § 552a(d)(2)-(4) (Supp. V 1975).

74. For a discussion of these provisions, see OMB Guidelines, *supra* note 69, at 28,958-60.

75. *See* note 24 *supra.*

76. *See* S. REP. No. 93-1183, *supra* note 6, at 20. An agency may not refuse the subject access to a record because of lack of proper interest. *See* OMB Guidelines, *supra* note 69, at 28,957.

77. *See* notes 136-57 *infra.*

78. 5 U.S.C. § 552a(c) (Supp. V 1975); *see* note 85 *infra.*

79. *See* notes 115 & 124 *infra.*

80. The individual may learn of the existence of a record if an agency requests his consent prior to disclosing a record about him pursuant to subsection (b) (conditions of disclosure). Unfortunately the broad exemptions and the general "prior consent" provision to subsection (b) will frequently prevent an individual from discovering the existence of personal records about him. *See* note 91 *infra* and accompanying text.

81. *See* S. REP. No. 93-1183, *supra* note 6, at 59; note 89 *infra.*

threatens to render the Act entirely unenforceable. An individual will not know that he is the subject of a record unless he initiates a request under subsection (d). He can exercise his rights under this provision only after combing the *Federal Register* to discover which agencies maintain records and contacting each agency that could conceivably have a record about him.[82] Relatively few individuals have sufficient time, money, knowledge, and initiative to attempt to discover the existence of files about them, much less begin proceedings to challenge the contents of a file. Accordingly, subsection (d) is commendable for recognizing the individual's continued interest in personal information held by the government. As a mechanism to enforce the Privacy Act, however, it is virtually worthless.

3. *Disclosure of Records*

The Privacy Act recognizes another crucial aspect of the individual's continuing interest in government held data concerning him—limiting its disclosure.[83] Subsection (b) addresses this goal, providing that unless one of eleven exemptions applies, "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the *prior written consent* of the individual to whom the record pertains. . . ."[84] Subsection (c) enables an individual to assure agency compliance with subsection (b) by requiring agencies to keep an accounting of the date, nature, purpose, and recipient of each disclosure.[85]

---

82. *See* notes 96-98 *infra* and accompanying text.

83. *See* S. REP. No. 93-1183, *supra* note 6, at 68.

84. 5 U.S.C. § 552a(b) (Supp. V 1975) (emphasis added). Neither this, nor any other provision of the Privacy Act authorizes disclosure to a person other than the subject of a record. *See* OMB Guidelines, *supra* note 69, at 28,953.

85. 5 U.S.C. § 552a(c) (Supp. V 1975). The accounting is intended: 1) to enable individuals to discover those to whom their records have been disclosed; 2) to facilitate the correction of erroneous records; and 3) to allow individuals to force agency compliance with the disclosure provisions of subsection (b).

Subsection (c)(2) requires agencies to retain all accountings "for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made." 5 U.S.C. § 552a(c)(2) (Supp. V 1975). This provision was the result of a compromise between the House and Senate Committees. *See* 120 CONG. REC. S21,817 (daily ed. Dec. 17, 1974). Subsection (c)(3) requires agencies to allow the subject of a record to examine any accounting but those required for law enforcement

Once again these provisions are conceptually sound. In the past, interagency transfers of personal information were routine,[86] and raised substantial problems of contextual inaccuracy.[87] More serious is the inequity of disclosing the individual's personal information for uses he has never contemplated and of which he would not approve.[88] An enforceable consent requirement would not only obviate these problems, but would, in addition, partially compensate for the Act's failure to require notification to individual subjects of records.[89] The request for permission to disclose personal records will notify the subject of their existence, permitting him to exercise his rights under subsection (d).[90]

For two reasons, however, subsection (b) may fail to fulfill these additional and necessary roles. First, the provision in subsection (b) permitting disclosure without notice to, or specific consent by, subjects who have given prior written consent[91] opens a major loophole. Agencies may attempt to evade the consent requirement by simply inserting routine waiver provisions in the original request for information. Accordingly, courts should construe this provision narrowly and reject an agency's claim of prior consent absent a clause in the original request specifically stipulating not only the anticipated uses, but the potential recipients of the data as well.[92] Second, the exemptions to the consent requirement are far too broad and threaten to destroy the individual's ability to control the flow of personal information. Sub-

---

purposes pursuant to subsection (b)(7). *See* note 167 *infra*. No accounting is necessary for disclosures required by the FOIA. *See* notes 259-61 *infra* and accompanying text).

86. *See* note 28 *supra*.

87. *See* notes 27-28 *supra*.

88. *See* note 28 *supra*.

89. The original draft of the Senate bill required an agency to notify all individuals about whom the agency maintained personal information. This requirement was abandoned due to the allegedly prohibitive cost of notification. Instead, the Act relies totally on the initiative of concerned citizens to seek out information pertaining to them. *See* S. REP. No. 93-1183, *supra* note 6, at 59.

The Senate bill also provided for a Privacy Commission responsible in part for publishing a Directory of Information Systems designed to enable individuals to discover easily if an agency maintained a personal record about them. The Act as passed contains no such provision, and individuals who wish to learn if any personal records about them exist must study the Federal Register religiously. *See* notes 100-06 *infra* and accompanying text.

90. *See* notes 72-74 *supra*.

91. *See* text accompanying note 84 *supra*.

92. *See* OMB Guidelines, *supra* note 69, at 28,954. Informing an individual of the purpose for which information will be used does not constitute prior consent to disclosure of such information. *Id.*

section (b)(3), for instance, is perhaps the largest loophole in the Privacy Act. This subsection allows an agency to disclose personal records to other agencies without the subject's consent if the disclosure is for a "routine use."[93] The Act defines a routine use as one whose "purpose . . . is compatible with the purpose for which [the record] was collected."[94] The original Senate bill contained no such exemption and would have placed tight restrictions on interagency transfers of information.[95] Under the enacted statute, however, an agency need only publish anticipated routine uses in the *Federal Register*.[96] Few Americans are aware of the existence of the *Federal Register*; still fewer read it on a regular basis.[97] Consequently, most individuals will never learn that an agency has declared a routine use and will be unable to challenge effectively wrongful agency declarations.

As a practical matter, subsection (b) does not significantly restrict interagency transfers; it merely requires agencies to consider in advance how information will be used.[98]

C. *Restrictions on Federal Agencies*

To complement and solidify the individual interests recognized in the Privacy Act, Congress imposed specific limitations on federal agencies that gather and use personal information. The substantive restrictions contained in subsections (b) and (e) parallel the individual interests they are designed to promote.[99] These substantive rules govern collection of new data, maintenance of new and existing files, and disclosure of agency records.

The Act also establishes various procedural requirements, of which

---

93. 5 U.S.C. § 552a(b)(3) (Supp. V 1975).

94. 5 U.S.C. § 552a(a)(7) (Supp. V 1975). This exemption is intended to "recognize the practical limitations of restricting use of information to explicit and express purposes for which it was collected." OMB Guidelines, *supra* note 69, at 16-17. One harmless example of a routine use given in the OMB Guidelines is the transfer of information from an agency to the Treasury Department for processing of payroll checks. *Id.*

95. *See* S. REP. NO. 93-1183, *supra* note 6, at 72-73. This provision constitutes a major concession to the House. *See* 120 CONG. REC. S21,815 (daily ed. Dec. 17, 1974).

96. 5 U.S.C. § 552a(e)(4)(D) (Supp. V 1975).

97. *But see* Project, *supra* note 12, at 1316.

98. *See* 120 CONG. REC. S21,816 (daily ed. Dec. 17, 1974); OMB Guidelines, *supra* note 69, at 28,953.

99. *See* notes 62-98 *supra* and 100-33 *infra* and accompanying text.

subsection (e)(4)[100] is the most critical. This subsection requires each agency that maintains a system of records to publish an annual notice in the *Federal Register* of the existence, character, name, and location of each system.[101] The annual notice must also specify the categories of individuals about whom information is maintained,[102] the kind of information maintained,[103] all routine uses of such data,[104] procedures by which an individual may discover if an agency's system contains a record about him,[105] and how he may gain access to the record.[106]

These procedural restrictions serve several functions. Public disclosure of the existence of record systems gives meaning to the Act's premise that there must be no secret information systems,[107] and helps

100. 5 U.S.C. § 552a(e)(4) (Supp. V 1975).

101. 5 U.S.C. § 552a(e)(4)(A) (Supp. V 1975). A "system of records" is defined as a group of any records under the control of any agency from which information 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) (emphasis added). The Act defines the term record as

> any item, collection, or grouping of information about an individual that is maintained by an agency, including but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or . . . other identifying particular assigned to the individual . . . . 5 U.S.C. § 552a(a)(4) (Supp. V 1975).

Although the broad definition of the term "record" will preclude agencies from refusing to comply with the Act on the pretext that an element of personal information does not constitute a record, the term "system of records" is potentially a major loophole in the Act. Virtually all provisions of the Privacy Act only apply to an agency if it *maintains a system of records.* This is a legitimate limitation with respect to subsections (e)(4)(publishing requirements) and (d) (access requirements). There is no justification, however, for applying this limitation to subsections (b) (conditions of disclosure) and (c) (accounting of disclosures). The effects of failing to apply these subsections to an agency that does not maintain a system of records are disastrous. First, these agencies can disclose personal information to anyone for any purpose. Second, the individual has no control over the use of information. Finally, agencies can avoid the Act entirely by claiming that personal records under their control do not compromise a "system." The Act itself provides no specific guidelines to aid in the determination of whether a group of records constitutes a system and those provided in the OMB Guidelines are insufficient. *See* OMB Guidelines *supra* note 69, at 28,963. The Guidelines merely admonish agencies: "systems . . . should not be subdivided or reorganized so that information which would otherwise have been subject to the Act is no longer subject to the Act."

102. 5 U.S.C. § 552a(e)(4)(B) (Supp. V 1975).

103. 5 U.S.C. § 552a(e)(4)(C) (Supp. V 1975).

104. 5 U.S.C. § 552a(e)(4)(D) (Supp. V 1975).

105. 5 U.S.C. § 552a(e)(4)(E)-(H) (Supp. V 1975).

106. 5 U.S.C. § 552a(e)(4)(H) (Supp. V 1975).

107. *See* S. REP. No. 93-1183, *supra* note 6, at 2; H.R. REP. No. 93-1416, *supra* note 54, at 4; OMB Guidelines, *supra* note 69, at 28,962.

preclude a government institution like the Army from ever again maintaining secret files on millions of law-abiding American citizens.[108] The procedural rules also enable individuals to exercise their right to inspect and challenge the contents of personal files, and thereby assist in the enforcement of the Act.[109]

The procedural rules will implement effectively the goals of the Privacy Act only to the extent that the substantive restrictions on the agencies are workable. To a disturbing degree, however, the substantive rules exhibit the same flaws as those sections of the Act that recognize individual interests. While conceptually sound, the substantive agency restrictions will often prove pragmatically worthless.

1. *Collection of New Data*

Subsection (e) of the Privacy Act contains explicit restrictions on the federal agencies' ability to gather new information. Subsection (e)(2)[110] recognizes the principle that the best source of accurate data about a person is the individual himself. Thus, agencies must "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 . . . ."[111]

As usual, this provision is soundly conceived. Congress properly recognized that information provided by third parties is often erroneous or biased.[112] Moreover, a requirement that agencies collect information from the subject of a record furthers the individual's interest in knowing of the existence of files about him and limiting the government's collection of personal data.[113] The major flaw in subsection (e)(2) is not conceptual but mechanical: the Act provides no criteria by which agencies or courts can determine when it is "impractical" to collect information directly from the subject. Apparently, the agencies

108. *See* note 16 *supra.*
109. *See* OMB Guidelines, *supra* note 69, at 28,962.
110. 5 U.S.C. § 552a(e)(2) (Supp. V 1975).
111. *Id.*
112. *See* OMB Guidelines, *supra* note 69, at 28,961.
113. *See* 120 CONG. REC. S21,817 (daily ed. Dec. 17, 1974) ("[A]n individual should to the greatest extent possible be in control of information about him which is given to the government.").

have effective discretion to decide the question themselves,[114] and the laudable purpose of subsection (e)(2) is largely unenforceable.

Subsection (e)(1),[115] which limits the kind of information that agencies may collect, is perhaps the most workable provision of the Act. Subsection (e)(1) requires an agency to "maintain in its records only such information about an individual as is *relevant and necessary* to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President."[116] Underlying this requirement are the congressional judgments that agencies should never acquire personal information unless necessary to the performance of a legitimate function, and that data neither collected nor maintained cannot be misused.[117] This provision should preclude agencies from asking such questions as those appearing on many civil service applications during the 1960's:

I believe there is a God.
I believe in the *second coming* of Chirst.
I go to church almost every week.
I am very strongly attracted by members of *my own sex.*
I loved my father.
My sex life is satisfactory.[118]

Even if such inquiries were relevant to job performance, the agency would be hard-pressed to defend their necessity in accordance with (e)(1).[119] Moreover, although the enforcement provisions of the Act are generally weak, it may be difficult for agencies to ignore the subsection

---

114. *See* OMB Guidelines, *supra* note 69, at 28,961 (providing relevant considerations); Project, *supra* note 12, at 1311-15 (criticizing subsection (e)(2)).

115. 5 U.S.C. § 552a(e)(1) (Supp. V 1975).

116. *Id.* (emphasis added).

117. *See* S. REP. No. 93-1183, *supra* note 6, at 45; OMB Guidelines, *supra* note 69, at 28,960.

118. Ervin, *The First Amendment: A Living Thought in the Computer Age, reprinted in Data Bank Hearings* (pt. II), *supra* note 11, at 1550, 1552; *see* S. REP. No. 93-1183, *supra* note 6, at 11.

119. The OMB Guidelines recognize necessity as a requirement and declare the following kinds of questions as guidelines for determining whether information is relevant and necessary:

1) How does the information relate to the purpose (in law) for which the system is maintained?; 2) What are the adverse consequences, if any, of not collecting the information?; 3) Does the information have to be in individually identifiable form?; 4) How long must the information be retained?; 5) What is the financial cost of maintaining the record compared to the risks/adverse consequences of not maintaining it? OMB Guidelines, *supra* note 69, at 28,960.

(e)(1) relevance and necessity requirement because agency collection practices are highly visible to the public.[120]

2. *Maintenance of Files*

The Privacy Act imposes several restrictions on agencies to complement the recognition of the individual's interest in accurate and timely personal records. If the Act's collection restraints are effective, records compiled after 1974 should be substantially correct when initially compiled. A major problem confronting Congress in drafting privacy legislation, however, was how to ensure the correction of inaccurate, dated, or incomplete records compiled before the passage of the statute and the continued updating of all records.[121] Congress sought to achieve these goals in two ways. First, agencies must grant individuals access to their records and correct information contained therein that is erroneous or otherwise fails to comply with the Act. The deficiencies of these provisions have been noted previously.[122] The Act also imposes a general duty on agencies to maintain only relevant and necessary information and a specific duty to ensure its accuracy and timeliness before using it to make a determination about a subject.

Subsection (e)(1), discussed previously, applies to the maintenance of new and existing agency files as well as to the collection of new data. Agencies should review their record systems on a periodic basis to ensure compliance with the "relevant and necessary" requirement of subsection (e)(1).[123] Although the rationale for this requirement applies as strongly to existing records as it does to the acquisition of new data, compliance in the former instance may be harder to achieve. Because the inner workings of the agencies are hidden from public view, pressure to update old records will be far less than pressure to force compliance with collection regulations. Thus, the absence of an adequate mechanism to enforce the Act will probably result in noncompliance.

---

120. *But see* Project, *supra* note 12, at 1305-08.

121. For discussion of problems with records compiled before the Privacy Act, see notes 18-36 *supra* and accompanying text.

122. *See* notes 81-82 *supra* and accompanying text.

123. *See* OMB Guidelines, *supra* note 69, at 28,961 (agencies should insure that record systems comply with subsection (e)(1): (1) in preparing public notices, (2) in developing new information systems, (3) upon changing a system, (4) at least annually).

The Privacy Act also imposes a specific duty on agencies to ensure the accuracy and timeliness of information used in making determinations about a subject. Subsection (e)(5) requires agencies to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination . . . ."[124] Although the desirability of accurate information in personal files should be self-evident, this section is a substantially watered down version of the measure originally proposed in the Senate. The Senate bill imposed a heavy burden on the agencies, requiring them to ensure that information contained in a record was accurate, relevant, timely, and complete whenever the record was disclosed, used to make determinations about the subject, or altered.[125] The compromise that emerged[126] as subsection (e)(5) of the Privacy Act accepts the House provision and requires an agency to assure the quality of only those records "which are used by the agency *in making any determination* about an individual."[127] Unfortunately, even if an agency does delete information in making a determination about an individual, it will undoubtedly consider such data when making the determination.[128] Consequently, the stated purpose of subsection (e)(5), fair determinations, will probably be the exception. Moreover, subsection (e)(5) will probably fail to fulfill the broader goal of accomplishing the destruction or correction of the vast quantity of existing information that violates the Privacy Act.

3. *Disclosure and Dissemination*

The recognition of an individual's continuing interest in government-held data that concerns him required the imposition of restrictions on the dissemination practices of federal agencies. The Privacy Act attempts to provide such restrictions in two ways.

---

124. 5 U.S.C. § 552a(e)(5) (Supp. V 1975).

125. *See* S. REP. No. 93-1183, *supra* note 6, at 50.

126. *See* 120 CONG. REC. S21,816 (daily ed. Dec. 17, 1974).

127. 5 U.S.C. § 552a(e)(5) (Supp. V 1975) (emphasis supplied).

128. Since all records except those compiled for statistical purposes, *see* subsection (a)(6), *may* be used to make determinations, this section could be interpreted to require agencies to insure the quality of all records but those subject to subsection (a)(6). *Cf.* OMB Guidelines, *supra* note 69, at 28,961 (similar argument made in discussion of subsection (e)(2)). Nevertheless, the legislative history conflicts with this interpretation and its adoption is unlikely.

First, subsection (b)[129] requires an agency to obtain the subject's consent before disclosing personal records. The problems of enforcing this subsection and the exemptions that largely defeat it have been noted.[130] The second restriction on agency dissemination is subsection (e)(6),[131] which requires that an agency "prior to disseminating any record about an individual to any person *other than an agency*, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes . . . ."[132] Once again, this subsection is conceptually sound and practically unenforceable. Its purpose is to assure that agencies transmit only reliable information to persons outside the federal government. Because the restrictions in the Privacy Act apply only to federal agencies, the subject of a record can not gain access to, or correct errors in, records disclosed to persons outside the federal government. Data disseminated to such persons should, therefore, be of the highest possible quality.[133] In practice, this subsection is likely to prove unenforceable. The individual can challenge an agency's decision to ignore this provision only by exercising his right of access under subsection (d). As noted above, the failure to provide individuals with effective notice of the existence of their records renders subsection (d) a useless enforcement device.[134] Moreover, subsection (e)(6) is inapplicable to material disclosed under the Freedom of Information Act—probably the largest category of disclosures made to persons "other than an agency."[135]

The substantive restrictions on agency practices, therefore, parallel almost exactly the individual interests recognized under the Privacy Act. In each case, the inability to enforce them obviates the value of conceptually sound approaches to protecting informational privacy. These deficiencies, and the manifold exemptions, render the Privacy Act little more than a legislative statement of unenforceable rights.

---

129. 5 U.S.C. § 552a(b) (Supp. V 1975).
130. *See* notes 84-98 *supra* and accompanying text.
131. 5 U.S.C. § 552a(e)(6) (Supp. V 1975).
132. *Id.* (emphasis added).
133. *See* 120 CONG. REC. S21,816 (daily ed. Dec. 17, 1974).
134. *See* notes 81-82 *supra* and accompanying text.
135. *See* notes 263-66 *infra* and accompanying text.

D. *Civil Remedies*

Subsection (g)[136] of the Privacy Act establishes civil remedies enabling individuals to seek equitable relief or damages from agencies that violate the Act. Other than criminal penalties of very limited scope,[137] these provisions are the only means to enforce the agency restrictions and implement the individual interests recognized in the Privacy Act. The original Senate bill provided for an independent Privacy Commission with power to investigate, hold hearings upon, and recommend prosecution of agency violations.[138] The legislative compromise replaced this body with a purely advisory commission,[139] leaving sole responsibility for enforcing the Act to individual citizens. Unfortunately, subsection (g) provides neither the tools nor the incentives necessary to make individual enforcement a reality.

Subsection (g) permits equitable relief in two situations. If the agency disregards the access provisions of subsection (d),[140] the individual may seek injunctive relief to force the agency to let him inspect his records.[141] If the agency refuses to amend a record upon request, or fails to review the individual's request for amendment as provided in subsection (d)(3),[142] the victim may also seek a court order compelling the agency to amend the record.[143] In both cases, the courts must determine the matter de novo and are empowered to award costs and attorney's fees to a substantially successful plaintiff.[144]

In addition, an individual may seek damages from an agency that

> fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be

136. 5 U.S.C. § 552a(g) (Supp. V 1975).

137. 5 U.S.C. § 552a(i) (Supp. V 1975).

138. *See* S. REP. No. 93-1183, *supra* note 6, at 23-24. The Senate Committee concluded an independent commission was essential to enforcement of the Act.

139. Privacy Act of 1974, Pub. L. No. 93-579, § 5, 88 Stat. 1896.

140. 5 U.S.C. § 552a(g)(1)(B) (Supp. V 1975).

141. 5 U.S.C. § 552a(g)(3)(A) (Supp. V 1975).

142. 5 U.S.C. § 552a(g)(1)(A) (Supp. V 1975).

143. 5 U.S.C. §§552a(g)(2)(A), (g)(3)(A) (Supp. V 1975). The only apparent difference between suits brought under these subsections is that under (g)(2)(A) the individual has the burden of proving that the agency wrongfully refused to amend a record while under (g)(3)(A) the agency must justify its refusal to grant access to the subject of a record. *See* OMB Guidelines, *supra* note 69, at 28,969.

144. 5 U.S.C. § 552a(g)(2)(B) (Supp. V 1975).

> made on the basis of such record, *and consequently a determination is made which is adverse to the individual*;[145] or fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as do [*sic*] have an adverse effect on an individual.[146]

Damages are only recoverable, however, if the agency acted "in a manner which was intentional or willful,"[147] in which case the individual is entitled to an award of actual damages or $1000, whichever is greater,[148] plus his costs and reasonable attorney's fees.[149] Punitive damages are not recoverable. To obtain any relief, plaintiff must normally file suit within two years after the violation occurs.[150]

It is unrealistic to expect these remedial provisions to provide adequate incentives for individuals to seek redress under the Act. First, the Act imposes an unreasonably heavy burden on the plaintiff. He must allege and prove that he has suffered an adverse determination in consequence of the agency's violation of the Act, and that the agency acted willfully or intentionally. Most plaintiffs will fail to meet these burdens. The most prevalent threats to privacy stem not from intentional action but from "inadvertent, careless, and unthinking collection, distribution, and storage of records."[151] Requiring proof of willful misbehavior assures that most abuses will go uncorrected. The requirement that the plaintiff must have suffered an adverse determination in

---

145. 5 U.S.C. § 552a(g)(1)(C) (Supp. V 1975) (emphasis added). The Guidelines define an adverse determination as "one resulting in the denial of a right, benefit, entitlement, or employment by an agency which the individual could reasonably have expected to have been given if the record had not been deficient." OMB Guidelines, *supra* note 69, at 28,969.

146. 5 U.S.C. § 552a(g)(1)(D) (Supp. V 1975).

147. 5 U.S.C. § 552a(g)(4) (Supp. V 1975). "On a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct, this standard is viewed as only somewhat greater than gross negligence." 120 CONG. REC. S21,817 (daily ed. Dec. 17, 1974).

148. 5 U.S.C. § 552a(g)(4)(A) (Supp. V 1975).

149. 5 U.S.C. § 552a(g)(4)(B) (Supp. V 1975). Unlike (g)(2) and (g)(3), which make the award of court costs and attorneys' fees discretionary, under (g)(4) costs and attorneys' fees are mandatory when an agency is adjudged liable. *See* OMB Guidelines, *supra* note 69, at 76.

150. 5 U.S.C. § 552a(g)(5) (Supp. V 1975). The Act contains an exception to this requirement when

> an agency has *materially and willfully misrepresented* any information required . . . to be disclosed to an individual and the *information so misrepresented is material to establishment of the liability* of the agency to the individual . . . the action may be brought at any time within two years after *discovery* by the individual of the misrepresentation. (emphasis added).

151. S. REP. NO. 93-1183, *supra* note 6, at 24.

order to recover is also unfortunate. Many agency violations will not result in determinations or cause measurable injury, further isolating agency abuse from corrective action.

Second, the Act provides insufficient recovery to stimulate private suits. Even if the plaintiff can prove actual injury, the damage award may be small. The Act's failure to provide for punitive damages virtually guarantees that the financial risks of the litigation will often exceed the rewards of the suit. The $1000 guarantee is a meager incentive to risk the expense of suing the federal government.[152] The Act thus fails to provide the adequate level of damages essential to effective citizen enforcement.

Finally, the two-year statute of limitations is unreasonable. Because agencies need not notify individuals when making adverse determinations based on personal records,[153] many individuals aggrieved by agency violations will not learn the cause of their injury until after the statute of limitations has run.

The enforcement scheme in the original Senate bill was far superior to that in the Act as passed. A strong Privacy Commission was expected to share responsibility for enforcing the Act.[154] The original Senate bill imposed liability for negligent as well as willful violations,[155] and authorized recovery of punitive damages where appropriate.[156]

---

152. *See* Project, *supra* note 12, at 1330: "The floor on recovery . . . presumably represents a compromise between the House proposal, which only allowed recovery of actual damages, and the Senate proposal, which allowed recovery of punitive damages where appropriate." (footnotes omitted).

153. *See* note 150 *supra* and accompanying text.

154. The Senate bill provided for an independent privacy commission responsible for: 1) monitoring and inspecting new information systems, 2) compiling a directory of information systems to enable individuals to take advantage of rights granted under the Act, and 3) investigating and holding hearings upon violations of the Act. *See* S. REP. No. 93-1183, *supra* note 60, at 23-24.

155. *See* S. 3418, § 303(c), 93d Cong., 2d Sess. (1974). ("Any person who violates the provisions of this Act . . . shall be liable to any person aggrieved thereby in an amount equal to the sum of—(1) any actual damages . . . (2) punitive damages where appropriate . . ."). *See also* 120 CONG. REC. S21,817 (daily ed. Dec. 17, 1974). Additionally, the Senate bill obligated the Attorney General to "challenge in court any violation of the Act which might affect the public at large, but which does not yet affect any particular citizen sufficiently . . . to induce a private person to endure the practical difficulties of litigation." S. REP. No. 93-1183, *supra* note 6, at 83. The omission of this crucial provision was inexcusable, particularly in light of the failure to allow punitive damages.

156. *See* text accompanying notes 135-36 *supra*.

Substitution of the House provisions in the final Act has once again reduced the Privacy Act to a legislative statement of unenforceable rights.

IV. The Privacy Act and the Social Need for Information

The first two goals of the Privacy Act—recognizing the continuing individual interest in government-held data, and restricting the information practices of federal agencies—are essentially compatible. As the original Senate bill demonstrates, drafting a statute that accomplishes these goals would have been a relatively easy task. The Act's third goal—striking an appropriate balance between the individual privacy interest and the legitimate social needs for information—is far more difficult to achieve. Resolving the conflict between these essentially incompatible interests requires a thorough understanding of each, and a well defined sense of their relative importance. The most formidable task facing Congress in drafting the Privacy Act, therefore, was the accommodation of individual privacy with such interests as administrative efficiency, effective law enforcement, and the public's right to know.

Unfortunately, those sections of the Privacy Act that consider other social interests are among the most ill-conceived sections of the Act. In virtually every instance when privacy conflicted with other legitimate objectives, Congress merely chose to sacrifice privacy. In protecting the two most important social interests—effective law enforcement and the public's right to know—the complete sacrifice of privacy significantly frustrates the operation of the Act. Moreover, in each instance, it is apparent that privacy need not have been wholly subordinated to the other interest: Congress could have struck a better balance. Examination of the interaction between the Freedom of Information Act (FOIA)[157] and the Privacy Act, and of the law enforcement exemptions to the latter, illustrates this thesis.

A. *The Law Enforcement Exemptions*

The social interest in enforcing the criminal law is clear. Equally obvious is the occasional sacrifice of individual liberties that effective law enforcement requires. During the last decade, however, agencies such as the FBI and the CIA perpetrated some of the most insidious in-

157. 5 U.S.C. § 552 (1970).

vasions of privacy in the name of "law and order." Curbing abusive practices by law enforcement agencies without seriously impairing their legitimate functions is a difficult task for any statute. One of the most disturbing aspects of the Privacy Act is its failure to evidence even an attempt to accomplish this goal.

Subsections (j)[158] and (k)[159] permit an agency to exempt certain types of record systems from many crucial provisions of the Act. Although no record system is automatically exempt, the head of an agency can easily obtain an exemption by determining that a system qualifies for exemption under subsection (j) or (k) and filing an appropriate notice in the *Federal Register*.[160]

Subsection (j) grants a blanket exemption to all record systems maintained by the CIA.[161] Other agencies or sub-agencies whose principal function pertains to the enforcement of criminal laws may exempt a system of records if it consists of one of three specific kinds of data.[162] Although subsection (j) enumerates ten sections to which the exemption is supposedly inapplicable, in practice the subsection grants immunity from almost every significant restriction in the Act.[163] For example, subsection (j) does not allow an exemption from the notice and consent provisions of subsection (b).[164] Under subsection (b)(7), however, any law enforcement agency of any governmental unit can acquire personal records without either notice to, or consent by, the subject, if the agency head requests the records in writing and certifies that they will be used for law enforcement purposes.[165] Similarly, although law enforcement agencies are not exempt from subsections (c)(1) and (c)(2), requiring an accounting of all disclosures,[166] subsection (c)(4) relieves agencies of the duty to make accountings of (b)(7) disclosures

158. 5 U.S.C. § 552a(j) (Supp. V 1975).

159. 5 U.S.C. § 552a(k) (Supp. V 1975).

160. *See* OMB Guidelines, *supra* note 69, at 28,971-72.

161. 5 U.S.C. § 552a(j)(1) (Supp. V 1975).

162. 5 U.S.C. § 552a(j)(2) (Supp. V 1975). Specifically, to qualify for exemption under subsection (j)(2), a record system must consist of information: a) compiled for the purpose of identifying suspects and offenders and which consists only of identifying data, *e.g.*, rap sheets; b) information compiled as part of a criminal investigation; or c) identifiable records compiled at any stage of the law enforcement process.

163. Subsection (j) does not exempt records from the requirements of subsections (b), (c)(1) and (2), (e)(4)(A)-(F), (e)(6), (7), (9), (10) and (11) and (i). 5 U.S.C. § 552a(j) (Supp. V 1975).

164. *See* note 84 *supra* and accompanying text.

165. 5 U.S.C. § 552a(b)(7) (Supp. V 1975).

166. *See* note 85 *supra* and accompanying text.

available to the subject on request.[167] Finally, although these agencies cannot, under subsection (j), escape the ban on collecting information about the exercise of first amendment rights,[168] subsection (e)(7) explicitly permits collection of such data if "pertinent to and within the scope of an authorized law enforcement activity."[169]

The only substantive restrictions from which law enforcement agencies can never gain immunity require them to exercise reasonable efforts to assure the reliability of, and obtain the individual's consent before disclosing, personal files to persons other than law enforcement agencies.[170] Neither provision is meaningful. The exceptions to the consent requirement of subsection (b) virtually nullify the rule.[171] The reliability restriction of subsection (e)(6) is wholly unenforceable against law enforcement agencies because subsection (j) permits exemption from the civil remedies provisions, and violation of this requirement would not constitute grounds for criminal prosecution.[172]

Subsection (k) enables an agency to exempt seven different types of records from various provisions of the Act.[173] These exemptions are not limited to record systems maintained by law enforcement agencies,[174] but they are not as extensive as those allowed under subsection (j). Subsection (k)(2), available to law enforcement records not covered by subsection (j), permits an agency to exempt

> investigatory material compiled for law enforcement purposes, other than material within the scope of Subsection (j)(2) . . . . *Provided, however*, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except 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 [of confidentiality], or, prior to the effective date of this [Act], under an implied promise [of confidentiality].[175]

167. 5 U.S.C. § 552a(c)(3) (Supp. V 1975).
168. *See* note 167 *supra* and accompanying text.
169. 5 U.S.C. § 552a(e)(7) (Supp. V 1975).
170. 5 U.S.C. § 552a(e)(6) & (b) (Supp. V 1975).
171. *See* note 169 *supra.*
172. *See* 5 U.S.C. § 552a(i) (Supp. V 1975) (restricting criminal penalties to violations of disclosure or notice provisions).
173. *See* 5 U.S.C. § 552a(k) (Supp. V 1975); OMB Guidelines, *supra* note 69, at 28,972-74.
174. *See* 5 U.S.C. § 552a(k)(1)-(7) (Supp. V 1975).
175. 5 U.S.C. § 552a(k)(2) (Supp. V 1975).

Virtually every law enforcement record qualifies for an exemption under either subsection (j) or (k)(2).[176] Although the statutory language suggests otherwise, there are but two significant distinctions between the exemptions available under these two subsections.[177] First, while an agency relying on subsection (k)(2) must ordinarily provide damaging information to an individual adversely affected by its use,[178] subsection (j) contains no such requirement. The second important distinction is that only subsection (j) exempts agencies from the civil remedies provisions of subsection (g).[179]

From the broad immunity conferred upon law enforcement agencies flows the unfortunate conclusion that Congress apparently believed legitimate law enforcement needs should always take priority over any individual privacy interest. The only legitimate grounds for exempting law enforcement records, however, are the need to protect the secrecy of a pending investigation, the safety of undercover agents, and the secrecy of certain investigative techniques.[180] None of these reasons justifies providing agencies wholesale immunity from the individual access

176. *See* Project, *supra* note 12, at 1332-36.

177. The remaining differences between subsections (j) and (k) are either unnecessary or unwarranted, and pragmatically insignificant. Subsection (j) allows an exemption from subsection (e)(2) (requiring agencies to collect information directly from subject to the "greatest extent practicable," *see* notes 110-11 *supra* and accompanying text), while subsection (k)(2) does not. This difference is meaningless because in criminal investigations it will obviously be impracticable to obtain most information from a suspect. Subsection (k)(2), unlike subsection (j), does not permit exemption from the requirements of subsection (e)(3), requiring agencies to inform the subject of the purpose and authority for requests for information. *See* notes 62-63 *supra*. This difference is also meaningless because most law enforcement agencies acquire information about a suspect from third parties, and subsection (e)(3) does not apply to requests made of third parties. *See* Project, *supra* note 12, at 1310.

The final distinction between subsections (j) and (k)(2) is that only the former permits an agency to ignore the requirements of subsection (e)(5) requiring agencies to insure the quality of records used in making determinations. *See* note 124 *supra* and accompanying text. This exemption is not only unwarranted, it is unnecessary given the discretion allowed law enforcement agencies elsewhere in the Act regarding the kinds of information they may acquire.

178. The legislative history emphasizes that courts should construe narrowly the exception that permits withholding information to protect the confidentiality of sources. Additionally, the Guidelines direct agencies to make express promises of confidentiality sparingly and to inform other sources that their identities may be disclosed. *See* 120 CONG. REC. S21,816 (daily ed. Dec. 17, 1974); OMB Guidelines, *supra* note 69, at 28,973.

179. *See* notes 135-44 *supra* and accompanying text.

180. *See* note 217 *infra* and accompanying text (discussing FOIA exemption).

and challenge provisions or from civil liability.[181] Subsection (j) should include the caveat contained in subsection (k)(2),[182] modified only as necessary to protect the legitimate government interests outlined above. Finally, it is astonishing to note that an individual is more likely to acquire his personal record from a law enforcement agency by means of an FOIA suit than by one brought under the Privacy Act.[183] A rational statutory scheme would surely recognize that the subject of a personal record has a greater interest in it than does the general public; the Privacy Act does not. Although an agency cannot withhold information from an individual based on a Privacy Act exemption when the FOIA requires disclosure,[184] the approach taken in the Privacy Act is extremely disturbing. It strongly suggests that Congress intended to protect privacy only when it conflicted with no other legitimate social interests. Because privacy conflicts with other interests more often than not, such an approach guarantees little protection to individual privacy.

The conclusion is inescapable that Congress refused to analyze in depth the conflict between privacy and law enforcement. Instead, whenever it perceived a conflict, Congress sacrificed the privacy interest without considering whether the marginal benefit to law enforcement exceeded the marginal cost to privacy. Consequently, the Pri-

---

181. *See* H.R. REP. No. 93-1416, *supra* note 54, at 37-39 (additional views of Reps. Abzug, Moss, Stanton, Gude, Burton, Fasell, Culver, Collins, Rosenthal, Conyers, Jr.):

> By narrowing the exemption categories and defining them in specific terms related to the use of records rather than to the agency maintaining them, Congress could provide agency heads with standards to meet in exercising their . . . authority to grant exemptions. Only in this way can we be assured that the Constitutional rights of individuals will be protected and will not be sacrificed to administrative discretion, expendiency or whim.

See also 120 CONG. REC. H12,248 (daily ed. Dec. 18, 1974) (remarks of Representative Koch). The failure to limit the exemptions for law enforcement agencies to active criminal investigations is unfortunate, particularly in light of experience under the seventh exemption to the FOIA prior to the 1974 amendments. *See* notes 219-22 *infra* and accompanying text.

182. *See* text accompanying note 175 *supra.*

183. The exemptions to the Privacy Act would often permit an agency to withhold a record from the subject where the FOIA would require disclosure. In these situations, "the Privacy Act should not be used to deny access to information about an individual which would otherwise have been *required* to be disclosed to that individual under the Freedom of Information Act." Office of Management and Budget, Implementation of the Privacy Act of 1974 (Supplementary Guidance), 40 Fed. Reg. 56,741, 56,742-43 (1975).

184. *Id.*

vacy Act needlessly excludes a principal enemy of individual privacy, law enforcement agencies, from its substantive restrictions.

B. *Privacy and the Public's Right to Know*

The public's right to know is, almost by definition, the antithesis of the individual's right to privacy.[185] The individual's interest in restricting disclosure of personal facts is almost directly opposed to the public interest in expanding public knowledge to ensure informed, democratic decision-making. Although the right to know may have constitutional foundations,[186] since 1966 its most significant legal base has been the Freedom of Information Act (FOIA).[187]

Material disclosed to the public under the FOIA is largely exempt from the Privacy Act. Subsection (b), requiring agencies to notify and obtain the consent of the subject of a personal record before releasing it,[188] is expressly inapplicable to material whose disclosure is required by the FOIA.[189] Under subsection (c)(1) agencies need not keep an accounting of the release of such materials.[190] Finally, subsection (e)(6), requiring agencies to make reasonable efforts to ensure the reliability of records released to persons other than an agency, does not apply when the FOIA requires disclosure.[191]

Congress obviously chose to subordinate the Privacy Act to the FOIA whenever it perceived a potential conflict between the interests protected by each Act. Because several provisions of the FOIA purport to safeguard privacy, Congress may have assumed that the FOIA had struck an appropriate balance between personal privacy and the right to know. Closer inspection of the FOIA, however, reveals that for two reasons, the Act as presently interpreted cannot protect individual privacy. First, courts interpreting the FOIA exemptions have almost completely ignored privacy interests. More fundamentally, because only the agency can invoke an exemption, the FOIA places the responsibil-

185. *See* Emerson, *Legal Foundations of the Right to Know*, 1976 WASH. U.L.Q. 1, 20.

186. For discussion of the constitutional dimensions of the right to know, see Emerson, *supra* note 185.

187. 5 U.S.C. § 552 (1970).

188. *See* note 84 *supra* and accompanying text.

189. 5 U.S.C. § 552a(b)(2) (Supp. V 1975).

190. 5 U.S.C. § 552a(c)(1) (Supp. V 1975).

191. 5 U.S.C. § 552a(e)(6) (Supp. V 1975).

ity of protecting individual privacy in the wrong hands—with the agency rather than the individual.

1. *The FOIA Exemptions*

A brief explanation of the operation of the FOIA is necessary to understand its inability to protect individual privacy. The FOIA directs federal agencies to release identifiable records to "any person" on request.[192] If the agency fails to comply, the individual may seek injunctive relief from the federal courts.[193] The agency bears the burden of justifying its action; unless one of nine specifically defined exemptions applies, the citizen must prevail.[194] The FOIA was intended to achieve maximum public access to government records[195] in order to develop an informed electorate capable of wisely selecting and monitoring the government.[196] In recognition of this basic purpose, courts have narrowly interpreted the exemptions.[197]

---

192. 5 U.S.C. § 552(a)(3) (1970).

193. 5 U.S.C. § 552(a)(4)(B)(Supp. IV 1974).

194. 5 U.S.C. § 552(c) (1970).

195. *See, e.g.*, Department of the Air Force v. Rose, 425 U.S. 352, 360-61 (1976); EPA v. Mink, 410 U.S. 73, 80 (1973); Bristol-Meyers Co. v. FTC, 424 F.2d 935, 938 (D.C. Cir.), *cert. denied*, 400 U.S. 824 (1970). For a general review of the FOIA, see Note, *The Freedom of Information Act: A Seven Year Assessment*, 74 COLUM. L. REV. 895 (1974). *See also* EPA v. Mink, *supra*; Department of the Air Force v. Rose, *supra*; Note, *The Freedom of Information Act and Equitable Discretion*, 51 DEN. L.J. 263 (1974); Note, *The Investigatory Files Exemption to the FOIA: The D.C. Circuit Abandons Bristol-Meyers*, 42 GEO. WASH. L. REV. 869 (1974); 40 GEO. WASH. L. REV. 527, 527-29 (1970).

196. *See, e.g.*, Soucie v. David, 448 F.2d 1067, 1080 (D.C. Cir. 1971); H.R. REP. No. 89-1497, 89th Cong., 2d Sess. 12 (1966) ("A democratic society requires an informed, intelligent electorate, and the intelligence of the electorate varies as the quantity and quality of its information varies.").

197. *See, e.g.*, Ditlow v. Shultz, 517 F.2d 166 (D.C. Cir. 1975); Rose v. Department of the Air Force, 495 F.2d 261, 263 (2d Cir. 1974), *aff'd*, 425 U.S. 352 (1976); Vaughn v. Rosen, 484 F.2d 820, 823 (D.C. Cir. 1973), *cert. denied*, 415 U.S. 997 (1974); Soucie v. David, 448 F.2d 1067 (D.C. Cir. 1971); Wellford v. Hardin, 444 F.2d 21, 24 (4th Cir. 1971); Bristol-Meyers Co. v. FTC, 424 F.2d 935, 938 (D.C. Cir.), *cert. denied*, 400 U.S. 824 (1970); M.A. Schapiro & Co. v. SEC, 339 F. Supp. 467 (D.D.C. 1972); Note, *Access to Broadcasters' Financial Statements Filed with the FCC, The Freedom of Information Act Alternative*, 42 GEO. WASH. L. REV. 145, 155-56 (1973); Note, *The Plain Meaning of the Freedom of Information Act: NLRB v. Getman*, 47 IND. L.J. 530, 543 (1972); Note, *Public Disclosure of Internal Revenue Service Private Letter Rulings*, 40 U. CHI. L. REV. 832, 844-55; 45 IND. L.J. 421.

Courts and commentators agree that the FOIA is a poorly drafted statute. *See, e.g.*, Epstein v. Resor, 421 F.2d 930, 932 (9th Cir.), *cert. denied*, 398 U.S. 965 (1970);

Three exemptions to the FOIA are relevant to personal privacy interests. Exemption four permits agencies to withhold "trade secrets and commercial or financial information obtained from a person and privileged or confidential."[198] Although the statutory language and the legislative history support the application of this exemption to all types of confidential information,[199] courts now agree that exemption four protects only privileged or confidential information which is commercial in nature.[200] Information is confidential for purposes of exemption four only if its disclosure would injure either the government's ability to obtain information in the future or the competitive position of the party supplying the information.[201]

Davis, *The Information Act: A Preliminary Analysis*, 34 U. CHI. L. REV. 761 (1967); Note, *The Freedom of Information Act, The Parameters of the Exemptions*, 62 GEO. L.J. 177 (1973). The statutory language is vague, confusing, and inconsistent with the House and Senate Reports, which in turn, conflict with each other. *See* Davis, *supra*, at 762-63; Note, *The Investigatory Files Exemption to the FOIA: The D.C. Circuit Abandons Bristol-Meyers*, 42 GEO. WASH. L. REV. 869, 872-75 (1974); Note, *The Freedom of Information Act: A Critical Review*, 38 GEO. WASH. L. REV. 150, 150-58 (1969); Note, *Public Disclosure of Internal Revenue Service Private Letter Rulings*, 40 U. CHI. L. REV. 832, 839-42 (1973). The House Report and the Attorney General's Memorandum, which generally follows it, *see* UNITED STATES DEPARTMENT OF JUSTICE, ATTORNEY GENERAL'S MEMORANDUM ON THE PUBLIC INFORMATION SECTION OF THE ADMINISTRATIVE PROCEDURE ACT III (1967) [hereinafter cited as ATTORNEY GENERAL'S MEMORANDUM] frequently give priority to the interests of privacy and confidentiality at the expense of disclosure. They conflict with the Senate Report, which emphasizes the Act's goal of providing for broad disclosure. In an attempt to further what they view as the purpose of the FOIA, courts interpreting the Act have ignored the House Report and the Attorney General's Memorandum.

198. 5 U.S.C. § 552(b)(4) (1970).

199. The House and Senate Reports explicitly state that the fourth exemption protects confidential information that is neither commercial nor financial. *See* S. REP. No. 89-813, 89th Cong., 2d Sess. 9 (1965); H.R. REP. No. 89-1497, *supra* note 196, at 10. Courts have disregarded the legislative history because it was drawn from an earlier version of the bill that explicitly protected noncommercial information. *See* Brockway v. Department of the Air Force, 518 F.2d 1184 (8th Cir. 1975). Professor Davis sadly concludes that the legislative history is inadequate support for the proposition that confidential noncommercial information may be exempt. He insists that courts should go outside the Act to protect confidential information. *See* Davis, *supra* note 197, at 788-92.

200. *See* National Parks & Conservation Ass'n v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974) (leading case). *See also* Continental Oil Co. v. FPC, 519 F.2d 31, 35 (5th Cir. 1975); Getman v. NLRB, 450 F.2d 670, 673 (D.C. Cir. 1971); 88 HARV. L. REV. 470 (1974). For discussion of various possible interpretations of the fourth exemption, see ATTORNEY GENERAL'S MEMORANDUM, *supra* note 197, at 32; Davis, *supra* note 197, at 787 (criticizing Attorney General).

201. *See* National Parks & Conservation Ass'n v. Morton, 498 F.2d 765, 770 (D.C. Cir. 1974).

The rationale for this interpretation is instructive. Courts have restricted the coverage of exemption four in order to further the perceived goal of the FOIA: maximum disclosure of public records. They have failed to recognize that maximum disclosure was merely a means to accomplish the FOIA's ultimate goal—governmental accountability.[202] While the two will often be synonymous, courts have failed to recognize that disclosing confidential noncommercial information could seriously injure privacy interests without contributing significantly to the public interest in government accountability. In short, they have failed to distinguish between different types of government-held information.[203] If there is to be an intelligent compromise between the interests of personal privacy and public knowledge, however, such distinctions are critical. In light of the Privacy Act, one can plausibly argue for reinterpretation of this exemption on the ground that its disclosure impedes the policies underlying the Privacy Act without furthering those of the FOIA.[204]

Exemption six permits the withholding of "personnel and medical files and similar files the disclosure of which would constitute a *clearly unwarranted invasion of personal privacy*."[205] The most significant question to arise under this exemption concerns the standard by which a court should determine when disclosure would produce a "clearly unwarranted invasion of personal privacy." Several courts have held that subsection (a)(3), requiring agencies to release information to "any person,"[206] precludes any balancing of the consequences of disclos-

---

202. *See* HEW REPORT, *supra* note 1, at 64-65. The FOIA amended the original Public Information Section of the Administrative Procedure Act, Act of June 11, 1946, ch. 324, § 3, 60 Stat. 238, under which an agency could withhold records if the information were "required for good cause to be held confidential," or if the requesting individual were not "properly and directly concerned." *Id.*

By simply labeling information exempt, agencies converted this section from a disclosure provision into a withholding act. *See, e.g.*, EPA v. Mink, 410 U.S. 73, 79 (1973); H.R. REP. No. 89-1497, *supra* note 196, at 4; S. REP. No. 89-813, *supra* note 199, at 3.

In order to eliminate such agency abuse and insure government accountability, the FOIA established a presumption in favor of disclosure to "any person."

203. *See* Comment, *The Freedom of Information Act's Privacy Exemptions and the Privacy Act of 1974*, 11 HARV. C.R.-C.L. L. REV. 596 (1976).

204. For discussion of the possible impact of the Privacy Act upon interpretation of the FOIA, see notes 253-54 *infra* and accompanying text.

205. 5 U.S.C. § 552(b)(6) (1970) (emphasis added).

206. 5 U.S.C. § 552(a)(3) (1970).

ure.[207] Several other courts, while agreeing that the Act ordinarily prohibits balancing, insist that the sixth exemption requires an exemption.[208] These courts hold that the words "clearly unwarranted invasion of privacy" leave no alternative to weighing the public benefit of disclosure against the private injury from invasion of privacy.

Both of these positions have problems. The requirement that agencies release information to "any person" was an unfortunate product of congressional frustration with agencies who abused the original disclosure section of the Administrative Procedure Act by withholding information under the pretext that the requesting party "was not properly concerned." In many instances, however, the standing of the party seeking information *is* a relevant consideration. As the Privacy Act demonstrates, the subject of a record clearly has a greater interest in examining it than does the general public. Moreover, it is impossible to determine if a given disclosure will produce an unwarranted invasion of personal privacy without considering what the requesting party intends to do with the information—*i.e.*, his need. Strict adherence to the "any person" requirement and failure to consider the interests of the requesting party preclude sensible resolution of problems arising under the sixth exemption. The recent Supreme Court decision in *Department of the Air Force v. Rose*[209] has evidently settled the basic issue. The Court held that Congress adopted the exemptions to "require a balancing of the individual's right of privacy against the preservation of the basic purpose of the Freedom of Information Act—'to open agency action to the light of public scrutiny.' "[210]

The balancing approach, however, suffers from its own deficiencies. As courts and commentators noted before *Rose*, this approach may pro-

207. *See* Robles v. EPA, 484 F.2d 843, 847 (4th Cir. 1973). *See also* Project, *supra* note 12, at 1080-85; 40 GEO. WASH. L. REV. 527, 535-36 (1972).

208. *See* Wine Hobby USA, Inc. v. IRS, 502 F.2d 133 (3d Cir. 1974); Rural Housing Alliance v. United States Dep't. of Agriculture, 498 F.2d 73, 78 (D.C. Cir. 1974); Rabbitt v. Department of the Air Force, 383 F. Supp. 1065, 1070 (S.D.N.Y.). *See also* Note, *The Plain Meaning of the Freedom of Information Act: NLRB v. Getman*, *supra* note 197, at 530. *See* Davis, *supra* note 197, at 806:

> This policy choice reflects pressure from the press that the public as a whole has a right to know and does not reflect a thoughtful rejection of the balancing approach that has been a part of all judge made law. When the time comes for further legislation, I think this policy choice might well be re-examined.

See also note 202 *supra*.

209. 425 U.S. 352 (1976).

210. *Id.* at 372.

duce perverse results. When little or no public benefit will result from disclosure, balancing mandates disclosure in the absence of a serious invasion of privacy. Similarly, when the anticipated benefit is significant, this approach would require disclosure even if it would unwarrantably invade personal privacy.[211]

The correct approach to interpreting the sixth exemption would require courts to consider the needs of the FOIA plaintiff solely for the purpose of determining the most likely effect of disclosure on the subject. If disclosure would produce a significant invasion of privacy, the exemption should attach in all cases except those involving high public officials,[212] in which case the strong public interest in disclosure would seem to leave courts no alternative to balancing interests.

Exemption seven was one of two exemptions amended in 1974.[213] In its original form, the seventh exemption permitted agencies to withhold "investigatory files compiled for law enforcement purposes except to the extent available by law to a party other than an agency."[214] Courts uniformly held this exemption applicable to investigatory files compiled for civil as well as criminal law enforcement purposes.[215]

The 1974 amendment was designed to overrule a series of decisions by the Court of Appeals for the District of Columbia that permitted the indefinite withholding of law enforcement files despite the absence of any legitimate purpose.[216] The seventh exemption now shields from disclosure

---

211. *See* sources cited note 207 *supra.*

212. For another feasible solution, see Comment, *supra* note 203, at 619-24.

213. The other exemption amended in 1974 was subsection (b)(1), pertaining to national security.

214. 5 U.S.C. § 552(b)(7) (1970) (amended 1974).

215. *See, e.g.*, Center for Nat'l Policy Review on Race & Urban Issues v. Weinberger, 502 F.2d 370, 373 (D.C. Cir. 1974); Aspin v. Department of Defense, 491 F.2d 24 (D.C. Cir. 1973); Cooney v. Sun Shipbuilding & Drydock Co., 288 F. Supp. 708 (E.D. Pa. 1968); Clement Bros. Co. v. NLRB, 282 F. Supp. 540 (N.D. Ga. 1968).

216. Prior to the 1974 amendments, courts split sharply over whether an agency attempting to invoke exemption seven was required to demonstrate that proceedings based upon requested investigatory files were either pending or reasonably likely in the near future. Courts deciding most of the early cases under the seventh exemption demanded such a showing. *See, e.g.*, Wellford v. Hardin, 444 F.2d 21 (4th Cir. 1971); Bristol-Meyers Co. v. FTC, 424 F.2d 935, 938 (D.C. Cir.), *cert. denied*, 400 U.S. 824 (1970) (government may not label all files investigatory on the possibility that proceedings may be launched in future—possibility must be concrete); M.A. Schapiro & Co. v. SEC, 339 F. Supp. 467 (D.D.C. 1972); Frankel v. SEC, 336 F. Supp. 675 (S.D.N.Y. 1971), *rev'd on other grounds*, 460 F.2d 813 (2d Cir.), *cert. denied*, 409 U.S. 889

> investigatory records compiled for law enforcement purposes, but only to the extent that the production of such records would (A) interfere with enforcement proceedings, (B) deprive a person of a right to a fair trial or an impartial adjudication, (C) *constitute an unwarranted invasion of personal privacy*, (D) disclose the identity of a confidential source and, in the case of a record compiled by a criminal law enforcement authority in the course of a criminal investigation, or by an agency conducting a lawful national security investigation, confidential information furnished only by the confidential source, (E) disclose investigative techniques and procedures, or (F) endanger the life or safety of law enforcement personnel.[217]

The amendment narrows the exemption by requiring proof that disclosure would interfere with either pending or imminent law enforcement proceedings. The addition of subsection (b)(7)(c), protecting personal privacy, however, constitutes a significant expansion of the exemption.[218] Before the 1974 amendments, courts interpreting exemption seven generally found that the exemption was designed exclusively to protect the government's case in court and preserve the secrecy of

---

(1972). *See also* Note, *The Investigatory Files Exemption, supra* note 86; 1974 WASH. U.L.Q. 463. The 1973 decisions by the Court of Appeals for the District of Columbia, however, held that once the court determined that an investigatory file had been compiled for law enforcement purposes its task was completed. The exemption attached indefinitely, and the unlikelihood or impossibility of future proceedings was immaterial. Center for Nat'l Policy Review on Race & Urban Issues v. Weinberger, 502 F.2d 370 (D.C. Cir. 1974); Rural Housing Alliance v. Department of Agriculture, 498 F.2d 73 (D.C. Cir. 1974); Ditlow v. Brinegar, 494 F.2d 1073 (D.C. Cir. 1974); Aspin v. Department of Defense, 491 F.2d 24 (D.C. Cir. 1973); Weisberg v. Department of Justice, 489 F.2d 1195 (D.C. Cir. 1973) (en banc), *cert. denied*, 416 U.S. 993 (1974). *See also* Evans v. Department of Transp., 446 F.2d 821 (5th Cir. 1971), *cert. denied*, 405 U.S. 918 (1972); Koch v. Department of Justice, 376 F. Supp. 313, 315 (D.D.C. 1974); Cowles Communications, Inc. v. Department of Justice, 325 F. Supp. 726 (N.D. Cal. 1971).

These decisions permitted the indefinite withholding of governmental information when no legitimate purpose was served. For discussion of the District of Columbia Circuit opinions, see Clark, *Holding Government Accountable: The Amended Freedom of Information Act*, 84 YALE L.J. 741, 761-63 (1975); Note, *The Investigatory Files Exemption to the FOIA: The D.C. Circuit Abandons Bristol-Meyers, supra* note 195. The legislative history clearly reveals a congressional intent to overrule these decisions. *See* 120 CONG. REC. S9336 (daily ed. May 30, 1974):

> (Mr. Kennedy) Does the amendment in effect override the court decisions in the court of appeals on Weisberg against the United States; Aspin against Department of Defense; Ditlow against Brinegar; and National Center against Weisberger?
>
> (Mr. Hart) . . . That is its purpose.

217. 5 U.S.C. § 552(b)(7) (Supp. V 1975) (emphasis added).

218. *See* Clark, *supra* note 216, at 762-63.

investigative techniques.[219] The privacy of the subjects of investigations was completely ignored.[220] Yet the individual privacy interest is far from trivial. Law enforcement agencies have great freedom to decide whom to investigate; public disclosure of investigatory files about an individual may produce unwarranted public humiliation,[221] particularly when no further proceedings, against him are contemplated. In these instances, disclosure would often constitute the de facto conviction of an individual who, for one reason or another, could not be prosecuted in a court of law. The earlier decisions by the District of Columbia Circuit allowing the indefinite withholding of files for purely governmental reasons inadvertently protected the individual against such disclosures.[222]

The requirement of an "unwarranted invasion of personal privacy" under amended exemption seven is no clearer than that of a "clearly unwarranted" invasion under exemption six.[223] Presumably, courts would apply similar criteria for each exemption. Whether the criteria

219. Courts generally held that the seventh exemption was designed exclusively to protect governmental interests. *See* Sears, Roebuck & Co. v. GSA, 384 F. Supp. 996, 1004 (D.D.C. 1974) ("exemption (b)(7) is clearly designed to protect interests of the government only."). *See also* Moore-McCormack Lines, Inc. v. I.T.O. Corp., 508 F.2d 945 (4th Cir. 1974); Weisberg v. Department of Justice, 489 F.2d 1195, 1199 (D.C. Cir. 1973); Getman v. NLRB, 450 F.2d 670, 673 (D.C. Cir. 1971); Wellford v. Hardin, 444 F.2d 21, 23-24 (4th Cir. 1971); Legal Aid Soc'y v. Shultz, 349 F. Supp. 771, 777 (N.D. Cal. 1972); Katz, *The Games Bureaucrats Play: Hide and Seek Under the Freedom of Information Act*, 48 TEX. L. REV. 1261, 1277 (1970).

220. For example, several courts held exemption seven inapplicable if an individual were aware of the contents of a file since no harm to the government would result from disclosure. *See* Wellford v. Hardin, 444 F.2d 21, 24 (4th Cir. 1971); Sears, Roebuck & Co. v. GSA, 384 F. Supp. 996, 1004 (D.D.C. 1974); Ditlow v. Volpe, 362 F. Supp. 1321, 1325 (D.D.C. 1973), *rev'd on other grounds*, 494 F.2d 1073 (D.C. Cir.), *cert. denied*, 419 U.S. 974 (1974); Legal Aid Soc'y v. Shultz, 349 F. Supp. 771, 776 (N.D. Cal. 1972). *But see* Center for Nat'l Policy Review on Race & Urban Issues v. Weinberger, 502 F.2d 370, 373-74 (D.C. Cir. 1974) (recognizing the need to protect the privacy of the subjects of past investigations); Cowles Communications, Inc. v. Department of Justice, 325 F. Supp. 726 (N.D. Cal. 1971) ("[I]n this day of increasing concern over the conflict between the citizen's right of privacy and the need of the Government to investigate, it is unthinkable that rights of privacy should be jeopardized further by making investigatory files available to private persons").

221. *See* Center for Nat'l Policy Review on Race & Urban Issues v. Weinberger, 502 F.2d 370, 374 (D.C. Cir. 1974); Cowles Communications, Inc. v. Department of Justice, 325 F. Supp. 726, 729 (N.D. Cal. 1973).

222. The District of Columbia Circuit cases effectively protected a subject's privacy because the exemption attached indefinitely once a court concluded that an investigatory file had been compiled for law enforcement purposes. *See* note 216 *supra*.

223. *See* notes 198-204 *supra*.

actually employed will effectively safeguard individual privacy interests remains to be seen.[224]

Interpretation of the original exemption seven complemented and closely paralleled the treatment accorded exemption four,[225] illustrating again the judicial myopia toward personal privacy interests under the FOIA. In both instances, courts ignored substantial individual interests and failed to consider whether disclosure would further the goal of the FOIA: improving government accountability. In considering both the advantages and the disadvantages of disclosure, therefore, courts consistently undervalued the privacy interest in nondisclosure and overvalued the utility of release. Although the exemptions as currently written might effectively safeguard personal privacy, the judicial bias against privacy in FOIA suits has ominous implications for the balancing process now required by exemptions six and seven.

2. *The Agencies as Guardians of Privacy*

More fundamental problems with the FOIA as a guardian of privacy are inherent in the structure of the Act. The FOIA is a disclosure statute—disclosure is never prohibited.[226] In general, federal agencies rather than individuals are responsible for claiming the exemptions. Neither the FOIA nor the Privacy Act[227] requires an agency to notify the subject of a record that information about him has been requested under the FOIA. Accordingly, when an individual surrenders personal information to an agency, he effectively appoints that agency legal guardian of his right to privacy.[228] Unfortunately, the agency is an incompetent guardian.

The FOIA assumes that the agencies will vigorously assert each applicable exemption because their interest always lies in withholding information. Ordinarily, agency interests coincide with the interests protected by the exemptions, and accordingly, this assumption is perfectly sound. The Department of State, for example, will always

224. For further discussion of the seventh exemption, see Project, *supra* note 12, at 1085-1101.

225. *See* notes 205-12 *supra* and accompanying text.

226. *See* Davis, *supra* note 197, at 806. *See also* A. MILLER, THE ASSAULT ON PRIVACY: COMPUTERS, DATA BANKS, AND DOSSIERS 154 (1971).

227. *See* notes 81-82 *supra* and accompanying text.

228. For a good discussion of this problem, see O'Reilly, *Government Disclosure of Private Secrets Under the Freedom of Information Act*, 30 BUS. L. REV. 1125 (1975).

want to protect national security information from disclosure.[229] Because the agency is the best and most logical representative of these interests, it is the proper party to assert the exemption. This critical assumption of the FOIA is incorrect, however, when applied to the privacy exemptions. Unlike national security, the agency has no inherent interest in protecting individual privacy; the incentive for a strong defense is missing.[230] Moreover, judicial interpretation of the FOIA has compounded this structural defect. To prevent frivolous claims of exemptions, courts have made it increasingly difficult for agencies to withhold information. In the leading case of *Vaughn v. Rosen*,[231] the Court of Appeals for the District of Columbia held that conclusory allegations would not support a claim of exemption.[232] Instead, the agency must make a "relatively detailed analysis [of the material] in manageable segments,"[233] and specify which parts should be exempt and why.[234] The *Vaughn* index is an excellent means to discourage recalcitrant agencies from indulging their usual preference for secrecy. In the context of the privacy exemptions, however, the disincentives far outweigh the minimal benefits the agency obtains from withholding personal information. Many agencies may prefer to disclose information rather than fight,[235] especially in light of the absence of any penalty for wrongful disclosure under the FOIA.

---

229. *See* Note, *Executive Privilege and the Freedom of Information Act: The Constitutional Foundation of the Amended National Security Exemption*, 1976 WASH. U.L.Q. 609.

230. HEW REPORT, *supra* note 1, at 65. The HEW REPORT correctly recognizes that the FOIA "is an instrument for disclosing information rather than for balancing the conflicting interests that surround the public disclosure and use of personal records." *Id.* at 35. The REPORT urged: "that the [FOIA] be amended to require an agency to obtain the consent of an individual before disclosing in personally identifiable form exempted-category data about him, unless the disclosure is within the purposes of the system as specifically required by statute." *Id.* at 65-66. The REPORT correctly notes that although adopting such an amendment might result in less disclosure, it would not detract from the effectiveness of the FOIA.

231. 484 F.2d 820 (D.C. Cir. 1973), *cert. denied*, 415 U.S. 977 (1974).

232. *Id.* at 825.

233. *Id.* at 826.

234. *Id.* at 827.

235. *Vaughn* properly held that an agency wishing to reap the benefits of an exemption must show that withholding is justified. The problem is that an agency frequently derives no benefit from an exemption that protects individuals' interests. Thus, in those instances the *Vaughn* requirements are inappropriate. The FOIA should be amended to prohibit disclosure of personal information unless the subject of the data is given notice and an opportunity to be heard. *See* HEW REPORT, *supra* note 1, at 35-36;

Before the Privacy Act, the majority of courts further exacerbated this problem by finding that an agency could disclose information notwithstanding the applicability of one of the nine exemptions—that is, the exemptions are merely discretionary.[236] To permit the government to waive exemptions designed to protect its own interests makes perfect sense; to allow the government to waive the individual interests underlying exemptions four, six, and seven, however, is ludicrous. These exemptions should be mandatory.[237] Even if an agency is compelled to assert an exemption, however, its claim is likely to be halfhearted. The FOIA thus contains an inherent procedural defect that significantly reduces its ability to protect personal privacy.

Courts have proven insensitive to the problem of the wrong party in interest. The issue has arisen in a few "reverse FOIA" suits, in which plaintiffs have attempted to prevent disclosure of trade secrets protected by the fourth exemption.[238] These suits present problems comparable to the privacy exemptions because the agency's interest in retaining future information sources is not wholly synonomous with in-

---

O'Reilly, *supra* note 228. For a discussion of *Vaughn*, see 87 HARV. L. REV. 854 (1974).

236. *See* Charles River Park "A", Inc. v. Department of HUD, 519 F.2d 935 (D.C. Cir. 1975); Moore-McCormack Lines, Inc. v. I.T.O. Corp., 508 F.2d 945, 950 (4th Cir. 1974); Davis, *supra* note 197, at 76 ("[t]he exemptions protect against required disclosure, not against disclosure"). Although the question has been sparsely litigated, the legislative history supports the view that agencies have discretion to release exempt information. *See* S. REP. No. 93-854, 93d Cong., 2d Sess. (1974) 6: "Congress did not intend the exemptions . . . to be used either to prohibit disclosure of information or to justify automatic withholding of information. Rather, they are only permissive." *See also* Project, *supra* note 12, at 158-60; Note, *Access to Broadcasters' Financial Statements Filed with the FCC: The Freedom of Information Act Alternative, supra* note 197, at 157; Note, *Freedom of Information: The Statute and the Regulations*, 56 GEO. L.J. 18, 28 (1967). *But see* note 237 *infra*.

237. *See* Continental Oil Co. v. FPC, 519 F.2d 31, 35-36 (5th Cir. 1975) (agency cannot always disclose even if subject to exemption); Westinghouse Elec. Corp. v. Schlesinger, 392 F. Supp. 1246, 1250 (E.D. Va. 1974); McCoy v. Weinberger, 386 F. Supp. 504, 506 (W.D. Ky. 1974).

238. *See* Charles River Park "A" Inc. v. HUD, 519 F.2d 935 (D.C. Cir. 1975); Babcock & Wilcox Co. v. Rumsfeld, 70 F.R.D. 595 (N.D. Ohio 1976); Westinghouse Elec. Corp. v. Schlesinger, 392 F. Supp. 1246 (E.D. Va. 1974); Neal-Cooper Grain Co. v. Kissinger, 385 F. Supp. 769 (D.D.C. 1974); Sears Roebuck & Co. v. GSA, 384 F. Supp. 996 (D.D.C.), *stay dissolved*, 509 F.2d 527 (D.C. Cir. 1974); Hughes Aircraft Co. v. Schlesinger, 384 F. Supp. 292 (C.D. Cal. 1974). For discussion of reverse FOIA suits in general, see Project, *supra* note 12, at 1157-62; Comment, *Reverse-Freedom of Information Act Suits: Confidential Information in Search of Protection*, 70 NW. U.L. REV. 995 (1976).

dustry's interest in keeping trade secrets. Although courts have granted the reverse FOIA plaintiff standing to sue,[239] the agency decision on the merits usually prevails.[240] Courts reason that Congress granted agencies the sole power to assert an exemption, and the agency decision is reversible only if arbitrary or capricious.[241] Those parties challenging release, and the one court that has enjoined disclosure have relied, at least in part, on statutory provisions outside the FOIA.[242] The courts have yet to realize that some exemptions protect a variety of public and private interests and that public agencies cannot be expected to assert purely private interests.

This brief review of the FOIA highlights the degree to which both Congress and the courts have misunderstood the complex interaction between individual privacy and government accountability. If Congress, in drafting the Privacy Act, did assume that the FOIA struck an appropriate balance between these two competing interests, the assumption is plainly wrong. The subject of a personal record, not its governmental custodian, is harmed by its disclosure. Yet only the latter may invoke the FOIA exemptions.[243] In construing the privacy

239. *See* Comment, *supra* note 238, at 1000 (no court has denied standing, but no court has considered the problem either).

240. Charles River Park "A" Inc. v. HUD, 519 F.2d 935 (D.C. Cir. 1975); Neal-Cooper Grain Co. v. Kissinger, 385 F. Supp. 769 (D.D.C. 1974) (denial of preliminary injunction); Sears Roebuck & Co. v. GSA, 384 F. Supp. 996 (D.D.C.), *stay dissolved*, 509 F.2d 527 (D.C. Cir. 1974); Hughes Aircraft Co. v. Schlesinger, 384 F. Supp. 292 (C.D. Cal. 1974); *cf.* Moore-McCormack Lines, Inc. v. I.T.O. Corp., 508 F.2d 945, 950 (4th Cir. 1974) (dictum that agencies have complete discretion to release exempt information).

241. Charles River Park "A" Inc. v. HUD, 519 F.2d 935, 941-43 (D.C. Cir. 1975); Babcock & Wilcox Co. v. Rumsfeld, 70 F.R.D. 595, 601 (N.D. Ohio 1976); Comment, *supra* note 238, at 1011-13.

242. *See* Westinghouse Elec. Corp. v. Schlesinger, 392 F. Supp. 1246, 1250 (E.D. Va. 1974) (relying in part on 18 U.S.C. § 1905 (1970) in granting relief in reverse FOIA suit); Sears Roebuck & Co. v. GSA, 384 F. Supp. 996, 1001-02, *stay dissolved*, 509 F.2d 527 (D.C. Cir. 1974) (rejecting several statutory grounds on which reverse FOIA plaintiff had relied).

243. In addition to the exemptions, two provisions of the Act authorize agencies to delete identifying details from materials the disclosure of which would otherwise produce an unwarranted invasion of privacy. *See* 5 U.S.C. § 552(a)(2) & (b) (Supp. V 1975). The addition to section (b) requires that "[a]ny reasonably segregable portion of a record shall be provided to any person requesting such record after deletion of the portions which are exempt . . . ." While subsection (b) may permit broader disclosure, it does not alter the exemptions or give agencies a greater incentive to invoke them. For discussion of this provision, see Project, *supra* note 12, at 1046.

exemptions, the courts usually overstate the public value of releasing personal data and ignore the privacy interest in nondisclosure.[244]

On a more fundamental level, the subordination of the Privacy Act to the FOIA again exposes the congressional preference for a simplistic statute to the difficult task of balancing and reconciling competing interests. This decision is tragic, not only because it wholly sacrifices privacy but because the sacrifice is unnecessary. Identifiable personal records have little to do with the FOIA's ultimate goals of developing an informed electorate and improving government accountability. Protecting individuals from the release of such files would significantly advance personal privacy interests with minimal effect on the underlying values served by the FOIA. As it did in drafting the law enforcement exemptions,[245] however, Congress preferred to adopt a blanket solution rather than make the hard choices required to fashion an effective and comprehensive approach to resolving the conflict between personal privacy and the public's right to know. In so choosing, Congress gave new meaning to Arthur Miller's plaintive lament that "in a very backhanded way, [the FOIA] probably does more to end privacy in the United States, ostensibly in pursuit of the public's right to know, than any other enactment in the last fifty or sixty years."[246]

---

244. Courts have blindly pursued a policy of demanding broad disclosure and have forgotten that "broad disclosure" was merely the means adopted under the FOIA to enable the public to know about *how the Federal Government conducts its activities*. *See* HEW REPORT, *supra* note 1, at 64. When that policy mandates the disclosure of personal information which not only fails to further the primary goal of the Act, but also threatens the equally important societal goal of protecting personal privacy, then it is time to re-evaluate that policy. Perhaps, as Judge MacKinnon admonished in his concurring opinion to Getman v. NLRB, 450 F.2d 670, 681 (D.C. Cir. 1971), amendment of the FOIA is the only alternative:

> [This] is not the sort of disclosure that Congress basically had in mind in enacting the [FOIA]. But in my opinion the Act as it presently exists practically requires the disclosure of [names and addresses] on demand. One need not elaborate on the various abuses that could result if lists of people as classified by the Government for particular purposes became available practically on demand in wholesale lots. If this situation is to be corrected, it will require an amendment to the Act.

For additional arguments in favor of amending the FOIA, see A. MILLER, *supra* note 226, at 154-61; A. WESTIN, *supra* note 2, at 387; *Data Bank Hearings, supra* note 11, at 826 (statement of A. Westin); Davis, *supra* note 197, at 291.

245. *See* note 196 *supra* and accompanying text.

246. *Data Bank Hearings, supra* note 11, at 25 (statement of A. Miller).

3. *Interaction between the FOIA and the Privacy Act*

The congressional decision to exempt FOIA information from many of the substantive requirements of the Privacy Act has some curious and probably unintended consequences. The interaction of the two statutes illustrates, as nothing else, the complete congressional failure to understand the complexity of the privacy problem. In general, the Privacy Act subordinates substantial privacy interests to insignificant FOIA interests. In some respects, however, the Privacy Act may encourage a reinterpretation of the FOIA, improving the latter Act's ability to protect individual privacy interests. Nevertheless, the FOIA's defects are so great, and the congressional intent to leave it unchanged so apparent, that amendment of the FOIA is probably the only means to strike the correct balance between the individual's right to privacy and the public's right to government information.

The consent provisions in subsection (b) of the Privacy Act best illustrate Congress' inability to comprehend the inadequacy of the FOIA's privacy exemptions. Subsection (b) prohibits disclosure of a personal record without the subject's consent.[247] Subsection (b)(2) waives this requirement for material whose disclosure is required by the FOIA.[248] The original House bill contained no such provision and was intended to "make all individually identifiable information in government files exempt from public disclosure" under the FOIA.[249] The original Senate bill exempted all records whose disclosure was either *required or permitted* by the FOIA.[250] Although the final draft of the Senate bill omitted this provision,[251] an altered version of it mysteriously reappeared in the Compromise Amendments and the Act as passed.[252]

247. 5 U.S.C. § 552a(b) (Supp. V 1975). *See* note 84 *supra* and accompanying text.

248. 5 U.S.C. § 552a(b)(2) (Supp. V 1975).

249. H.R. REP. NO. 93-1416, *supra* note 54, at 3.

250. S. REP. NO. 93-1183, *supra* note 6, at 71.

> This provision was included to meet the objections of press and media representatives that the statutory right of access to public records and the right to disclosure of government information might be defeated if such restrictions were placed on the public and press. The Committee believed it would be unreasonable and contrary to the spirit of the Freedom of Information Act to attempt keep, [*sic*] an accounting of the nature and purpose of access and disclosures involving the press and public or to impose guarantees of security and confidentiality on the data they acquire.

251. *See* 120 CONG. REC. S19,831 (daily ed. Nov. 21, 1974). The provision appeared to have been abandoned; no explanation was given.

252. *See* 120 CONG. REC. S21,816 (daily ed. Dec. 17, 1974).

The final version of subsection (b) is a distinctly mixed blessing. In limiting the waiver of the consent requirement to instances in which the FOIA *requires* disclosure, it improves both the original Senate proposal and the FOIA by removing agency discretion to waive the FOIA privacy exemptions.[253] Specifically, if one of these exemptions applies, the FOIA does not *require* disclosure, subsection (b) of the Privacy Act still applies, and the Privacy Act *prohibits* disclosure absent the subject's consent. A corollary of this requirement is a significant improvement in the success of reverse FOIA suits. When courts have rejected such suits on the merits, the rationale has been agency discretion to waive or assert the privacy exemptions.[254] By depriving agencies of that discretion, subsection (b) makes the privacy exemptions mandatory and grants the reverse FOIA plaintiff a legal right under the Privacy Act to prevent disclosure.

Unfortunately, the structural defects in the Privacy Act and the FOIA largely nullify the practical benefit of making the FOIA privacy exemptions mandatory. A reverse FOIA suit is possible only if the subject learns of the request for his personal records in time to object. Because neither Act requires agencies to notify the subject of such requests,[255] the agency may disclose personal information before he can assert his rights. In practice, therefore, the wrong party in interest—the agency—must still assert the exemption. The agency's probable failure to represent individual interests vigorously may result in the disclosure of personal information that should remain confidential.[256]

Technically, such halfhearted agency action may violate the Privacy Act. Indeed, one commentator has noted with alarm the agencies' exposure to FOIA suits if they invoke the exemption, and to damage suits under the Privacy Act if they fail to assert it.[257] This dilemma is wholly theoretical. The plaintiff's burden of proof in a damage suit under the Privacy Act is so great that only in rare cases can the victim expect recovery.[258] In any reasonably close case, disclosure should avoid liability under both statutes.

Several other provisions of the Privacy Act exacerbate the problem created in subsection (b). Ordinarily, subsection (c) requires an

253. *See* notes 236-37 *supra* and accompanying text.
254. *See* notes 238-42 *supra* and accompanying text.
255. *See* note 257 *infra* and accompanying text.
256. *See* notes 226-35 *supra* and accompanying text.
257. *See* Comment, *supra* note 203, at 627-31.
258. *See* notes 147-56 *supra* and accompanying text.

agency to keep, and make available an accounting of the date, nature, purpose, and recipient of each disclosure of a personal record.[259] Subsection (c)(1) waives this obligation for disclosures required by the FOIA.[260] This provision is difficult to justify.[261] Its only benefit is to relieve agencies of the administrative task of recording what personal information is released and to whom. The damage to individual subjects far outweighs this trivial concern. The absence of an accounting assures that many individuals will never discover that agencies have wrongfully disclosed their records under the guise of the FOIA, and thereby erects still another barrier to effective enforcement of the Privacy Act. Moreover, waiving the accounting requirement prevents the subject from tracing and correcting unreliable information disclosed by federal agencies to private parties.

The inability to restrict the use of personal information subsequent to its disclosure pursuant to the FOIA would lead one to assume that federal agencies should at least be required to assure the quality of records so released. Congress recognized that because the restrictions in the Privacy Act apply only to federal agencies, disclosure to any party other than another federal agency threatens privacy more seriously than do interagency transfers.[262] Accordingly, subsection (e)(6) requires the custodial agency to check a record for accuracy, timeliness, completeness, and relevance before releasing it to parties outside the federal government.[263] The absence of an accounting requirement for FOIA disclosures rendered this subsection the individual's only protection against disclosure of unreliable data. Nevertheless, (e)(6) is inapplicable to disclosures required by the FOIA.[264] The sole rationale for this exemption is the need for speedy processing of FOIA re-

259. 5 U.S.C. § 552a(c) (Supp. V 1975). *See* note 85 *supra* and accompanying text.

260. 5 U.S.C. § 552a(c)(1) (Supp. V 1975).

261. The reason given for releasing agencies from the duty to keep an accounting is that it would be contrary to the spirit of the FOIA (*see* note 250 *supra*); this constitutes no justification at all. Since the public's right to know is the antithesis of the individual's right to privacy, attempts to protect one interest will frequently intrude on the other. The question then should not be "is this provision of the Privacy Act contrary to the FOIA?", but rather "how can we protect privacy without seriously impairing the public's right to know?" When the problem is addressed in this light, the congressional solution embodied in subsections (b)(2) and (c)(1) of the Privacy Act is clearly unsatisfactory.

262. *See* notes 133-35 *supra* and accompanying text.

263. 5 U.S.C. § 552a(e)(6) (Supp. V 1975).

264. *Id.*

quests;[265] acceptance thereof demonstrates a congressional preference for speed to privacy.

The Privacy Act's various exemptions for FOIA disclosures and the FOIA's inability to safeguard individual privacy require one of two conclusions: either Congress intentionally subordinated privacy interests to public information interests in *every* case of conflict, or Congress was wholly ignorant of the complex interaction between the two statutes. There are problems with each conclusion.

The first conclusion at least produces a simple rule for courts to follow when considering the conflict between individual privacy and the public's right to know. It is hard to believe, however, that Congress really intended to sacrifice privacy at every juncture. First, the unilateral sacrifice of privacy is unnecessary: requiring an accounting of FOIA disclosures, for example, would promote privacy interests without measurably impeding the operation of the FOIA. Secondly, this interpretation attributes to Congress the perverse desire to eliminate agency regulations precisely when they are most needed.[266] Given the strong congressional desire to enact privacy legislation, and the explicit recognition of the agencies as the foremost enemy of privacy, Congress surely could not have intended to leave the protection of privacy in the hands of the agencies. It makes little sense to assume that Congress intentionally subordinated the Privacy Act to the FOIA knowing the consequence to be the pointless destruction of significant aspects of the Privacy Act. It seems apparent, therefore, that Congress simply failed to realize that the FOIA could not adequately protect privacy and that subordinating the Privacy Act to the FOIA is tantamount to sacrificing privacy interests. This conclusion would suggest that courts should consider the principles underlying both the Privacy Act and the FOIA to attempt a reconciliation of their conflicting demands.

The underlying purpose of the Privacy Act is to protect informational privacy—to ensure that each individual has control over the information that directly affects his life.[267] The purpose of the FOIA is to develop an informed public able to make intelligent electoral choices and to ensure that government remains accountable to the people.[268] Focusing

265. *See* OMB Guidelines, *supra* note 69, at 60.

266. Most disclosures to which subsection (e)(6) applies, for example, will be required by the FOIA. Nevertheless, subsection (e)(6) is by its terms inapplicable in these instances.

267. *See* note 54 *supra* and accompanying text.

268. *See* note 196 *supra* and accompanying text.

on the underlying purposes would permit courts to give effect to both legislative intents. If disclosure would do little to promote government accountability, releasing the information would be inappropriate, especially if it would involve a serious invasion of individual privacy. Conversely, if release would significantly improve government accountability without seriously injuring privacy interests, disclosure would be appropriate. In any given case, the courts should balance the underlying interests served by each statute.

Fortunately, the sixth exemption to the FOIA would readily permit this type of interest balancing.[269] The Supreme Court's recent interpretation of this exemption in *Department of the Air Force v. Rose*[270] makes it clear that courts must balance "the individual's right to privacy against the preservation of the basic purpose of the Freedom of Information Act . . . ."[271] The Privacy Act dictates that any disclosure of personal information without consent always constitutes an invasion of privacy. Unless disclosure would substantially further the underlying goals of the FOIA, courts should liberally apply the exemption to refuse disclosure without the consent of the subject.

The problem with this approach is that it would require explicit judicial recognition of congressional ignorance. Given the explicit legislative history demonstrating congressional satisfaction with the FOIA,[272] courts are more likely to conclude that Congress intentionally, if unintelligently, chose to sacrifice privacy interests in favor of the public's right to know.

In this event, amendment of the FOIA would be the most sensible course to pursue. Specifically, agencies should be required to notify the subject of a record prior to disclosing information about him in identifiable form.[273] The agency should also supply the individual with a copy of the requested record and notice that failure to object within a specified time will constitute consent to disclosure. A less desirable amendment could require agencies to keep an accounting of disclosures and to assure the reliability of records disclosed under the FOIA.

269. 5 U.S.C. § 552(b)(6) (1970). *See* notes 205-12 *supra* and accompanying text.

270. 425 U.S. 352 (1976).

271. *Id.* at 372.

272. The legislative history states clearly that the Privacy Act was designed to "preserve the *status quo* as interpreted by the courts regarding the disclosure of personal information under [the FOIA]." 120 CONG. REC. S21,816 (daily ed. Dec. 17, 1974). *See* Project, *supra* note 12, at 1336-40.

273. *See* note 235 *supra.*

V. CONCLUSION

We live in a society in which personal information has assumed ever-increasing importance in fulfilling our most critical social responsibilities. The development of the computer and the increasing amount of personal information in governmental hands, however, poses substantial and growing dangers for the congeries of interests encompassed by the notion of privacy. The Privacy Act of 1974 attempts to resolve this dilemma, as the courts and the common law could not, by establishing substantive and procedural restrictions on the gathering and use of information about Americans by government agencies.

Although the Privacy Act is in many respects disappointing, it is nevertheless the most important piece of federal privacy legislation since the fourth amendment.[274] The Act exhibits an understanding of the serious problems posed by computers and is conceptually sound. At the very least, it constitutes an expression of congressional policy that will prompt federal agencies to exercise greater caution in handling personal information. Perhaps most important, the Privacy Act enables ambitious individuals to control the flow of information about them, to assure agency compliance with the Act, and to recover damages for serious invasions of privacy that were not actionable at common law.

The defects in the Privacy Act are structural. The failure to provide for an independent commission to aid in the enforcement of the Act was inexcusable. The Act places responsibility for assuring agency compliance almost exclusively upon the individual, but gives him neither the tools nor the incentive to do so. The absence of required notice to subjects of records, the inadequate regulations concerning existing files containing material in violation of the Privacy Act, and the unsatisfactory remedies under the Act render it an unenforceable statement of policy.

In the final analysis, however, the Privacy Act's most serious deficiency is the failure to make even a serious attempt to accommodate privacy with such crucial conflicting interests as effective law enforcement and the public's right to know. Indeed, whether by design or inadvertance, Congress adopted a scheme in both instances that systematically sacrifices the very interests the Privacy Act purports to protect. Nothing short of amendment will remedy these defects.

274. *See* 120 CONG. REC. H12,243 (daily ed. Dec. 18, 1974) (remarks of Rep. Moorehead) (discussing significance of Privacy Act).