

DOES THE PRIVACY ACT OF 1974 PROTECT YOUR RIGHT TO PRIVACY? AN EXAMINATION OF THE ROUTINE USE EXEMPTION

TODD ROBERT COLES

INTRODUCTION

Congressional, executive, and public support for privacy legislation coalesced in the Privacy Act of 1974.¹ Before passage of the Privacy Act, Congress struggled with many of the problems raised by increased government collection and use of personal information.² Congressional findings accompanying the Privacy Act reveal

1. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified at 5 U.S.C. § 552a (1988)); see Ehlke, *The Privacy Act After a Decade*, 18 J. MARSHALL L. REV. 829, 835-40 (1985) (examining amendments to Privacy Act).

2. See, e.g., *Privacy: The Collection, Use and Computerization of Personal Data: Joint Hearings Before the Subcomm. on Privacy and Information Systems of the Senate Comm. on Government Operations and the Subcomm. on Constitutional Rights of the Senate Comm. on the Judiciary*, 93d Cong., 2d Sess. (1974) (reporting hearings on threat to personal privacy posed by computerized informational systems maintained by federal government); *Right to Privacy of Federal Employees: Hearings Before the Subcomm. on Retirement and Employee Benefits of the House Comm. on Post Office and Civil Service*, 93d Cong., 2d Sess. (1974) (reporting hearings on federal agency actions affecting privacy of federal employees); *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. (1971) [hereinafter *Hearings on Federal Data Banks*] (reporting hearings on nature and scope of personal information held by federal agencies); see also Hanus & Relyea, *A Policy Assessment of the Privacy Act of 1974*, 25 AM. U.L. REV. 555, 565-69 (1976) (surveying congressional hearings on informational privacy issues as well as other congressional activity preceding passage of Privacy Act); STAFF OF SUBCOMM. ON CONSTITUTIONAL RIGHTS OF THE SENATE COMM. ON THE JUDICIARY, 93D CONG., 2D SESS., *FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS* iv-v (Comm. Print 1974) [hereinafter *FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS*] (reviewing comprehensive survey of enormous number of federal data banks, and recommending establishment of privacy safeguards, provision for notice and review to citizens in data bank, continued legislative oversight, and constraint on interagency transfers of personal information); *id.* at xv-xxxii (reviewing legislative privacy initiatives from 1965-1972).

The amount of personal information held by the federal government is staggering. See, e.g., *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) [hereinafter *Records Maintained by Government Agencies*] (statement of Rep. Edward Pattern) (noting average American is subject of estimated 10-20 files compiled by government on private organizations); STAFF OF SUBCOMM. ON ADMINISTRATION PRACTICE AND PROCEDURE OF THE SENATE COMM. ON THE JUDICIARY, 90TH CONG., 1ST SESS., *GOVERNMENT DOSSIER 1* (Comm. Print 1967) (examining 1966 survey on personal information held by government agencies and

Congress' recognition of the need to safeguard individual privacy in personal information.³ President Gerald Ford, a strong advocate of individual privacy, voiced executive branch support for the Privacy Act.⁴ Additional support was forthcoming from the public which, in the wake of technological advances, evinced increased apprehension over government invasion of individual privacy.⁵

finding more than 3 billion records on individuals, including 27.2 billion names, 2.3 billion addresses, 264 million criminal histories, 280 million mental health records, 916 million profiles on alcoholism and drug addiction, and 1.2 billion financial records); see also *The Computer and Invasion of Privacy: Hearings Before the Special Subcomm. on Invasion of Privacy of the House Comm. on Government Operations*, 89th Cong., 2d Sess. 12-13 (1966) (statement of Vance Packard) (describing dangers of proposed federal data bank center and expressing concern that use of information as form of control by government increases greatly as centralization of information grows).

3. Privacy Act of 1974, 5 U.S.C. § 552a (1988) (Congressional Findings and Statement of Purpose). Congress found that:

(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

Id.

4. See President's Remarks at Dedication of Stanford School of Law, 11 WEEKLY COMP. PRES. DOC. 1044, 1046 (Sept. 21, 1975) (discussing government invasion of personal privacy and need for Privacy Act). President Ford's commitment to the right to privacy stems, in part, from his participation in the Domestic Council Committee on the Right of Privacy (Privacy Committee) to which he was appointed chairman by President Richard Nixon. President's Address on Nationwide Radio on the American Right of Privacy, 10 WEEKLY COMP. PRES. DOC. 245, 246 (Feb. 23, 1974). President Nixon requested the Privacy Committee to examine the collection, maintenance, and use of personal information and safeguards of such information against improper disclosure. *Id.* at 246-47. Prophetically, President Nixon commented in his address that "[a]dvanced technology has created new opportunities for America as a Nation, but it has also created the possibility for new abuses of the individual." *Id.* A year later, President Ford noted that Congress had incorporated many of the Privacy Committee's recommendations. President's Remarks at Dedication of Stanford School of Law, 11 WEEKLY COMP. PRES. DOC. 1044, 1046 (Sept. 21, 1975).

5. See L. HARRIS, *THE ROAD AFTER 1984: A NATIONWIDE SURVEY OF THE PUBLIC AND ITS LEADERS ON THE NEW TECHNOLOGY AND ITS CONSEQUENCES FOR AMERICAN LIFE* (1983) (examining perceived effect of new technology on public). According to the 1983 survey, 48% of the public voiced strong concern about threats to personal privacy, a two-fold increase from 1978. *Id.* at 22. In addition, 60% of the public believed their personal privacy required limitations on the use of computers. *Id.* at 23. Finally, a majority of the public considered their personal privacy likely to be seriously invaded by the transfer of personal information among government agencies. *Id.* at 25; see also *FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS*, *supra* note 2, at ix-xiv (noting public reaction to invasion of personal privacy by technology). See generally L. HARRIS & A. WESTIN, *THE DIMENSIONS OF PRIVACY* (1981) (examining public concern over personal privacy).

President Ford acclaimed the Privacy Act as an important first step toward safeguarding individual privacy.⁶ Further, both Congress and the public voiced their support for the Privacy Act.⁷ The principal purpose of the Privacy Act, the protection of individual privacy, was praiseworthy. Whether the Privacy Act would actually achieve its goal, however, had yet to be determined.

The centerpiece of the Privacy Act, the prohibition on nonconsensual disclosure of personal information,⁸ is subject to numerous exemptions.⁹ One of these, the routine use exemption, permits nonconsensual disclosure of personal information where the purpose for collection is compatible with its use by the federal agency.¹⁰ The routine use exemption has threatened to emasculate the Privacy Act's protection of individual privacy.¹¹ Neither the federal agencies nor the Office of Management and Budget (OMB) has actively overseen the exemption's use.¹² Nor has Congress deterred continued abuse of the exemption.¹³ Finally, statutory and procedural barriers have prevented the courts from averting abuse of the exemption through judicial action.¹⁴

6. President's Statement Upon Signing the Bill (Privacy Act) Into Law, 11 WEEKLY COMP. PRES. DOC. 7, 7 (Jan. 1, 1975). The President recognized the Privacy Act as "an initial advance in protecting a right precious to every American—the right of individual privacy." *Id.* While approving of the Privacy Act as an important beginning, the President recognized that the Privacy Act did not "adequately protect the individual against unnecessary disclosures of personal information." *Id.* at 7-8.

7. See Berman & Goldman, *A Federal Right of Information Privacy: The Need for Reform*, 4 BENTON FOUNDATION PROJECT ON COMMUNICATIONS & INFORMATION POLICY OPTIONS 1-3 (1989) (noting strong congressional and public support for Privacy Act).

8. Privacy Act of 1974, 5 U.S.C. § 552a(b) (1988); see H.R. REP. NO. 1416, 93d Cong., 2d Sess. 12 (1974) [hereinafter H.R. REP. NO. 1416] (considering prohibition on non-consensual disclosure perhaps most important provision of bill), reprinted in STAFF OF SENATE COMM. ON GOVERNMENT OPERATIONS, 94TH CONG., 2D SESS., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY 305 (Joint Comm. Print 1976) [hereinafter SOURCE BOOK ON PRIVACY].

9. Privacy Act of 1974, 5 U.S.C. § 552a(b)(1)-(12) (1988); see *infra* notes 49-60 and accompanying text (providing statutory language of exemptions).

10. Privacy Act of 1974, 5 U.S.C. § 552a(b)(3) (1988); see *infra* note 61 (providing statutory language of routine use exemption); *infra* notes 134-35 and accompanying text (examining compatibility requirement of routine use exemption).

11. See, e.g., Comment, *The Privacy Act of 1974: An Overview*, 1976 DUKE L.J. 301, 314 [hereinafter *An Overview*] (noting potential for serious abuse of routine use exemption); Comment, *Narrowing the "Routine Use" Exemption to the Privacy Act of 1974*, 14 U. MICH. J.L. REF. 126, 132-33 (1980) [hereinafter *Narrowing the "Routine Use" Exemption*] (examining problems presented by routine use exemption); Note, *The Privacy Act of 1974: An Overview and Critique*, 1976 WASH. U.L.Q. 667, 684-85 [hereinafter *Overview and Critique*] (recognizing that exemptions, especially routine use exemption, destroy individual's control over personal information).

12. See *infra* notes 136-86 and accompanying text (discussing failure of OMB and federal agencies to oversee and to enforce Privacy Act).

13. See *infra* notes 187-215 and accompanying text (discussing limited success of Congress in preventing abuse of routine use exemption).

14. See *infra* notes 226-80 and accompanying text (discussing judicial efforts at combating abuse of routine use exemption).

This Comment evaluates the extent to which the Privacy Act has succeeded in safeguarding individual privacy through an examination of the application of the routine use exemption. Part I traces the origins of the constitutional right to privacy and examines its limited application to the collection and dissemination of personal information by the federal government. Part II surveys relevant portions of the Privacy Act, including provisions designed to protect individual privacy. Part III explores the disparate legislative history of the Privacy Act generally and the routine use exemption specifically. Part IV finds federal agency and OMB implementation and oversight of the Privacy Act wanting. Part V examines the marginal effect of congressional oversight. Part VI reviews judicial efforts to restrain abuse of the routine use exemption. This Comment concludes that although an important first step toward safeguarding individual privacy, the Privacy Act, left to the courts, is impotent without more effective oversight and enforcement by Congress and the federal agencies.

I. CONSTITUTIONAL RIGHT TO PRIVACY

Justice Brandeis defined the constitutional right to privacy as "the right to be let alone—the most comprehensive of rights and the right most valued by civilized men."¹⁵ Because the United States Constitution does not provide an explicit right to privacy,¹⁶ its development has been slow and irregular.¹⁷ The Supreme Court continues to grapple with the nature and scope of the constitutional

15. *Olmstead v. United States*, 277 U.S. 438, 478 (1928) (Brandeis, J., dissenting).

In 1890, Louis Brandeis and Samuel Warren first identified the right to privacy. Warren & Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 213 (1890). After exploring the nature and scope of the right to privacy, the authors concluded that "[i]t is the unwarranted invasion of individual privacy which is reprehended, and to be, so far as possible, prevented." *Id.* at 214-15. While commentators differ on the precise wording of the definition of privacy, most recognize the individual's right to determine what personal information is to be shared with others. See, e.g., A. BRECKENRIDGE, *THE RIGHT TO PRIVACY* 1 (1970) (defining privacy as "the rightful claim of the individual to determine the extent to which he wishes to share of himself . . . [and] the individual's right to control dissemination of information about himself"); A. WESTIN, *PRIVACY AND FREEDOM* 7 (1967) (defining privacy as "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others"); Project, *Government Information and the Rights of Citizens*, 73 MICH. L. REV. 971, 1225 (1975) (defining privacy as "the right to control the flow of information concerning the details of one's individuality"); Parker, *A Definition of Privacy*, 27 RUTGERS L. REV. 275, 281 (1974) (defining privacy as "control over when and by whom the various parts of us can be sensed by others").

16. See *Paul v. Davis*, 424 U.S. 693, 712 (1976) (noting right to privacy not found in any specific constitutional guarantee); *Roe v. Wade*, 410 U.S. 113, 152 (1973) (finding no explicit mention of right to privacy in Constitution).

17. See Seng, *The Constitution and Informational Privacy, or How So-Called Conservatives Countenance Governmental Intrusion into a Person's Private Affairs*, 18 J. MARSHALL L. REV. 871, 875 (1985) (concluding privacy decisions reflect Supreme Court's schizophrenia on right to privacy).

right to privacy.¹⁸

In 1977, the Supreme Court in *Whalen v. Roe*¹⁹ distinguished between the "interest in independence in making certain kinds of important decisions" and the "individual interest in avoiding disclosure of personal matters."²⁰ The former interest has been identified as "privacy of autonomy," while the latter has been termed "disclosural privacy."²¹ The Court has recognized a constitutional right to privacy of autonomy in decisions relating to marriage,²² procreation,²³ contraception,²⁴ family relationships,²⁵

18. See *Roe v. Wade*, 410 U.S. at 152 (finding only fundamental individual rights protected under right of personal privacy); *Griswold v. Connecticut*, 381 U.S. 479, 484 (1965) (recognizing zones of privacy).

In *Roe v. Wade*, the Supreme Court recognized the existence of "a right of personal privacy, or a guarantee of certain areas or zones of privacy." *Roe v. Wade*, 410 U.S. at 152. After surveying earlier cases basing the right to privacy on various constitutional provisions such as the first amendment, *Stanley v. Georgia*, 394 U.S. 557, 564 (1969); the fourth and fifth amendments, *Terry v. Ohio*, 392 U.S. 1, 8-9 (1968), *Katz v. United States*, 389 U.S. 347, 350 (1967); the penumbras of the Bill of Rights, *Griswold*, 381 U.S. at 484-85; the ninth amendment, *id.* at 486 (Goldberg, J., concurring); and the fourteenth amendment, *Meyer v. Nebraska*, 262 U.S. 390, 399 (1923), the Court concluded that only individual rights deemed " 'fundamental' or 'implicit in the concept of ordered liberty' " are found in the guarantee of personal privacy. *Roe v. Wade*, 410 U.S. at 152 (quoting *Palko v. Connecticut*, 302 U.S. 319, 325 (1937)).

In *Griswold*, the Supreme Court found that "[v]arious guarantees [in the Bill of Rights] create zones of privacy." *Griswold*, 381 U.S. at 484. Specifically, the Court recognized zones of privacy formed by the first amendment right of association, the third amendment prohibition against quartering of soldiers in homes during peace time without consent, the fourth amendment right of individuals to be secure from unreasonable search and seizure, and the fifth amendment protection against self-incrimination. *Id.*

19. 429 U.S. 589 (1977).

20. *Whalen v. Roe*, 429 U.S. 589, 599-600 (1977); see *infra* note 33 (discussing Supreme Court's failure in *Whalen* to find violation of constitutional right to privacy based on either interest).

21. See Project, *supra* note 15, at 1283 (exploring constitutional basis of disclosural privacy and privacy of autonomy). While never invoked by the Supreme Court, the disclosural/autonomy language provides a useful and insightful framework with which to distinguish the Court's privacy decisions.

22. See *Loving v. Virginia*, 388 U.S. 1, 12 (1967) (recognizing freedom of choice to marry protected by fourteenth amendment); *Griswold v. Connecticut*, 381 U.S. 479, 485-86 (1965) (recognizing right to privacy in marriage).

23. See *Skinner v. Oklahoma*, 316 U.S. 535, 541 (1942) (recognizing procreation and marriage as basic civil rights); *Roe v. Wade*, 410 U.S. 113, 153 (1973) (holding right to privacy protects woman's decision whether or not to terminate pregnancy). But see *Buck v. Bell*, 274 U.S. 200, 208 (1927) (upholding state law authorizing forced sterilization of insane and imbecile prison inmates).

24. See *Eisenstadt v. Baird*, 405 U.S. 438, 453-54 (1972) (recognizing right to privacy as freedom "from unwarranted governmental intrusion into matters so fundamentally affecting a person as the decision whether to bear or beget a child"); *Griswold*, 381 U.S. at 485 (invalidating state statute prohibiting use of contraceptives as impermissible invasion of right to privacy in marriage).

25. See *Prince v. Massachusetts*, 321 U.S. 158, 165-66 (1944) (recognizing parental authority over children and child-rearing as sacred, private interest).

obscene material in the home,²⁶ and child rearing and education.²⁷ Although the Court has continued to develop a right to privacy of autonomy, it seldom has advanced the right to disclosural privacy.²⁸

Usually associated with the first²⁹ and fourth amendments³⁰ to the United States Constitution, disclosural privacy concerns the right of an individual to control the flow of personal information.³¹ The Supreme Court rarely has recognized a constitutional right to disclosural privacy,³² and has yet to find the right violated.³³ Further,

26. See *Stanley v. Georgia*, 394 U.S. 557, 564-65 (1965) (recognizing right to privacy in what one reads at home).

27. See *Pierce v. Society of Sisters*, 268 U.S. 510, 534-35 (1925) (recognizing right of parents to direct upbringing and education of children).

28. Compare *Paul v. Davis*, 424 U.S. 693, 713 (1976) (failing to recognize constitutional right to privacy preventing public disclosure of personal arrest information) and *Seng*, *supra* note 17, at 874 (finding little judicial protection of right to disclosural privacy after *Paul*) with *Whalen v. Roe*, 429 U.S. 589, 609 (1977) (Stewart, J., concurring) (asserting no "general interest in freedom from disclosure of private information") and *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 455 n.18 (1977) (noting that in joining Court's opinion, Justice Stewart "adheres to his views on privacy as expressed in his concurring opinion in *Whalen*").

In *Paul*, the Court held that respondent's claim that the state could not publicly disclose an official arrest record was "far afield" of its earlier privacy decisions. *Paul*, 424 U.S. at 713. Distinguishing respondent's claim based on the right to disclosural privacy from its earlier decisions recognizing the right to privacy of autonomy, the Court declined to expand its earlier privacy decisions, none of which recognized respondent's claim to disclosural privacy. *Id.* In his dissent, Justice Brennan characterized the Court's opinion as an implicit repudiation of a substantial body of case law, resulting in the failure to recognize a constitutional privacy interest in reputation. *Id.* at 729 (Brennan, J., dissenting).

29. See *NAACP v. Alabama*, 357 U.S. 449, 460-63, 466 (1958) (invalidating state statute mandating that private association disclose member names as violative of due process clause of fourteenth amendment and its protection of right to privacy of association); see also Note, *The Interest in Limited Disclosure of Personal Information: A Constitutional Analysis*, 36 VAND. L. REV. 139, 151-53 (1983) [hereinafter *A Constitutional Analysis*] (examining first amendment origins of constitutional interest in limited disclosure).

30. See, e.g., *Katz v. United States*, 389 U.S. 347, 351-53 (1967) (holding evidence obtained from listening and recording device outside of phone booth, privacy of which defendant justifiably relied upon, violated fourth amendment); *Olmstead v. United States*, 277 U.S. 438, 478-79 (1928) (Brandeis, J., dissenting) (advocating broader interpretation of fourth amendment to prohibit home telephone wire tap and "every unjustifiable intrusion by the Government upon the privacy of the individual, whatever the means employed"); *Boyd v. United States*, 116 U.S. 616, 630 (1886) (invalidating statute authorizing court-ordered compulsory production of personal papers as unreasonable search and seizure under fourth amendment); see also *A Constitutional Analysis*, *supra* note 29, at 154-59 (examining fourth amendment origins of constitutional interest in limited disclosure); Note, *The Concept of Privacy and the Fourth Amendment*, 6 U. MICH. J.L. REF. 154, 189 (1972) (concluding that fourth amendment right to privacy cases reflect confusion and inconsistency).

31. See *A Constitutional Analysis*, *supra* note 29, at 177-82 (examining scope of disclosural privacy); Project, *supra* note 15, at 1283 (exploring right to disclosural privacy).

32. See *A Constitutional Analysis*, *supra* note 29, at 176-79 (finding basis for constitutional right to disclosural privacy only in *Whalen* and *Nixon*).

33. See *Whalen v. Roe*, 429 U.S. 589, 599 (1977) (failing to find constitutional right to disclosural privacy violated); *Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 457-59, 465 (1977) (finding no unconstitutional invasion of right to disclosural privacy).

In *Whalen*, the Court upheld a state statute requiring disclosure of private medical information to state authorities. *Whalen*, 429 U.S. at 603-04. The Court found it significant that limitations placed on the disclosure of medical information made public exposure unlikely. *Id.* at 600-02. Of importance was the Court's recognition of the threat to individual privacy posed

the Court has not detailed the requirements of a successful claim based on a constitutional right to disclosural privacy.³⁴ Because the Court has neither consistently recognized a constitutional right to,

by government collection of personal information. Justice Stevens, writing for the majority, stated:

We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. The collection of taxes, the distribution of welfare and social security benefits, the supervision of public health, the direction of our Armed Forces and the enforcement of the criminal laws, all require the orderly preservation of great quantities of information, much of which is personal in character and potentially embarrassing or harmful if disclosed.

Id. at 605. Having recognized the potential threat to individual privacy, the Court refused to decide the issue. *Id.* at 605-06.

In his concurring opinion, Justice Brennan examined the restrictions placed on dissemination of medical information by the New York statute under scrutiny and found sufficient safeguards against unwarranted disclosure. *Id.* at 606-07 (Brennan, J., concurring). Justice Brennan cautioned that a constitutionally protected privacy right would be implicated if the restrictions were not in place and the medical information was broadly disseminated by the state. *Id.* at 606 (Brennan, J., concurring). If a protected privacy interest was threatened, the state would be required to establish a compelling state interest to justify deprivation of the right to privacy. *Id.* at 607 (Brennan, J., concurring). In response to Justice Brennan's concurring opinion, Justice Stewart wrote a separate concurring opinion asserting that the Court had not recognized a "general interest in freedom from disclosure of private information." *Id.* at 609 (Stewart, J., concurring).

Writing for the majority in *Nixon*, Justice Brennan considered a disclosural privacy claim involving the Presidential Records and Materials Preservation Act (Preservation Act). Pub. L. No. 93-526, 88 Stat. 1695 (1974) (codified at 44 U.S.C. § 2107 (1988)). Under the Preservation Act, the Administrator of General Services was directed to take custody of Nixon's presidential papers and supervise their screening to determine which papers the government would maintain. *Nixon*, 433 U.S. at 429. Reviewing the Preservation Act's screening process, Justice Brennan stressed that the Preservation Act was drafted to minimize an invasion of privacy. *Id.* at 464. Justice Brennan concluded that no "less restrictive means" existed to accomplish the purpose of the Preservation Act, and Nixon's "legitimate expectation in privacy" had not been violated. *Id.* at 464-65.

Chief Justice Burger dissented, arguing that the Preservation Act should "be subjected to the most searching kind of judicial scrutiny," given its intrusion into highly personal communications. *Id.* at 526 (Burger, C.J., dissenting). Balancing the government's interest in disclosure against the individual's interest in privacy, the Chief Justice concluded that the individual's right to privacy must prevail against impermissible government intrusion. *Id.* at 534-36 (Burger, C.J., dissenting).

Although the Court failed in *Whalen* and *Nixon* to find that a constitutionally protected right to disclosural privacy had been violated, the Court has found that a similar statutorily protected privacy right was violated under the Freedom of Information Act. *See* Department of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989). In *Reporters Committee*, the Court recognized a privacy interest "in avoiding disclosure of personal matters" contained in an FBI criminal rap sheet. *Id.* Weighing the public interest in disclosure against the individual interest in privacy, the Court found the former at its nadir and the latter at its apex. *Id.* at 480. The Court concluded that disclosure of law-enforcement records was an unwarranted invasion of privacy. *Id.*

34. *See* Seng, *supra* note 17, at 879 (concluding that both *Whalen* and *Nixon* recognize right to freedom from unrestrained government disclosure of personal information, but finding no clear understanding of requirements for right to apply). Although the Supreme Court has not outlined the requirements for raising a constitutional right to disclosural privacy, the Court appears to have determined the appropriate judicial standard of review to be applied. *See A Constitutional Analysis*, *supra* note 29, at 192-93 (concluding Court applies heightened scrutiny analysis, balancing individual's interest in non-disclosure against government's interest in disclosure).

nor articulated a working definition of disclosural privacy, federal judicial protection has been marginal.³⁵

While the language of the United States Constitution has restrained judicial development of the right to privacy, state constitutions have explicitly recognized the right to privacy.³⁶ Although state recognition of the right to privacy has afforded individuals limited protection from state action, federal action has remained unaffected.³⁷ Absent an enforceable constitutional right to privacy in personal information held by the federal government, congressional legislation offered the only remaining safeguard. With the Privacy Act of 1974, Congress attempted to provide individuals needed protection against government invasion of privacy in personal information.³⁸

35. See *supra* note 33 (examining Supreme Court decisions where disclosural privacy claims failed); *A Constitutional Analysis*, *supra* note 29, at 172-74 (finding uncertainty in lower court decisions considering right to disclosural privacy); see also *J.P. v. DeSanti*, 653 F.2d 1080, 1089 (6th Cir. 1981) (declining to construe isolated statements in *Whalen* and *Nixon* beyond their context recognize general constitutional right to disclosural privacy where state statute provided for compilation and dissemination of juvenile social histories to state agencies and social and religious organizations, absent clear direction from Supreme Court); *Saint Michael's Convalescent Hosp. v. California*, 643 F.2d 1369, 1374-75 (9th Cir. 1981) (refusing to recognize violation of privacy interest in state statute requiring that health care providers publicly disclose cost information); *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 580 (3d Cir. 1980) (recognizing disclosural privacy interest in employee medical records, but holding that strong public interest in disclosure together with minimal intrusion on privacy was constitutionally acceptable).

36. See *Seng*, *supra* note 17, at 889-91 (reviewing state constitutions recognizing right to privacy); *Project*, *supra* note 15, at 1242-69 (examining state constitutional and statutory protection of privacy); see also G. Trubow, "The Development and Status of 'Information Privacy' Law and Policy in the United States," *Invited Papers on Privacy: Law, Ethics, and Technology*, *National Symposium on Personal Privacy and Information Technology*, 1981 ABA Sec. Indiv. Rights and Responsibilities, Committee on the Right to Privacy 6 (finding effectiveness of some 20 general state privacy laws "narrow and relatively insignificant"). See generally R. SMITH, *COMPILATION OF STATE & FEDERAL PRIVACY LAWS* (1988) (presenting comprehensive examination of state laws providing privacy protection).

37. The United States Constitution protects individuals against government but not private action; protection from private action is left to the states. *Katz v. United States*, 389 U.S. 347, 350-51 (1967). At the time of its adoption, the Privacy Act was considered a necessary complement to state and municipal laws protecting individual privacy. S. REP. NO. 1183, 93d Cong., 2d Sess. 17 (1974) [hereinafter S. REP. NO. 1183], *reprinted in SOURCE BOOK ON PRIVACY*, *supra* note 8, at 170. State efforts to guarantee and safeguard the right to privacy is rendered ineffective, however, once personal information becomes integrated into federal information systems. *Id.*

38. See Privacy Act of 1974, 5 U.S.C. § 552a (1988) (Congressional Findings and Statement of Purpose) (recognizing right to privacy as "a personal and fundamental right protected by the Constitution of the United States"). For a sampling of other congressional efforts to protect informational privacy see Cable Communications Policy Act of 1984, Pub. L. No. 98-549, 98 Stat. 2779 (codified as amended at 47 U.S.C. § 521 (1988)) (providing cable subscribers opportunity to limit disclosure and check accuracy of personal information); Right to Financial Privacy Act of 1978, Pub. L. No. 95-630, 92 Stat. 3641 (codified as amended at 12 U.S.C. § 3401 (1988)) (proscribing procedures for federal agencies seeking to gain access to private bank records); Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520 (codified as amended at 26 U.S.C. § 6103 (1988)) (making individual tax return information private, with limited exceptions); Family Education Rights and Privacy Act of 1974, Pub. L. No. 93-

II. THE PRIVACY ACT OF 1974

The Privacy Act of 1974 attempted to strike a delicate balance between the government's need to gather and to use personal information and the individual's competing need to maintain control over such personal information.³⁹ In furtherance of these competing goals, the Privacy Act requires every federal agency⁴⁰ maintaining a record⁴¹ on an individual⁴² within a system of records⁴³ to: (1) permit the individual to control the use and dissemination of information contained in the record;⁴⁴ (2) permit the individual to review, to correct, or to amend information contained in the record;⁴⁵ (3) regulate and restrict the collection, maintenance, use, and

380, 88 Stat. 484 (codified as amended at 20 U.S.C. § 1232 (1988)) (requiring schools and colleges to grant students and parents access to student records and prescribing procedures for verification and correction of information); Crime Control Act of 1973, Pub. L. No. 93-83, 87 Stat. 97 (codified as amended at 42 U.S.C. § 3701 (1988)) (requiring state criminal justice information systems to ensure privacy and security of personal information); Fair Credit Reporting Act of 1970, Pub. L. No. 91-508, 84 Stat. 1114 (codified as amended at 15 U.S.C. § 1681 (1988)) (proscribing access, verification, correction, and disclosure guidelines pertaining to personal credit information maintained by federal agencies).

39. See H.R. REP. NO. 1416, *supra* note 8, at 4 (recognizing attempted delicate balance between need of individual to protect personal information furnished to government and need of government to access personal information required to function properly), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 297; *Analysis of House and Senate Compromise Amendments to the Federal Privacy Act*, 120 CONG. REC. 40,405, 40,881 (1974) [hereinafter *Analysis of Compromise Amendments*] (noting difficulty of balancing "public's right to know about the conduct of their government and their equally important right to have information which is personal to them maintained with the greatest degree of confidence by Federal agencies"), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 858, 989. The *Analysis of Compromise Amendments* was ordered printed in the *Congressional Record* by both the Senate, 120 CONG. REC. 40,405-09 (1974), and the House, 120 CONG. REC. 40,881-83 (1974). Both printings appear in SOURCE BOOK ON PRIVACY, *supra* note 8, at 858-66, 987-94. All cites to *Analysis of Compromise Amendments* are to the House printing in the *Congressional Record* and its reprinting in SOURCE BOOK ON PRIVACY.

40. Privacy Act of 1974, 5 U.S.C. § 552a(a)(1) (1988). The Privacy Act adopts the definition provided in FOIA that defines "agency" as including "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." *Id.* § 552a(f).

41. *Id.* § 552a(a)(4). "Record" is defined 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 the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph.

Id.

42. *Id.* § 552a(a)(2). "Individual" is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence." *Id.*

43. *Id.* § 552a(a)(5). "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." *Id.*

44. *Id.* § 552a (Congressional Findings and Statement of Purpose); see *infra* notes 48-61 and accompanying text (discussing exemptions to disclosure prohibition).

45. Privacy Act of 1974, 5 U.S.C. § 552a (1988) (Congressional Findings and Statement

dissemination of information in the record;⁴⁶ and (4) be subject to civil suit for specified violations of the Privacy Act.⁴⁷ Collectively, these safeguards are designed to protect individual privacy, while preserving the government's ability to gather and to use personal information.

The first safeguard prohibits any federal agency from disclosing any record contained in a system of records, without written consent of the individual to whom the record pertains.⁴⁸ The expansive scope of this prohibition on nonconsensual disclosure, however, is subject to numerous exemptions.⁴⁹ Specific exemptions exist for disclosure to agency employees,⁵⁰ the Bureau of the Census,⁵¹ the National Archives and Records Administration,⁵² Congress or its committees,⁵³ the Comptroller General,⁵⁴ and the consumer protection agencies.⁵⁵ Also exempted is disclosure required under the Freedom of Information Act,⁵⁶ for statistical research⁵⁷ or law enforcement purposes,⁵⁸ in response to emergency circumstances,⁵⁹

of Purpose); see *infra* notes 62-66 and accompanying text (discussing guidelines allowing individual access to personal records).

46. Privacy Act of 1974, 5 U.S.C. § 552a (1988) (Congressional Findings and Statement of Purpose); see *infra* notes 67-74 and accompanying text (discussing restrictions on federal agency collection and use of personal information).

47. Privacy Act of 1974, 5 U.S.C. § 552a (1988) (Congressional Findings and Statement of Purpose); see *infra* notes 79-83 and accompanying text (discussing available civil and criminal remedies).

48. Privacy Act of 1974, 5 U.S.C. § 552a(b) (1988).

49. *Id.* § 552a(b)(1)-(12).

50. *Id.* § 552a(b)(1). Section 552a(b)(1) provides that information may be disclosed "to those officers and employees of the agency which maintain the record who have a need for the record in the performance of their duties." *Id.*

51. *Id.* § 552a(b)(4). Section 552a(b)(4) provides in pertinent part that information may be disclosed "to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity . . ." *Id.*

52. *Id.* § 552a(b)(6). Section 552a(b)(6) provides that information may be disclosed "to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value." *Id.*

53. *Id.* § 552a(b)(9). Section 552a(b)(9) provides that information may be disclosed "to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee." *Id.*

54. *Id.* § 552a(b)(10). Section 552a(b)(10) provides that information may be disclosed "to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the General Accounting Office." *Id.*

55. *Id.* § 552a(b)(12).

56. *Id.* § 552a(b)(2).

57. *Id.* § 552a(b)(5). Section 552a(b)(5) provides that information may be disclosed "to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable." *Id.*

58. *Id.* § 552a(b)(7). Section 552a(b)(7) provides that information may be disclosed to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity

or pursuant to court order.⁶⁰ Finally, the broadest exemption is for disclosure pursuant to a "routine use."⁶¹

The second safeguard provides that every federal agency must grant the individual access to pertinent records upon request.⁶² Specifically, the federal agency must permit the individual to review⁶³ or to request amendment⁶⁴ of any record pertaining to the individual. Should the federal agency fail to amend the record, the individual may request the federal agency to review its decision.⁶⁵ If after review the federal agency refuses to amend the record, the individual may seek judicial review of the decision.⁶⁶

The third safeguard regulates and limits the collection, maintenance, use, and dissemination of personal information by federal agencies.⁶⁷ Federal agencies may gather only that information required to accomplish the purpose for its collection.⁶⁸ Information must be collected directly from the individual whenever practicable⁶⁹ and, in any event, must be maintained accurately and completely.⁷⁰ Every federal agency must publish a notice in the *Federal Register* describing each system of records it maintains and each routine use it employs.⁷¹ Federal agencies also must keep an accurate

if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought.

Id.

59. *Id.* § 552a(b)(8). Section 552a(b)(8) provides that information may be disclosed "to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such an individual." *Id.*

60. *Id.* § 552a(b)(11).

61. *Id.* § 552a(b)(3). "Routine use" is defined, "with respect to the disclosure of a record, [as] the use of such record for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7). Individuals providing information to a federal agency must be informed of the routine uses for which the information may be used. *Id.* § 552a(e)(3)(C). Additionally, such routine uses must appear annually in the *Federal Register*. *Id.* § 552a(e)(4)(D).

62. *Id.* § 552a(d).

63. *Id.* § 552a(d)(1).

64. *Id.* § 552a(d)(2).

65. *Id.* § 552a(d)(3).

66. *Id.* § 552a(g)(1)(A).

67. *Id.* § 552a(c), (e), (f).

68. *Id.* § 552a(e)(1). Specifically, the purpose must be one required by statute or executive order. *Id.* Unless exclusively authorized by statute or by the individual, no record may be maintained which describes the individual's exercise of first amendment rights. *Id.* § 552a(e)(7).

69. *Id.* § 552a(e)(2).

70. *Id.* § 552a(e)(5). Prior to dissemination of any record, the federal agency must make reasonable efforts to assure the accuracy and completeness of the record. *Id.* § 552a(e)(6).

71. *Id.* § 552a(e)(4). Notice must be given in the *Federal Register* of "each routine use of the records contained in the system [of records], including the categories of users and the purpose of such use." *Id.* § 552a(e)(4)(D). In addition, any federal agency that proposes to

accounting of all records disclosed and the purpose and nature of such disclosures.⁷² In addition, federal agencies must promulgate rules of conduct for their employees charged with the maintenance of any record or system of records⁷³ and must establish procedures to review the requests of individuals to amend their records.⁷⁴

Although the third safeguard restricts the collection and use of personal information by federal agencies, general and specific exemptions allow the heads of federal agencies to promulgate rules that exempt their federal agency's systems of records from provisions of the Privacy Act.⁷⁵ The general exemptions provide that systems of records maintained by the Central Intelligence Agency or criminal law enforcement agencies may be excused from compliance with the access, collection, and use provisions of the Privacy Act.⁷⁶ In addition, there are seven specific exemptions that excuse systems of records from compliance with these provisions of the Privacy Act.⁷⁷ Neither the general nor the specific exemptions excuse observance of the nondisclosure and remedial provisions.⁷⁸

The final safeguard makes civil remedies available to any individual bringing suit against a federal agency for specified violations of the Privacy Act.⁷⁹ The Privacy Act recognizes four violations. The first is for a federal agency's failure to amend the individual's record as requested, or to review the individual's request.⁸⁰ The second arises from a federal agency's refusal to permit review of the individual's records.⁸¹ The third is for a federal agency's failure to maintain the individual's records properly, resulting in an adverse

establish or to amend a system of records is required to provide advance notice to the House Committee on Government Operations, the Senate Committee on Governmental Affairs, and OMB for evaluation. *Id.* § 552a(r).

72. *Id.* § 552a(c). Accountings are made available upon request to any individual named in the record. *Id.* § 552a(c)(3).

73. *Id.* § 552a(e)(9).

74. *Id.* § 552a(f).

75. *Id.* § 552a(j), (k).

76. *Id.* § 552a(j).

77. *Id.* § 552a(k)(1)-(7). The specific exemptions apply to record systems containing: classified material, investigatory materials for law enforcement agencies, information used to protect the President, statistical records, investigatory materials for civil employment, military service or government contracts, employment testing materials, and armed service evaluative materials for promotion. *Id.*

78. *Id.* § 552a(j), (k); see *Tijerina v. Walters*, 821 F.2d 789, 795-97 (D.C. Cir. 1987) (holding that general exemption does not exclude compliance with civil remedies provisions).

79. Privacy Act of 1974, 5 U.S.C. § 552a(g) (1988).

80. *Id.* § 552a(g)(1)(A). The court shall review the matter *de novo* and may order the federal agency to amend the individual's record. *Id.* § 552a(g)(2)(A).

81. *Id.* § 552a(g)(1)(B). The court may enjoin the federal agency from withholding the record and order the federal agency to produce it, or the court may examine the contents of the record to determine whether the record is exempt from disclosure. *Id.* § 552a(g)(3)(A). The court shall review the matter *de novo* and the burden is on the federal agency to sustain its action. *Id.*

determination against the individual.⁸² The last violation for which civil remedies are provided is worded broadly to encompass a federal agency's failure to adhere to any provision of the Privacy Act that causes the individual to suffer an adverse effect.⁸³

III. LEGISLATIVE HISTORY

Although Congress addressed distinct informational privacy concerns in earlier legislation,⁸⁴ the Privacy Act of 1974 was Congress' first attempt at a comprehensive plan for safeguarding individual privacy in personal information.⁸⁵ The Privacy Act was preceded by exhaustive congressional hearings on individual privacy,⁸⁶ and the consideration of over 100 alternative privacy bills.⁸⁷ Of still greater importance was a 1973 Department of Health, Education, and Welfare report proposing a Code of Fair Information Practices (Code).⁸⁸ The Code figured prominently in the legislative drafting process of the Privacy Act.⁸⁹

82. *Id.* § 552a(g)(1)(C). Court costs, attorney fees, and actual damages sustained by the individual are available for section 552a(g)(1)(C) and 552a(g)(1)(D) violations where the court determines that the federal agency's actions were intentional or willful. *Id.* § 552a(g)(4).

83. *Id.* § 552a(g)(1)(D).

In addition to civil remedies, the court may impose criminal penalties upon any federal agency employee or person violating the Privacy Act. *Id.* § 552a(i). Any federal agency employee who knowingly and willfully discloses personal records, or who willfully maintains a system of records without complying with the notice requirements, is subject to criminal penalties. *Id.* § 552a(i)(1), (2). Any person who knowingly and willfully requests or obtains personal records under false pretenses is also subject to criminal penalties. *Id.* § 552a(i)(3). Persons subject to criminal penalties may be guilty of a misdemeanor and subject to a maximum fine of \$5,000. *Id.* § 552a(i)(1)-(3).

84. See Project, *supra* note 15, at 1297-303 (reviewing earlier congressional initiatives protecting privacy in personal information); Hanus & Relyea, *supra* note 2, at 567-69 (discussing prior congressional measures aimed at guarding privacy); see also *supra* note 2 (examining earlier congressional privacy hearings and legislation).

85. 120 CONG. REC. 40,880 (1974) (statement of Rep. Moorhead), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 986.

86. See *supra* note 2 (surveying congressional hearings on personal privacy). Senator Sam Ervin, Chairman of the Subcommittee on Constitutional Rights and chief sponsor of the Privacy Act, held hearings on personal privacy for several years before the Privacy Act was adopted by Congress. See FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS, *supra* note 2, at iii-v (reviewing efforts of Senator Ervin to advance privacy legislation).

87. Comment, *Privacy and the Freedom of Information Act*, 27 ADMIN. L. REV. 275, 275 (1975).

88. U.S. DEPARTMENT OF HEALTH, EDUCATION, AND WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS: REPORT OF THE SECRETARY'S ADVISORY COMM. ON AUTOMATED PERSONAL DATA SYS. xxiii-xxvi (1973) [hereinafter HEW REPORT]. A product of the Secretary's Advisory Committee on Automated Personal Data Systems, the Code addressed significant problems arising from the application of computer technology to the collection, maintenance, use, and dissemination of personal information. See *id.* at x-xi (describing principles upon which Code rests).

89. See 2 J. O'REILLY, FEDERAL INFORMATION DISCLOSURE, ch. 20.02, at 20-7 to -8 (1989) (noting deference shown Code in drafting process); S. REP. NO. 1183, *supra* note 37 (citing favorably to Code throughout report), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8; H.R. REP. NO. 1416, *supra* note 8, at 7 (stating House bill embodies major principles of Code), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 300. A comparison of the Code to the

A. House and Senate Compromise

The final version of the Privacy Act was the result of a last minute compromise between competing Senate and House bills.⁹⁰ Commentators critical of congressional haste claim that the compromise produced an act that lacks internal consistency and clear legislative intent.⁹¹ Moreover, the compromise diluted the protection afforded

Privacy Act reveals the influence of the former over the latter. Indeed, the Privacy Act embodies all five principles upon which the Code was based: (1) there must be no secret personal data systems; (2) an individual must be able to determine whether personal information is held in personal data systems and how it is used; (3) an individual must be able to exercise control over the use of personal information held in personal data systems; (4) an individual must be able to correct errors in information held in personal data systems; and (5) any agency with control over personal information must be able to guarantee its reliability and protect it from misuse. HEW REPORT, *supra* note 88, at xx-xxi.

90. Compare S. 3418, 93d Cong., 2d Sess., 120 CONG. REC. 36,917-21 (1974) [hereinafter S. 3418], *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 334-74 with H.R. 16,373, 93d Cong., 2d Sess., 120 CONG. REC. 36,652-54 (1974) [hereinafter H.R. 16,373], *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 258-93.

The Senate passed S. 3418 on November 21, 1974 by a vote of 74 to 9, with 17 senators not voting. 120 CONG. REC. 36,917 (1974), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 838. On the same day, the House passed H.R. 16,373 by a vote of 353 to 1, with 80 representatives not voting. *Id.* at 36,976-77, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 981. The House took up S. 3418, but retained only the enacting clause. *Id.* at 39,204, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 984. After substituting the House language, the House passed S. 3418 on December 11, 1974. *Id.*

Because insufficient time remained in the session to submit the competing versions to a conference committee, an informal process was adopted to reconcile the bills. Hanus & Relyea, *supra* note 2, at 572. Staff members from the Senate and House committees and the principal sponsors engaged in a series of informal meetings to reach a compromise. *Id.* House sponsor Representative Moorhead explained the informal procedure by which differences in the two bills were reconciled:

Because of the lateness in the session and the pressures on Members of both bodies due to other pressing legislative business, we determined that it would not be possible to resolve the complex differences between the two bills in a conference committee. Yet the sponsors and floor managers of the legislation on both sides firmly agreed that it was imperative that final action be taken on privacy legislation before the end of Congress.

* * *

... [Compromise] amendments were informally negotiated by the staffs of the House and Senate committees and are based on agreements between the principal sponsors of the privacy bills in the two bodies.

120 CONG. REC. 40,880 (1974) (statement of Rep. Moorhead), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 985-86; *see id.* at 40,400 (statement of Sen. Ervin) (reporting reconciliation process), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 845-46. As amended, the Senate passed S. 3418 on December 17, 1974 by a vote of 77 to 8, with 15 senators not voting. *Id.* at 40,413, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 877. The next day the House passed the amended S. 3418. *Id.* at 40,886, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 1001. In lieu of a conference report, the *Analysis of Compromise Amendments* was introduced into the *Congressional Record*. *Analysis of Compromise Amendments*, *supra* note 39, at 40,881-83, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 987-94. President Ford signed the amended bill on December 31, 1974. *See supra* note 6 (reviewing President's remarks upon signing Privacy Act).

91. See 2 J. O'REILLY, *supra* note 89, ch. 20.03, at 20-9 (noting flaws in Privacy Act as compromise legislation and questioning existence of congressional intent); *Oversight of the Privacy Act of 1974: Hearings Before a Subcomm. of the House Comm. on Government Operations*, 98th Cong., 1st Sess. 231 (1983) [hereinafter *Hearings on Oversight of Privacy Act*] (statement of Ronald Plessler) (stating Privacy Act is "its own worst enemy"). As one commentator remarked:

to individual privacy in personal information.⁹²

The House bill embodied a conservative approach to safeguarding individual privacy in personal information.⁹³ The bill's restraint is attributable to House efforts to accommodate and to involve the executive branch in the drafting process.⁹⁴ In order to facilitate the orderly conduct of government, the House bill proposed a "routine use" exemption to the nondisclosure provision.⁹⁵ The exemption was adopted to quell fears that the nondisclosure provision would prohibit "routine" transfers of information by federal agencies.⁹⁶ In addition, the exemption precluded the need for Congress to detail every appropriate use of information.⁹⁷

Notice provisions in the House bill required federal agencies to

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 Consequently, courts are likely to have great difficulty interpreting the Act and vigorous enforcement may be impossible.

R. BOUCHARD & J. FRANKLIN, GUIDEBOOK TO THE FREEDOM OF INFORMATION AND PRIVACY ACT 45 (1980).

92. See Project, *supra* note 15, at 1305-40 (examining deficiencies and interpretative difficulties in Privacy Act including federal agency evasion of disclosure requirements, severe limitations on access to civil remedies, and failure to draft narrow exemptions); Ehlik, *supra* note 1, at 829 (finding Privacy Act ambitious in theory, but ineffective in practice).

93. See 2 J. O'REILLY, *supra* note 89, ch. 20.03, at 20-11 (stating that House bill was more conservative than Senate bill).

94. *Id.* at 20-11 to -12 (noting involvement of OMB and Privacy Committee during drafting process and high degree of cooperation); Hanus & Relyea, *supra* note 2, at 571 (finding that House subcommittee staff was sensitive to Privacy Act's impact on information-handling procedures of federal agencies and, thus, was inclined to defer to executive branch expertise); H.R. REP. NO. 1416, *supra* note 8, at 11 (explaining technical details of House bill were worked out through informal meetings with OMB staff and Privacy Committee), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 304; 120 CONG. REC. 36,966-97 (1974) (statement of Rep. Moorhead) (conveying President Ford's support for House bill), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 956-57. Unlike the House, the Senate involved the executive branch only marginally in the drafting process. See 2 J. O'REILLY, *supra* note 89, ch. 20.03, at 20-12 (recognizing that Senate involvement in Watergate proceedings may explain lack of interaction with executive branch); Hanus & Relyea, *supra* note 2, at 570-71 (hypothesizing that executive branch cooperation in Senate bill was limited because of Senate involvement in Watergate investigation).

95. H.R. 16, 373, *supra* note 90, § 552a(b)(2), 120 CONG. REC. 36,653, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 279; see H.R. REP. NO. 1416, *supra* note 8, at 12 (explaining routine use will prevent impeding orderly government or delaying services), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 305; see *Records Maintained by Government Agencies*, *supra* note 2, at 131 (statement of H. Peterson, Assistant Attorney General, Criminal Division, Department of Justice) (observing House bill "could materially interfere with the agency's performance of its mission in ways other than increased administrative work").

96. H.R. REP. NO. 1416, *supra* note 8, at 12, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 305. Federal agencies complained that because they could not obtain consent from every individual whose information was subject to routine transfer, they would be prevented from making useful and efficient exchanges of information. *Id.*; see *infra* notes 123-24, 130-35 and accompanying text (discussing legislative origins and scope of routine use exemption).

97. See 120 CONG. REC. 36,967 (1974) (statement of Rep. Moorhead) (noting routine use exemption would preclude "impossible legislative task" of attempting "to set forth all of the appropriate uses"), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 957.

inform individuals of the nature and scope of personal information maintained by the government and the purposes of its collection and use.⁹⁸ The House bill also professed to guarantee relief to injured individuals⁹⁹ and advocated private enforcement as an effective check against federal agency abuses.¹⁰⁰ The restrictive language of the House bill's remedial provisions, however, prevented aggressive private enforcement and limited the relief available to injured individuals.¹⁰¹

In contrast to the House bill, the Senate bill was more aggressive and its scope was more expansive.¹⁰² By holding federal agencies strictly liable for violations, the Senate bill favored the individual and allowed greater access to civil remedies.¹⁰³ The Senate bill also encouraged private enforcement by providing injunctive relief and punitive damages where appropriate.¹⁰⁴ In addition, the Senate bill

98. H.R. 16,373, *supra* note 90, § 552a(e), 120 CONG. REC. 36,653, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 283-85; *see* H.R. REP. NO. 1416, *supra* note 8, at 15-16 (discussing notice provisions), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 308-09.

99. H.R. REP. NO. 1416, *supra* note 8, at 17, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 310.

100. *See id.* at 15 (relying on "constant vigilance" of individuals supported by "legal redress" to combat abuse by federal agencies), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 308.

101. H.R. 16,373, *supra* note 90, § 552a(g), 120 CONG. REC. 36,654, *reprinted in* SOURCE BOOK ON PRIVACY *supra* note 8, at 287-89; *see* H.R. REP. NO. 1416, *supra* note 8, at 17-18 (requiring individual to establish adverse effect, causally related to willful, arbitrary, or capricious federal agency action), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 310-11. If successful, relief was limited to actual damages, court costs, and attorney fees. H.R. 16,373, *supra* note 90, § 552a(g)(3), 120 CONG. REC. 36,654 *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 288. Several members of the House Foreign Operations and Government Information Subcommittee wrote separately, arguing that effective private deterrence required the restoration of punitive and liquidated damages. H.R. REP. NO. 1416, *supra* note 8, at 38, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 330.

102. *See* S. 3418, *supra* note 90, §§ 202(a), (b), 301(2)-(5), 120 CONG. REC. 36,920-21 (providing expansive coverage of nondisclosure provision and recognizing few exemptions), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 359-60, 367. Most importantly, the Senate bill made no exemption for routine use disclosures. *Id.* § 202(b), 120 CONG. REC. 36,920, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 359-60; *see* S. REP. NO. 1183, *supra* note 37, at 20 (stating exemptions are to be kept to absolute minimum), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 173. In addition, the Senate bill was not restricted to information systems held by the federal government, but extended to state, local, and private information systems. *Id.* at 17-18, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 170-71.

103. S. 3418, *supra* note 90, § 303(c), 120 CONG. REC. 36,921, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 371; *see* S. REP. NO. 1183, *supra* note 37, at 82-83 (noting need for "widest possible citizen enforcement" because of lack of independent enforcement body), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 235-36. *Compare* H.R. 16,373, *supra* note 90, § 552a(g), 120 CONG. REC. 36,654 (requiring that injured party establish actual personal damages causally related to willful federal agency action), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 287-89 with S. 3418, *supra* note 90, § 303, 120 CONG. REC. 36,921 (holding federal agencies strictly liable for actions), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 370-72.

104. S. 3418, *supra* note 90, § 303(a)-(c), 120 CONG. REC. 36,921, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 370-71; *see* S. REP. NO. 1183, *supra* note 37, at 16 (recognizing need for and encouraging private enforcement), *reprinted in* SOURCE BOOK ON PRIVACY, *supra*

authorized the Attorney General to seek an injunction against existing or threatened violations affecting the public at large.¹⁰⁵ Comprehensive notice requirements assisted individuals when exercising their rights under the Senate bill.¹⁰⁶ Finally, the Senate bill proposed the establishment of a Privacy Protection Commission (Privacy Commission) with broad investigatory and enforcement powers.¹⁰⁷

The Senate's greatest concession in the compromise reached between the House and Senate bills was its abandonment of the Privacy Commission.¹⁰⁸ Unable to overcome House and executive branch opposition, proponents of the Privacy Commission agreed to a compromise.¹⁰⁹ In place of the Privacy Commission, the Privacy Act authorized the establishment of a Privacy Protection Study Commission (Study Commission).¹¹⁰ Unlike its predecessor, the Study Commission, stripped of investigatory and enforcement pow-

note 8, at 169; *id.* at 83 (noting broad availability of damages and injunctive relief), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 236.

105. S. 3418, *supra* note 90, § 303(b), 120 CONG. REC. 36,921, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 371; *see* S. REP. NO. 1183, *supra* note 37, at 83 (providing enforcement by Attorney General where individual lacks standing or incentive to bring suit), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 236.

106. S. 3418, *supra* note 90, § 201, 120 CONG. REC. 36,918-19, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 348-59; *see* S. REP. NO. 1183, *supra* note 37, at 48, 58-59 (recognizing notice requirements as protection against arbitrary information gathering by government), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 201, 211-12.

107. S. 3418, *supra* note 90, §§ 101-107, 120 CONG. REC. 36,917-18, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 334-47. The Privacy Commission was authorized to conduct inspections, hold hearings, take testimony, issue subpoenas, receive complaints, and take action as needed. *Id.* § 105(a), 120 CONG. REC. 36,918, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 342-43. In addition, the Privacy Commission was required to study government data banks and their effect on personal privacy and periodically report its findings to Congress and the President. *Id.* §§ 106-107, 120 CONG. REC. 36,918, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 344-47; *see* S. REP. NO. 1183, *supra* note 37, at 24-26 (recommending Privacy Commission aid Congress when enacting future privacy legislation and assume needed oversight role Congress was unable to fulfill), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 177-79; *see also id.* at 25 (noting rejection of original Senate bill proposal for establishment of Federal Privacy Board with broad regulatory powers), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 178.

108. Hanus & Relyea, *supra* note 2, at 572.

109. *See id.* (noting strong opposition of OMB to Privacy Commission); 2 J. O'REILLY, *supra* note 89, ch. 20.03, at 20-12, 20-14 n.29 (recognizing executive branch and House objection to establishment of another independent agency); 120 CONG. REC. 36,967 (1974) (statement of President Ford) (disfavoring any separate bureaucratic privacy agency), *reprinted in* SOURCE BOOK ON PRIVACY *supra* note 8, at 956-57.

Several members of the House Foreign Operations and Government Information Subcommittee broke ranks and supported the Senate proposal to establish an administrative oversight body with enforcement powers. H.R. REP. NO. 1416, *supra* note 8, at 38-39, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 330-31. The members expressed their concern that Congress not "repeat the experience of the Freedom of Information Act in holding out rights to individuals but providing them only with the costly and cumbersome mechanism of a judicial remedy." *Id.* at 38, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 330.

110. Privacy Act of 1974, Pub. L. No. 93-579, § 5, 88 Stat. 1986, 1905-09, *amended by*, Pub. L. No. 95-38, § 5(g), 91 Stat. 179 (1977).

ers, was directed to study and to report on federal agency protection of personal information.¹¹¹ Although the Privacy Commission's enforcement provisions were abandoned, the oversight provisions were retained and assigned to OMB with instructions to promulgate guidelines for and to assist in the implementation of the Privacy Act.¹¹²

The adoption of a compromise standard of proof for civil remedies restricted recovery of actual damages to instances of "willful or intentional" federal agency action.¹¹³ The compromise eliminated punitive damages, limited injunctive relief, and restricted recovery of reasonable costs and attorney fees.¹¹⁴ The notice requirements from the House and Senate bills were incorporated into the Privacy Act largely unchanged.¹¹⁵ Finally, the House "routine use" language was adopted as an exemption to the nondisclosure provision.¹¹⁶

111. *Id.* Compare *supra* note 107 (examining expansive powers and responsibilities of Privacy Commission) with *Analysis of Compromise Amendments*, *supra* note 39, at 40,881 (explaining restricted role of Study Commission), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 987. The Study Commission was restricted to a non-renewable two year term as a "study commission." *Id.* An effort to grant the Study Commission permanent status failed on the House floor. 120 CONG. REC. 36,962-65 (1974), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 945-52. In addition to preparing an annual report to Congress and the President, the Study Commission was directed to submit a final report at the conclusion of its term. *Analysis of Compromise Amendments*, *supra* note 39, at 40,881, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 987. In 1977, the Study Commission issued its final report, complete with an assessment of the Privacy Act and recommendations for its improvement. PRIVACY PROTECTION STUDY COMMISSION, PERSONAL PRIVACY IN AN INFORMATION SOCIETY (1977) [hereinafter PRIVACY PROTECTION STUDY COMMISSION].

112. Privacy Act of 1974, 5 U.S.C. § 552a(v) (1988). Section 552a(v) directs the Director of OMB to:

(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and

(2) provide continuing assistance to and oversight of the implementation of this section by agencies.

Id.

113. *Analysis of Compromise Amendments*, *supra* note 39, at 40,882, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 989-90. The compromise standard of proof was explained as reflecting the

belief that a finding of willful, arbitrary, or capricious action is too harsh a standard of proof for an individual to exercise the rights granted by this legislation. Thus the standard for recovery of damages was reduced to 'willful or intentional' action by an agency. On a continuum between negligence [(Senate version)] and the very high standard of willful, arbitrary, or capricious conduct [(House version)], this standard is viewed as only somewhat greater than gross negligence.

Id.

114. *Id.*

115. Privacy Act of 1974, 5 U.S.C. § 552a(e)(3)(C), (4) (1988); see *supra* note 71 and accompanying text (providing statutory language of notice requirements).

116. *Analysis of Compromise Amendments*, *supra* note 39, at 40,881, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 987.

The compromise clearly favored the House bill¹¹⁷ and revealed a preference for the government's right to gather and to use personal information over the individual's right to privacy. By adopting a higher standard of proof for actual damages while limiting the availability of other damages, the compromise restricted access to civil remedies and diminished the role of private enforcement.¹¹⁸ Furthermore, under the compromise, the advisory authority of the Study Commission was substituted for the investigatory and enforcement powers of the Privacy Commission.¹¹⁹ Finally, adoption of the routine use language freed federal agencies from strict adherence to the nondisclosure provision and introduced a means to circumvent the Privacy Act.¹²⁰ Only the active support and oversight of Congress and the executive branch could redress the imbalance.

B. *The Routine Use Exemption*

Routine use language first appeared in the House bill introduced by Congressman William S. Moorhead, Chairman of the Subcommittee on Foreign Operations and Government Information.¹²¹ The language was incorporated as an exemption to "one of the most important, if not the most important, provision of the [House] bill"—the nondisclosure provision.¹²² Under the routine use exemption, federal agencies were permitted to disclose personal information without the consent of the individual, provided that the

117. See *supra* notes 108-16 and accompanying text (reviewing compromise reached and finding House provisions favored over competing Senate provisions).

118. The compromise crippled the individual's ability to be made whole in two ways. First, the higher burden of proof insulated careless or inadvertent disclosures from remedial action. See S. REP. NO. 1183, *supra* note 37, at 24 (noting that "major threat to most Americans lies in the inadvertent, careless, and unthinking collection, distribution, and storage of records"), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 177. Consequently, the standard of proof ensured that a majority of abuses went unaddressed. See *id.* Second, damages were so limited as to remove any incentive to bring suit, except for the most egregious violations. *Id.* at 28, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 181. These conclusions are particularly troubling given that both the House and Senate recognized the need for private enforcement. See *id.* at 82 (stressing importance of private enforcement, absent independent enforcement authority), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 235; H.R. REP. NO. 1416, *supra* note 8, at 38 (advocating restoration of punitive or liquidated damages to ensure essential private enforcement), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 330; see also Project, *supra* note 15, at 1331 (finding that combination of higher standard of proof and reduced damages makes impossible fulfillment of congressional purpose of Privacy Act).

119. See *supra* notes 108-11 and accompanying text (contrasting powers of Privacy Commission with those of Study Commission).

120. See *infra* notes 136-68 and accompanying text (examining federal agency abuse of routine use exemption).

121. H.R. 16,373, *supra* note 90, § 552a(b)(2), 120 CONG. REC. 36,653, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 279.

122. H.R. REP. NO. 1416, *supra* note 8, at 12, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 305.

nature and scope of the routine use was published in the *Federal Register*.¹²³ The purpose of the routine use exemption was to facilitate orderly government conduct by allowing federal agencies to routinely exchange information for "housekeeping measures."¹²⁴ Recognizing the possibility for abuse, the House Committee on Government Operations pledged to oversee vigorously federal agency use of the exemption.¹²⁵

The Senate bill placed greater restrictions on the disclosure of personal information¹²⁶ and recognized fewer exemptions.¹²⁷ Unlike the House bill, the Senate bill did not provide for a "routine use" exemption.¹²⁸ The authors of the Senate bill considered such an exemption, but rejected it due to the potential for misuse.¹²⁹

The compromise reached between the Senate and House bills adopted the routine use language.¹³⁰ In lieu of a conference report,

123. *Id.*

124. *Analysis of Compromise Amendments*, *supra* note 39, at 40,881, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 988; *see supra* notes 95-96 and accompanying text (examining concern over impediment to orderly government conduct); Office of Management and Budget, Privacy Act Implementation Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 28,953 (1975) [hereinafter *OMB Guidelines*] (noting routine use exemption introduced in recognition of corollary purposes to which collected information may be "appropriate and necessary" for "efficient conduct of government" and "in the best interest of both the individual and the public"), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 1030. Representative Moorhead explained the rationale of the exemption:

It would be an impossible legislative task to attempt to set forth all of the appropriate uses of Federal records about an identifiable individual. It is not the purpose of the bill to restrict such ordinary uses of the information. Rather than attempting to specify each proper use of such records, the bill gives each Federal agency the authority to set forth the 'routine' purposes for which the records are to be used under the guidance contained in the committee's report.

In this sense 'routine use' does not encompass merely the common and ordinary uses to which records are put, but also includes all of the proper and necessary uses even if such use occurs infrequently.

120 CONG. REC. 36,967 (1974) (statement of Rep. Moorhead), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 957.

125. H.R. REP. NO. 1416, *supra* note 8, at 12, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 305.

126. S. 3418, *supra* note 90, § 202(a), 120 CONG. REC. 36,920, (providing that personal information was not to be disclosed unless individual written consent was obtained, recipient of information maintained its records in conformity with Privacy Act, and information was used for purpose for which it was collected), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 359.

127. *See id.* § 202(b)(1)-(4), 120 CONG. REC. 36,920 (recognizing as only exemptions disclosure: to agency personnel with need for such information in performance of their duties, to Bureau of Census, for statistical reporting or research, and pursuant to compelling circumstances affecting personal health or safety), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 359-60; *see also* S. REP. NO. 1183, *supra* note 37, at 20 (stating exemptions are to be kept to absolute minimum), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 173.

128. S. REP. NO. 1183, *supra* note 37, at 68-70, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 221-23.

129. *Id.* at 69, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 222.

130. *See Analysis of Compromise Amendments*, *supra* note 39, at 40,881 (examining and reconciling Senate and House disclosure requirements), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 987-88.

an Analysis of House and Senate Compromise Amendments to the Federal Privacy Act (*Analysis of Compromise Amendments*) was ordered printed in the *Congressional Record*.¹³¹ Neither the *Analysis of Compromise Amendments* nor OMB guidelines promulgated pursuant to the Privacy Act provide adequate insight into Congress' intent in adopting the routine use exemption.¹³²

The legislative history generally supports an interpretation of the routine use exemption consistent with the House bill, with one notable exception.¹³³ While the House bill permitted the federal agency discretion when establishing routine uses, the compromise language required that the routine use be compatible with the purpose for which the information was collected.¹³⁴ OMB guidelines interpreting the routine use language found mere compatibility inadequate and required that the routine use also "relate" to the purpose for collection.¹³⁵ Given the paucity of legislative history, interpretation

131. See *supra* note 39 (explaining printing of *Analysis of Compromise Amendments* in *Congressional Record*). The *Analysis of Compromise Amendments* provides in pertinent part:

The House bill contains a provision not provided for in the Senate measure exempting certain disclosures of information from the requirement to obtain prior consent from the subject when the disclosure would be for a 'routine use'. The compromise would define 'routine use' to mean: 'with respect to the disclosure of a record, the use of such records for a purpose which is compatible with the purpose for which it was collected.'

Where the Senate bill would have placed tight restrictions upon the transfer of personal information between or outside Federal agencies, the House bill, under the routine use provision, would permit an agency to describe its routine uses in the Federal Register and then disseminate the information without the consent of the individual or without applying the standards of accuracy, relevancy, timeliness or completeness so long as no determination was being made about the subject.

The compromise definition should serve as a caution to agencies to think out in advance what uses it will make of information. This act is not intended to impose undue burdens on the transfer of information to the Treasury Department to complete payroll checks, the receipt of information by the Social Security Administration to complete quarterly posting of accounts, or other such housekeeping measures and necessarily frequent interagency or intra-agency transfers of information. It is, however, intended to discourage the unnecessary exchange of information to other persons or to agencies who may not be as sensitive to the collecting agency's reasons for using and interpreting the material.

Analysis of Compromise Amendments, *supra* note 39, at 40,881, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 987-88.

132. See *supra* note 131 (providing discussion of routine use in *Analysis of Compromise Amendments*); OMB Guidelines, *supra* note 124, at 28,953 (providing series of excerpts from *Congressional Record*, but little substantive direction), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 1030-31.

133. See *supra* notes 131-32 and accompanying text (examining limited legislative history of routine use). When determining Congressional intent, courts have focused on the House bill. See *Perry v. FBI*, 759 F.2d 1271, 1279 n.4 (7th Cir. 1985) (finding House report "often the best barometer of Congressional intent"), *rev'd en banc on other grounds*, 781 F.2d 1294, *cert. denied*, 479 U.S. 814 (1986).

134. *Analysis of Compromise Amendments*, *supra* note 39, at 40,881, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 987.

135. OMB Guidelines, *supra* note 124, at 28,953, reprinted in SOURCE BOOK ON PRIVACY, *supra*

of the routine use exemption was left largely to the discretion of the federal agencies and the courts.

IV. FEDERAL AGENCY IMPLEMENTATION

A. Federal Agency Compliance

Recognizing the limits of congressional oversight and private enforcement,¹³⁶ the Senate Committee on Government Operations concluded that "realistically . . . the implementation of the Act rests, finally, with the departments and agencies of the executive branch and the good faith, ethical conduct and integrity of the Federal employees who serve in them."¹³⁷ In reaching this conclusion, the Committee failed to acknowledge that compliance with the Privacy Act conflicted with the fundamental need of federal agencies to gather and to use information.¹³⁸ Entrusting federal agencies with responsibility for enforcement, therefore, rendered compliance problematic.¹³⁹

The tension between competing institutional and privacy interests is manifest in the routine use exemption.¹⁴⁰ The exemption was adopted to facilitate routine transfers of information by federal agencies, not to allow indiscriminate circumvention of the nondisclosure provision of the Privacy Act.¹⁴¹ To prevent abuse of the exemption, Congress required federal agencies to provide notice in the *Federal Register* of the nature and scope of every routine use.¹⁴²

note 8, at 1031. Although the literal distinction appears insignificant, it is apparent that OMB believed something more than mere compatibility was required. *Id.*

136. S. REP. NO. 1183, *supra* note 37, at 28, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 181.

137. *Id.*; see *An Overview*, *supra* note 11, at 326-27 (recognizing limited benefit of congressional oversight and concluding that agencies bear burden of enforcement).

138. See Belair, *Agency Implementation of the Privacy Act and the Freedom of Information Act: Impact of the Government's Collection, Maintenance and Dissemination of Personally Identifiable Information*, 10 J. MARSHALL J. PRAC. & PROC. 465 (1977) (examining impact of Privacy Act upon information collection and dissemination efforts by federal agencies and concluding that limitations imposed on federal agency authority by Privacy Act often conflict with actual federal agency practice).

139. One commentator aptly articulated the conflict:

To rely upon agencies to police the [Privacy] Act is, at best, to invite problems. Agency interest in efficiency, budgetary restrictions, and need for information could all too often conflict with the individual's desires and rights under this statute. Agencies cannot reasonably be expected to promote zealously that which is felt to be in conflict with their own interests.

An Overview, *supra* note 11, at 327.

140. Privacy Act of 1974, 5 U.S.C. § 552a(b)(3) (1988); see *supra* note 61 (providing statutory language of routine use exemption).

141. Privacy Act of 1974, 5 U.S.C. § 552a(b) (1988); see *supra* notes 121-24 and accompanying text (discussing purpose behind adoption of routine use exemption).

142. Privacy Act of 1974, 5 U.S.C. § 552a(e)(4) (1988); see *supra* note 71 (providing statutory language of routine use notice requirement). Notice is also provided through the statutorily required "Privacy Act Statement" which informs individuals for whom information is

This notice requirement was intended to facilitate the exercise of individual rights under the Privacy Act, while deterring the secret infringement of individual privacy by federal agencies.¹⁴³

Federal agencies, however, have used the notice requirement to bypass the nondisclosure provision through the publication of broadly worded routine use notices.¹⁴⁴ Federal agencies engaged in this practice treat the Privacy Act as a procedural notice statute, rather than a safeguard against government invasion of individual privacy.¹⁴⁵ After reviewing two years of federal agency performance

collected of the purpose for which the information will be used and the consequences of not providing the information. Privacy Act of 1974, 5 U.S.C. § 552a(c)(3) (1988).

143. See *supra* notes 106, 115 and accompanying text (discussing congressional intent and compromise when adopting notice requirements).

The notice requirement, however, is of questionable value to the average individual who is unlikely to have access to the *Federal Register*. See *The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974 CY 1982-1983* 118 (Dec. 4, 1985), cited in OFFICE OF TECHNOLOGY ASSESSMENT, ELECTRONIC USES AND INDIVIDUAL PRIVACY 17, 19 (1986) [hereinafter OFFICE OF TECHNOLOGY ASSESSMENT] (noting problem with value of notice requirement is limited access of general public to *Federal Register* in which notice is provided). Moreover, it is doubtful whether the average individual can read, let alone comprehend, the notices appearing in the *Federal Register*. See PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 506-10 (discussing limited effectiveness of federal agency notice to general public). Alternatively, the individual may seek out the annual compilation of Privacy Act notices. Once located, however, the individual faces the arduous task of attempting to find the relevant notice provision in a multi-volume compilation spanning more than 3,700 pages. See Office of the Federal Register, Privacy Act Issuances, 1987 Compilation V (1987) (composing 5 volumes and 3,732 pages of "descriptions of systems of records maintained on individuals by federal agencies which were published in the *Federal Register*" and "rules of each agency which set out the procedures that agencies will follow in helping individuals who request information about their records").

144. See H.R. REP. NO. 927, 101st Cong., 2d Sess. 67 (1990) (noting that "some agencies apply automatically all general routine uses to all systems of records" without adequate consideration for whether "some or all [of the] general routine uses are not compatible with the purpose of each system of records"); Berman & Goldman, *supra* note 7, at 17 (noting that concern of federal agencies is over compliance with notice requirements rather than compatibility of disclosure with purpose for collection).

145. See H.R. REP. NO. 927, *supra* note 144, at 67. The report states that:

Agencies proceed on the apparent belief that any disclosure can be authorized as long as a routine use has been established in accordance with the Privacy Act's procedures. This is a distortion of the law. There must be a connection between the purpose of the disclosure and the purpose for which the information was collected. In absence of a sufficient nexus between these two purposes, an agency cannot create routine uses simply because a disclosure would be convenient or to avoid the procedural requirements established in subsection (b) [nondisclosure provision] of the Privacy Act.

Id.

Representative Glenn English expressed the sentiment of many critics of federal agency complacency:

One of my chief concerns is that the bureaucracy, with the approval of OMB, has drained much of the substance out of the [Privacy] Act. As a result, the Privacy Act tends to be viewed as strictly a procedural statute. For example, agencies feel free to disclose personal information to anyone as long as the proper notices have been published in the *Federal Register*. No one seems to consider whether the Privacy Act prohibits a particular use of information.

Hearings on Oversight of Privacy Act, supra note 91, at 5 (opening statement of Rep. English).

under the Privacy Act, the Study Commission concluded that the routine use exemption had been applied "loosely and exclusively from the agency's point of view."¹⁴⁶

Federal agencies continue to circumvent the nondisclosure provision through broadly worded routine use notices.¹⁴⁷ In order to advance institutional interests and to achieve increased operational efficiency, federal agencies have abused the routine use exemption. The following examples illustrate the nature and extent of the abuse.

To ensure the efficient and accurate distribution of limited benefits and services, many federal agencies have developed enforcement branches to assist in the verification of eligible recipients and the detection of fraud and waste.¹⁴⁸ In furtherance of this goal, these federal agencies have adopted broadly worded routine uses to facilitate inter-agency exchange of enforcement and investigative information.¹⁴⁹ These federal agencies, however, have not considered whether the purpose of exchange is "compatible" with the purpose of collection and is thereby consistent with the statutory language of the routine use exemption.¹⁵⁰

Law enforcement agencies have also employed the routine use exemption to avoid the restrictive language of an applicable disclosure exemption.¹⁵¹ In 1975, Attorney General Edward H. Levi requested all federal agencies to establish a routine use for the transfer to law enforcement agencies of records indicating potential violations of the law.¹⁵² The United States Department of Justice (DOJ) also requested federal agencies to authorize as a routine use the transfer of personal information to DOJ for use in employment and security

146. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 519; see *Hearings on Oversight of Privacy Act*, *supra* note 91, at 51 (stating that notice requirement was "designed to require that the agencies examine the data, see if the use that the other agency was going to put it to was compatible with the reason for which it was collected, then issue notice so the public and other agencies and OMB could comment on the propriety of the exchange").

147. Belair, *supra* note 138, at 501; see *Narrowing the "Routine Use" Exemption*, *supra* note 11, at 133 (noting manner of federal agency application of routine use exemption is inconsistent with purpose of Privacy Act).

148. See *A Constitutional Analysis*, *supra* note 29, at 150 (noting that driving force behind federal agency expansion of enforcement and investigative mechanisms is accurate and proper distribution of federal entitlements).

149. See *id.* (finding widespread abuse of routine use exemption to facilitate "free flow" of enforcement and investigative information).

150. *Id.*; see *supra* note 61 (providing definition of routine use); *supra* notes 134-35 and accompanying text (examining compatibility requirement of routine use exemption).

151. See *Narrowing the "Routine Use" Exemption*, *supra* note 11, at 133-34 (examining efforts by Department of Justice to circumvent statutory restrictions of Privacy Act through routine use exemption).

152. *Id.* at 133; Belair, *supra* note 138, at 501.

investigations.¹⁵³ DOJ officials continued the practice, even after they recognized that the proposed uses for the collected information did not conform with the statutory definition of routine use.¹⁵⁴

The single greatest abuse of the routine use exemption, however, came from its application to computer matching.¹⁵⁵ Computer matching involves the comparison of separate federal agency record systems in an effort to detect fraud, waste, or abuse in government programs.¹⁵⁶ Although commendable, computer matching conflicted with the purpose of the routine use exemption and the goal of the Privacy Act to safeguard individual privacy.¹⁵⁷

In 1977, the Carter Administration instituted "Project Match," the first computer matching program designed by the Department of Health, Education, and Welfare to identify federal government employees who were fraudulently receiving welfare payments.¹⁵⁸ Proponents of the program justified it under the routine use exemption, arguing that the detection of fraud or waste in government programs furthered the protection of legitimate government interests and, therefore, was compatible with the purpose of computer matching.¹⁵⁹ Carl F. Goodman, General Counsel for the United

153. *Narrowing the "Routine Use" Exemption*, *supra* note 11, at 133; Belair, *supra* note 138, at 501.

154. *Narrowing the "Routine Use" Exemption*, *supra* note 11, at 134; Belair, *supra* note 138, at 501.

155. See *Hearings on Oversight of Privacy Act*, *supra* note 91, at 276-79 (statement of John Shattuck, American Civil Liberties Union) (noting misuse of routine use exemption to evade nondisclosure provision for computer matching). See generally *Computer Matching and Privacy Protection Act of 1986: Hearings on S. 2756 Before the Subcomm. on Oversight of Government Management of the Senate Comm. on Governmental Affairs*, 99th Cong., 2d Sess. (1986) (examining impact of computer matching on Privacy Act); *Oversight of Computer Matching to Detect Fraud and Mismanagement in Government Programs: Hearings Before the Subcomm. on Oversight of Government Management of the Senate Comm. on Governmental Affairs*, 97th Cong., 2d Sess. (1982) [hereinafter *Oversight of Computer Matching to Detect Fraud*] (surveying and reviewing computer matching programs by federal agencies).

156. Shattuck, *In the Shadow of 1984: National Identification Systems, Computer Matching, and Privacy in the United States*, 35 HASTINGS L.J. 991, 992 (1974). Similar problems have arisen from the use of "front-end verification." Berman & Goldman, *supra* note 7, at 18-20. Front-end verification is a form of computer matching which permits computer verification of information at the time an individual applies for benefits. *Id.* Although more restricted in scope than computer matching, front-end verification places the same privacy interests at risk. *Id.*

157. See *supra* notes 134-35 and accompanying text (examining compatibility requirement of routine use exemption); *infra* notes 243, 259-62 and accompanying text (reviewing judicial enforcement of compatibility test for routine use exemptions).

158. See STAFF OF HOUSE COMM. ON GOVERNMENT OPERATIONS, 98TH CONG., 1ST SESS., WHO CARES ABOUT PRIVACY? OVERSIGHT OF THE PRIVACY ACT OF 1974 BY THE OFFICE OF MANAGEMENT AND BUDGET AND BY THE CONGRESS 10 (Comm. Print 1983) [hereinafter *Who CARES ABOUT PRIVACY?*] (discussing Project Match); Shattuck, *supra* note 156, at 1003 (reviewing initial reluctance and ultimate acceptance of computer matching programs such as Project Match).

159. Berman & Goldman, *supra* note 7, at 15-16. The proponent's position was reflected in the routine use notices published in the *Federal Register*. *Id.* at 14. For example, one notice of a proposed match between records maintained by the Office of Personnel Management and

States Civil Service Commission, and other critics of the program rejected the proponents' compatibility argument as tenuous and opposed the program as violative not only of the routine use exemption, but also of the Privacy Act's protection of individual liberties.¹⁶⁰ The proponents of computer matching eventually prevailed, and initial reluctance gave way to widespread acceptance of the position that computer matching was justified under the routine use exemption.¹⁶¹ The pervasiveness of computer matching was staggering.¹⁶² In a 1986 study, the Office of Technology Assessment reported that in 1984, eleven cabinet-level departments and four independent federal agencies conducted 110 separate computer matching programs, consisting of 700 total matches and involving seven billion records.¹⁶³ Such abuse of the routine use exemption continued for eleven years before Congress took action.

In 1988, Congress enacted the Computer Matching and Privacy Protection Act (Computer Matching Act) which precludes treatment of computer matching as a routine use.¹⁶⁴ Although the Computer Matching Act eliminated one widespread abuse of the routine use exemption, it had no effect upon other questionable applications of the exemption.¹⁶⁵ Moreover, federal agency treatment of computer matching as a routine use is symptomatic of a greater problem—a

the Veterans' Administration proposed the following routine use: "An integral part of the reason these records are maintained is to protect the legitimate interests of the government, and therefore, such a disclosure is compatible with the purposes for maintaining these records." *Id.* at 14 n.43. See generally Kirchner, *Privacy: A History of Computer Matching in the Federal Government*, *COMPUTERWORLD*, Dec. 14, 1981, "In Depth" at 1 (providing comprehensive historical examination of bureaucratic battle over computer matching when first instituted and effect of OMB practices on matching practices).

160. Letter from Carl F. Goodman, General Counsel, Civil Service Commission, to Charles Ruff, Deputy Inspector General, Department of Health, Education, and Welfare (July 27, 1977), reprinted in *Oversight of Computer Matching to Detect Fraud*, *supra* note 155, at 122-25; Berman & Goldman, *supra* note 7, at 15 n.46.

161. Shattuck, *supra* note 156, at 1003.

162. See *Oversight of Computer Matching to Detect Fraud*, *supra* note 155, at 1-76 (noting that files of welfare and medicaid recipients, draft-aged taxpayers, veterans, federal employees, persons entitled to supplemental security income, and others were involved in computer matches).

163. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 143, at 52.

164. The Computer Matching and Privacy Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507-2514 (codified as amended at 5 U.S.C. §§ 552a(o)-(r) (1988)); see *infra* notes 209-11 and accompanying text (discussing enactment of Computer Matching Act and Privacy Act).

165. Examples of violations of the routine use exemption include the Securities and Exchange Commission's routine disclosure of derogatory information to other agencies and the Civil Service Commission's transmission of information on an individual's character, reputation, and personal characteristics to other agencies. *FEDERAL DATA BANKS AND CONSTITUTIONAL RIGHTS*, *supra* note 2, at xlv. These and similar abuses were not affected by the Computer Matching Act. *Id.*; see *id.* at xlv-xlv (concluding that Internal Revenue Service and Selective Service System profess confidentiality yet allow routine use disclosures to other agencies).

problem not addressed by the Computer Matching Act.¹⁶⁶ Left unchecked, the institutional interests of federal agencies will continue to eclipse individual privacy interests.¹⁶⁷ As long as federal agency compliance with the Privacy Act rests on self-enforcement, individual privacy will remain subject to unjustified government intrusion.¹⁶⁸

B. OMB Oversight

The Privacy Act assigns OMB chief responsibility for formulating guidelines on federal agency implementation of and for overseeing federal agency compliance with the Privacy Act.¹⁶⁹ In 1975, OMB issued comprehensive guidelines implementing and interpreting the Privacy Act,¹⁷⁰ which it later supplemented.¹⁷¹ Since 1975, OMB has sporadically issued guidelines on issues affecting the Privacy Act,¹⁷² but has yet to provide significant guidance on the application of the routine use exemption.¹⁷³

166. See *supra* notes 138-47 and accompanying text (examining internal agency conflict between administrative efficiency and protection of individual privacy interests).

167. See WHO CARES ABOUT PRIVACY?, *supra* note 158, at 36 (finding that "[p]rivacy interests frequently conflict with other important governmental interests such as economy and efficiency. As a result, there is a constant risk that privacy concerns will not be fully or fairly considered by federal agencies"); OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 143, at 6 (noting change in executive branch focus from privacy-related concerns to interest in efficiency, management, and budget).

168. See OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 143, at 17 (noting from review of studies on Privacy Act that major weakness of Privacy Act is its reliance upon individual federal agency initiative).

169. Privacy Act of 1974, 5 U.S.C. § 552a(v) (1988); see *supra* note 112 (providing statutory language of OMB responsibilities).

The Paperwork Reduction Act of 1980 (Paperwork Act) further requires OMB to monitor federal agency compliance with the Privacy Act. Pub. L. No. 96-511, 94 Stat. 2812 (codified as amended at 44 U.S.C. §§ 3501-3520 (1988)). For a discussion of the effect of the Paperwork Act on OMB responsibilities see WHO CARES ABOUT PRIVACY?, *supra* note 158, at 18-20 (finding no basis for claim that Paperwork Act enlarged scope of OMB oversight role).

170. OMB Guidelines, *supra* note 124, at 28,948-78.

171. Office of Management and Budget, Supplementary Guidance, 40 Fed. Reg. 56,741-43 (1975), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 1131-33.

172. See, e.g., Office of Management and Budget, Revised Supplemental Guidance on Implementation of the Privacy Act of 1974, 49 Fed. Reg. 12,338 (1984) (presenting OMB guidelines on relationship between Freedom of Information Act and Privacy Act); Office of Management and Budget, Privacy Act of 1974; Guidelines on the Relationship of the Debt Collection Act of 1982 to the Privacy Act of 1974, 48 Fed. Reg. 15,556 (1983) (presenting OMB guidelines on effect of Debt Collection Act of 1982); Office of Management and Budget, Privacy Act of 1974; Supplemental Guidance for Matching Programs, 44 Fed. Reg. 23,138 (1979) (presenting OMB guidelines on computer-matching programs), revised, Office of Management and Budget, Privacy Act of 1974; Revised Supplemental Guidance for Conducting Matching Programs, 47 Fed. Reg. 21,656 (1982).

173. H.R. REP. NO. 927, *supra* note 144, at 67. The report notes that

[p]art of the problem of routine use abuse is the result of a failure of OMB to issue sufficiently detailed guidance on interpreting the routine use provision of the law. OMB has also failed to publish model routine uses that prescribe the terms and conditions for disclosures that agencies throughout government must use.

After reviewing OMB's guidelines, the House Committee on Government Operations concluded that OMB had failed to fulfill its responsibility under the Privacy Act to provide guidance to the federal agencies.¹⁷⁴ OMB guidelines also fail to reflect changes in case law or federal agency experience under the Privacy Act.¹⁷⁵ In addition, OMB guidance has occasionally sanctioned federal agency practices which, arguably, were inconsistent with the Privacy Act.¹⁷⁶

In 1975, for example, in contravention of the language and spirit of the Privacy Act, OMB advised federal agencies to consider disclosure of records to congressional staff a routine use.¹⁷⁷ Another example involved OMB guidance on computer matching. In 1979, OMB promulgated the first guidelines on computer matching,¹⁷⁸

174. WHO CARES ABOUT PRIVACY?, *supra* note 158, at 2. The conclusion of the House Committee is widely shared. *See id.* at 8-9 (reviewing complaints of witnesses that OMB abandoned its responsibilities under Privacy Act).

175. *See* 2 J. O'REILLY, *supra* note 89, ch. 21.06, at 21-23 (noting OMB reluctance to conform with case law); WHO CARES ABOUT PRIVACY?, *supra* note 158, at 35 (finding OMB guidance not "reflective of experience with the law, problems encountered by agencies, or court decisions").

176. *See* OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 143, at 17 (noting after review of Privacy Act studies that OMB guidelines contradict purpose of Privacy Act).

177. Office of Management and Budget, Implementation of the Privacy Act of 1974, Supplementary Guidance, 40 Fed. Reg. 56,741 (1975). OMB recommended that federal agencies adopt a routine use for all record systems to permit disclosure "to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual." *Id.* at 56,742. The proposed routine use would "obviate the need for the written consent of the individual in every case where an individual requests assistance of the member which would entail a disclosure of information pertaining to the individual." *Id.* Moreover, OMB advocated that:

[i]n those cases where congressional inquiry indicates that the request is being made on behalf of a person other than the individual whose record is to be disclosed, the agency should *advise* the congressional office that the written consent of the subject of the record is required. The agency should not contact the subject unless the congressional office requests it to do so.

Id. Although expedient, the proposed routine use effectively provided that federal agencies should abandon their oversight and enforcement responsibilities under the Privacy Act.

The guidelines were OMB's response to congressional pressure and complaints about the refusal of federal agencies to release records in response to congressional staff inquiries. *Narrowing the "Routine Use" Exemption*, *supra* note 11, at 134. The federal agencies properly rejected the staff inquiries as outside the scope of the congressional disclosure exemption, which is limited to requests from either house of Congress or its committees. *Id.*; *see* Privacy Act of 1974, 5 U.S.C. § 552a(b)(9) (1988).

178. Office of Management and Budget, Privacy Act of 1974; Supplemental Guidance for Matching Programs, 44 Fed. Reg. 23,138 (1979). The revised guidelines were proposed "to aid agencies in balancing the government's need to maintain the integrity of Federal programs with the individual's right to personal privacy." *Id.* at 23,139. The most significant requirement imposed by the guidelines was the need for a cost-benefit analysis. *Id.* Additional reporting and operating requirements were established. *Id.* at 23,139-42. Computer matching continued after the promulgation of the guidelines, although at a reduced pace. Kirchner, *supra* note 159, "In Depth" at 15-16. For a discussion of computer matching programs and their implementation by federal agencies, *see supra* notes 155-63 and accompanying text (discussing use of routine use exemption to facilitate computer matching programs).

which it revised in 1982¹⁷⁹ to eliminate virtually every safeguard established in its earlier guidelines.¹⁸⁰ Predictably, the revised guidelines encouraged, rather than discouraged, federal agency misuse of the routine use exemption.¹⁸¹

In addition to promulgating guidelines, OMB is responsible for oversight of federal agency compliance with the Privacy Act.¹⁸² In this capacity, OMB has been severely criticized for failing to meet its obligations under the Privacy Act.¹⁸³ Critics claim that OMB has "virtually abdicated responsibility" for overseeing federal agency compliance.¹⁸⁴ In particular, OMB has failed to exercise effective oversight of the routine uses employed by federal agencies.¹⁸⁵ Con-

179. Office of Management and Budget, Privacy Act of 1974; Revised Supplemental Guidance for Conducting Matching Programs, 47 Fed. Reg. 21,656 (1982).

180. See WHO CARES ABOUT PRIVACY?, *supra* note 158, at 11-13 (comparing requirements under 1979 and 1982 guidelines). The guidelines eliminated the cost-benefit analysis requirement and relaxed the notice and reporting requirements. *Id.* at 10-12.

181. See *id.* (reviewing OMB guidelines on computer matching and concluding that they resulted in increased use of computer matching); *id.* at 35 (recognizing influential role of Inspectors General who operated numerous matching programs behind revised guidelines); see also *supra* notes 155-63 and accompanying text (discussing misuse of routine use exemption to allow computer matching).

182. Privacy Act of 1974, 5 U.S.C. § 552a(v) (1988); see *supra* note 169 (reviewing expanded oversight responsibility of OMB under Paperwork Act); see also WHO CARES ABOUT PRIVACY?, *supra* note 158, at 17-24 (describing scope of OMB oversight role).

183. See Berman & Goldman, *supra* note 7, at 17 (concluding that "neither OMB nor any of the other agencies . . . have played an aggressive role in making sure that agencies . . . are equipped to comply with the [Privacy] Act and are, in fact, doing so") (quoting PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 21); WHO CARES ABOUT PRIVACY?, *supra* note 158, at 21, 38 (finding OMB oversight based solely on submitted record systems reports which do not include information on "limitations in disclosure; accounting requirements; access and correction procedures; notice requirements; information collection and maintenance limitations; and the requirement for safeguarding of information").

184. *Hearings on Oversight of Privacy Act*, *supra* note 91, at 259 (statement of John Shattuck, American Civil Liberties Union). For similar views, see *id.* at 201 (statement of Professor David H. Flaherty) (stating that "OMB has never done any effective monitoring of the implementation and impact of the Privacy Act"); *id.* at 46 (statement of James Davidson) (stating "today it [(the Privacy Act)] is probably lying there relatively dormant with very little enforcement or at least only occasional enforcement"); *id.* at 240 (statement of Ronald Plessner, Counsel to Commission) (stating that "OMB has done relatively little in conjunction with its statutory requirements to provide guidance and assistance to oversight of the implementation of the provisions of the Privacy Act").

185. Currently, OMB employs approximately 50 desk officers to oversee federal agency compliance with the Privacy Act. Telephone interview with OMB Staff Specialist (Oct. 3, 1990) [hereinafter *Telephone Interview*]. Each desk officer is assigned to one or more federal agencies and is responsible for reviewing agency reports on new or altered systems and proposed *Federal Register* notices submitted pursuant to the Privacy Act. Privacy Act of 1974, 5 U.S.C. § 552a(r) (1988); see Office of Management and Budget, Management of Federal Information Resources, Circular No. A-130, Appendix I, 50 Fed. Reg. 52,730, 52,739-41 (1985) [hereinafter OMB Circular No. A-130] (outlining contents and procedural requirements of reports). These reports include information concerning how proposed routine uses satisfy the compatibility requirement of the Privacy Act. *Id.* at 52,740.

Neither the Privacy Act nor OMB require an independent review of routine uses employed by federal agencies. *Telephone Interview*, *supra*. OMB oversight, therefore, is limited to those routine uses reported by the federal agencies. *Id.* Once a record system has been approved, however, there is a presumption that any proposed routine use is compatible and proper

sequently, objectionable federal agency practices have gone unchecked.¹⁸⁶ OMB's performance to date evinces its inability to provide adequate oversight and guidance to the federal agencies.

V. CONGRESSIONAL OVERSIGHT

Absent a constitutionally protected right to privacy in personal information, responsibility for safeguarding personal privacy fell upon Congress.¹⁸⁷ Recognizing this duty, the House Committee on Government Operations voiced its intention to "exercise a vigorous oversight check on agencies" in order to ensure strict compliance with the routine use exemption.¹⁸⁸ The Senate also recognized the need for aggressive oversight of the Privacy Act.¹⁸⁹

The principal congressional oversight mechanism in the Privacy Act is the requirement that every federal agency report to Congress

under the Privacy Act. *Id.* Consequently, any routine use proposed subsequent to OMB approval can escape review. *Id.*

Any problems with the submitted reports or proposed notices are brought to the attention of the federal agency by the assigned desk officer. *Id.* Although the Privacy Act does not empower OMB with enforcement authority, the federal agencies are generally very responsive and willing to effectuate requested changes. *Id.* Unfortunately, because of a regular turnover in federal agency personnel charged with the enforcement of Privacy Act provisions, many of the errors and mistakes of predecessors are repeated. *Id.*

186. See H.R. REP. NO. 927, *supra* note 144, at 67, 68 (noting that "[t]here is no evidence OMB has increased its oversight of routine uses since 1982" and that "OMB has not attempted any systematic review of new routine uses"); WHO CARES ABOUT PRIVACY?, *supra* note 158, at 22 (finding that OMB failed to apply its oversight authority to temper agency utilization of routine use exemption).

187. 120 CONG. REC. 40,410 (1974) (remarks of Sen. Muskie) (noting that while courts recognize government's potential to invade individual privacy, responsibility to protect against such invasion lies with Congress), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 869.

188. H.R. REP. NO. 1416, *supra* note 8, at 12, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 305. One commentator observed the need for congressional oversight to protect against abuse of the routine use exemption:

The routine use provision carries with it the potential for serious abuse. Congressional oversight is presently the major check against wholesale agency publication designed to establish routine uses which cover situations where, in keeping with the spirit and the letter of the [Privacy] Act, disclosure would require the consent of the individual concerned. Individual actions against agencies provide a partial solution to this potential problem, but the overwhelming volume of material recently published by agencies suggests that the availability of such actions may not be sufficient to deter agency abuse.

An Overview, *supra* note 11, at 314.

189. 120 CONG. REC. 40,409 (1974) (statement of Sen. Ervin) (recognizing need for "aggressive" oversight by Senate Committee on Government Operations), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 867. *But see* S. REP. NO. 1183, *supra* note 37, at 24 (recognizing limited congressional resources to keep track of every federal agency and data bank as required for "consistently constructive policy analysis"), *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 177. Clearly, the Senate's proposal for the establishment of a Privacy Commission with broad investigative and enforcement powers indicated a recognition of the potential limits and constraints of congressional oversight. *See supra* note 107 and accompanying text (examining authority of Privacy Commission).

on any proposal to establish or to amend a system of records.¹⁹⁰ Although not explicitly required by the statutory language of the reporting requirements in the Privacy Act, routine uses are included in the reports submitted by federal agencies.¹⁹¹ The reports are directed to the House Committee on Government Operations and the Senate Committee on Governmental Affairs¹⁹² and are intended to allow Congress to evaluate the potential impact of a proposed system of records on individual privacy rights.¹⁹³

Through its oversight of federal agency reports, Congress has been able to prevent some abuses of the routine use exemption.¹⁹⁴ The scope of congressional oversight, however, is limited by the content of the reports.¹⁹⁵ The reports provide information on proposed routine uses, but do not include information on their actual implementation.¹⁹⁶ Consequently, Congress is often unable to eval-

190. Privacy Act of 1974, 5 U.S.C. § 552a(r) (1988); see OMB Circular No. A-130, *supra* note 185, at 52,739-41 (presenting federal agency guidelines on contents and requirements of reports); see also WHO CARES ABOUT PRIVACY?, *supra* note 158, at 24-27 (reviewing reports submitted to Congress and finding them of limited usefulness). In addition to these federal agency reports, biennially Congress receives a report from the President that includes identification of changes to or additions in record systems. Privacy Act of 1974, 5 U.S.C. § 552a(s) (1988); see OMB Circular No. A-130, *supra* note 185, at 52,739 (outlining information federal agencies should be prepared to supply OMB for biennial reports). Finally, notice of all proposed routine uses must appear in the *Federal Register*. Privacy Act of 1974, 5 U.S.C. § 552a(e)(4)(D), (e)(11) (1988).

191. See OMB Circular No. A-130, *supra* note 185, at 52,740 (requiring federal agencies to provide information on why proposed routine uses comply with compatibility requirements); see also *infra* note 213 (examining proposed congressional initiative to explicitly require inclusion of routine uses in federal agency reports). In addition, the federal agencies must attach a copy of any proposed notices of routine uses that are to appear in the *Federal Register*. *Id.*

192. Privacy Act of 1974, 5 U.S.C. § 552a(r) (1988). Although both the House and Senate receive reports, only the former has shown any interest in exercising its oversight responsibilities. *Telephone Interview*, *supra* note 185; see also H.R. REP. NO. 927, *supra* note 144, at 68 (stating that "[r]outine uses have been regularly reviewed by this Committee [House Committee on Government Operations] whenever a notice has been received").

193. Privacy Act of 1974, 5 U.S.C. § 552a(r) (1988). Earlier language expanded upon the purpose to include "an evaluation of the probable or potential effect" on "the disclosure of information relating to such individuals." *Id.* § 552a(r) (Amendments). The change in statutory language resulted from amendments to the Privacy Act in 1988. Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, § 3(b), 102 Stat. 2507-2514 (codified as amended at 5 U.S.C. § 552a(r) (1988)).

194. Several federal agencies heeded congressional objection to their proposed information uses. See, e.g., WHO CARES ABOUT PRIVACY?, *supra* note 158, at 41 (responding to congressional objection of routine use as vague and overly broad, United States Postal Service modified routine use language); *id.* at 41 (reacting to congressional questioning of necessity of routine uses proposed by Federal Emergency Management Agency and resulting in their deletion); *id.* at 42 (objecting to automatic application of 11 general routine uses to new system of records by National Bureau of Standards and finding disclosures incompatible with narrow purpose of system of records); *id.* at 43 (finding Department of Transportation notice inconsistent with proposed routine uses and causing appropriate amendment of notice); *id.* at 50-51 (finding Department of Labor routine use too broad to indicate nature of disclosures and requiring amendment of notice).

195. See *id.* at 38-39 (noting limitations on congressional oversight); *supra* note 183 and accompanying text (discussing limitations of reporting requirements of 5 U.S.C. § 552a(r)).

196. WHO CARES ABOUT PRIVACY?, *supra* note 158, at 38-39.

uate whether actual disclosures are compatible with the proposed routine uses.¹⁹⁷ More importantly, while Congress may recommend modifications to proposed routine uses, it is powerless to enforce its suggestions.¹⁹⁸

For instance, in 1981, the United States Department of State proposed a routine use as part of a newly established system of records that would allow disclosures to other domestic or foreign government bodies "having interest" in the records.¹⁹⁹ Congress objected to the "interest" language in the proposed routine use as impermissibly vague.²⁰⁰ The Department of State responded with an explanation of its position, but refused to amend the routine use notice.²⁰¹

The Central Intelligence Agency (CIA) was even less receptive to congressional oversight.²⁰² In 1982, the CIA proposed a routine use for all of its systems of records to allow disclosure whenever "necessary or appropriate to enable the Central Intelligence Agency to carry out its responsibilities under any federal statute."²⁰³ Congress objected to the proposed routine use because it identified neither the purpose for disclosure nor the class of recipients.²⁰⁴ Congress asserted that because virtually any disclosure could be covered under the broad language, the proposed routine use was clearly contrary to the purpose and intent of the routine use exemption.²⁰⁵ William Casey, the Director of the CIA, rejected Congress' recommendations, stating that a more narrow routine use would be unworkable because it "would not be very helpful" to provide a detailed listing of every possible routine use.²⁰⁶ Congress responded that a comprehensive listing was, in fact, exactly what the Privacy Act required.²⁰⁷ The CIA chose to disregard Congress' suggestions and implemented the routine use as proposed.²⁰⁸

197. *Id.* at 38.

198. Based on information provided in the reports, the Government Information, Justice and Agriculture Subcommittee of the House Committee on Government Operations makes written or telephone inquiries to federal agencies recommending changes to proposed routine uses or notices or other actions inconsistent with the Privacy Act. *See id.*

199. *Id.* at 43.

200. *Id.* at 44. Routine uses must be "compatible" with the purpose for which the information was collected. Privacy Act of 1974, 5 U.S.C. § 552a(a)(7) (1988).

201. WHO CARES ABOUT PRIVACY?, *supra* note 158, at 44.

202. *See id.* at 46 (reviewing CIA confrontation with Congress over proposed routine use).

203. *Id.* (quoting Central Intelligence Agency, Privacy Act of 1974; Proposed Amendment of the Statement of General Routine Uses of the Systems of Records, 47 Fed. Reg. 18,943 (1982)).

204. *Id.*

205. *Id.*

206. *Id.*

207. *Id.*

208. *Id.*

While these examples suggest that Congress is powerless to enforce its recommendations on proposed routine uses, it can take legislative action to remedy perceived defects in the Privacy Act. Exercising that power, Congress finally took action in 1988 to rectify a long standing abuse of the routine use exemption.²⁰⁹ The Computer Matching Act ended years of misuse of the routine use exemption as a justification for computer matching.²¹⁰ Instead of prohibiting computer matching, however, the Computer Matching Act merely establishes independent procedural safeguards to protect individual privacy.²¹¹

The Computer Matching Act has been the only significant amendment to the Privacy Act.²¹² Congress has repeatedly declined to act upon proposed recommendations for legislative reform, including suggested revisions of the routine use exemption.²¹³ Congress has

209. Congress has expressly authorized the very kind of computer matching programs which prompted enactment of the Computer Matching Act. *See, e.g.*, Tax Reform Act of 1976, Pub. L. No. 94-455, 90 Stat. 1520 (codified at 26 U.S.C. § 1 (1988)); Social Security Amendments of 1977, Pub. L. No. 95-216, 91 Stat. 1510 (codified as amended at 7 U.S.C. § 441 (1988)); Food Stamp Act Amendments of 1977, Pub. L. No. 96-58, 93 Stat. 389-392 (1979) (codified as amended at 7 U.S.C. § 2012 (1988)); Food Stamp Act Amendments of 1980, Pub. L. No. 96-249, 94 Stat. 357 (codified as amended at 7 U.S.C. § 2012 (1988)); Food Stamp and Commodity Distribution Amendments of 1981, Pub. L. No. 97-98, 95 Stat. 1282 (codified as amended at 7 U.S.C. § 612c note (1988)); Department of Defense Authorization Act of 1983, Pub. L. No. 97-252, 96 Stat. 718 (codified at 5 U.S.C. § 5312 (1988)); Deficit Reduction Act of 1984, Pub. L. No. 98-369, 98 Stat. 494 (codified at 26 U.S.C. § 1 (1988)).

210. The Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507-2514 (codified at 5 U.S.C. §§ 552a(o)-(r) (1988)). Under the Computer Matching Act, computer matching is no longer considered a "routine use" of federal agency records. *Id.*; *see supra* notes 155-63 and accompanying text (discussing earlier abuse of routine use exemption to facilitate computer matching).

211. Privacy Act of 1974, 5 U.S.C. §§ 552a(o)-(r) (1988). The Computer Matching Act requires federal agencies to enter into a written agreement specifying the purpose for the match, the records to be matched, and a cost-benefit analysis for the match. *Id.* § 552a(o). Notice requirements provide that an individual subject to a match must be informed of the proposed match. *Id.* § 552a(o)(1)(D). The Computer Matching Act prohibits federal agencies from taking adverse action against an individual as the result of a match without first independently verifying the basis for the action. *Id.* § 552a(p). An individual also has the right to a hearing before any adverse action is taken depriving the individual of any benefits. *Id.*

212. *See* Ehlke, *supra* note 1, at 835-40 (examining three minor amendments to Privacy Act).

213. In The President's Annual Report on the Agencies' Implementation of the Privacy Act of 1974 for 1982 and 1983, Congress was encouraged to consider problems of interpretation and implementation of routine uses by federal agencies and to give clearer guidance on routine use disclosures. OFFICE OF TECHNOLOGY ASSESSMENT, *supra* note 143, at 18-19.

As part of its final report, the Study Commission recommended several legislative reforms, including a revised routine use test. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 519. Congress has not acted upon any of these proposals. *See* Ehlke, *supra* note 1, at 840 (recognizing failure of Congress to take action on Study Commission recommendations).

Recently, H.R. 3695 was introduced in the second session of the 101st Congress to make changes in federal agency requirements applying to the collection of information. H.R. 3695, 101st Cong., 2d Sess., 136 CONG. REC. H 11,895 (daily ed. Oct. 23, 1990) [hereinafter 3695]. After H.R. 3695 passed the House, it was conveyed to the Senate Committee on Governmental Affairs where it died in committee. 120 CONG. REC. H 11,903 (daily ed. Oct. 23, 1990)

Significantly, H.R. 3695 proposed to amend the Privacy Act's reporting requirements to

even been reluctant to hold oversight hearings on the Privacy Act, and, in fact, waited nine years before convening the first oversight hearings in 1983.²¹⁴ Because no legislative proposals were forthcoming, the hearings focused almost exclusively upon OMB guidance and oversight efforts.²¹⁵

A. *Recommendations for Improved Compliance and Oversight*

Current oversight and enforcement efforts have been unsuccessful in preventing widespread abuse of the Privacy Act. Federal agencies have been unwilling to police themselves.²¹⁶ Similarly, the efforts of Congress and OMB to provide guidance and to ensure compliance have met with limited success.²¹⁷ Seventeen years after the passage of the Privacy Act, neither Congress, OMB nor the federal agencies appear to be any more capable of effective oversight or enforcement. Ultimately, it is the flawed statutory enforcement and oversight scheme that is responsible for the failings of the Privacy Act.

If federal agency compliance is to improve, responsibility for guidance, oversight, and enforcement of the Privacy Act should be vested in an independent agency.²¹⁸ A "Privacy Board," modeled after the Senate's proposed Privacy Commission, should provide much-needed oversight and guidance.²¹⁹ In order to neutralize the inherent conflict between the information-gathering interests of federal agencies and the privacy-protection interests of private individuals, the Privacy Board should be authorized to promulgate binding

facilitate increased OMB and congressional oversight. H.R. REP. NO. 927, *supra* note 144, at 64-68. Section 204(a)(1) required the Director of OMB to conduct a review of federal agency routine uses with an emphasis on uniformity and consistency with applicable laws and published guidelines. H.R. 3695, *supra* § 204(a)(1), 136 CONG. REC. H 11,901. Results of the review were to be reported to Congress. *Id.* § 204(a)(2).

Section 204(b)(2) amended subsection (r) of the Privacy Act to require federal agencies to report on the establishment of proposed routine uses or significant changes to existing routine uses. *Id.* § 204(b)(2). The provision was included "because the existing requirement has not been uniformly interpreted to include the advance reporting of new and changed routine uses." H.R. REP. NO. 927, *supra* note 144, at 66.

214. See *Hearings on Oversight of Privacy Act*, *supra* note 91, at 1.

215. *Id.* at 22-24.

216. See *supra* notes 136-68 and accompanying text (discussing failure of federal agencies to enforce compliance); H.R. REP. NO. 927, *supra* note 144, at 67-68 (finding federal agency abuse of routine use provision of Privacy Act).

217. See *supra* notes 136-215 and accompanying text (reviewing limited success of OMB and Congress to prevent abuse and ensure compliance); see also H.R. REP. NO. 927, *supra* note 144, at 67 (recognizing OMB's failure to prevent abuse of routine use by federal agencies).

218. See PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 37 (recommending establishment of Federal Privacy Board empowered to enforce Privacy Act); *Hearings on Oversight of Privacy Act*, *supra* note 91, at 6 (statement of Rep. English) (voicing support for establishment of permanent, independent enforcement agency).

219. See *supra* note 107 (examining powers and responsibilities of Senate proposed Privacy Commission).

guidelines to coordinate federal agency compliance with the Privacy Act.²²⁰ In addition, Congress should grant the Privacy Board investigatory powers so that it might conduct inspections to oversee and to ensure compliance with the Privacy Act.²²¹ Finally, the Privacy Board must be empowered to enforce the Privacy Act.²²² Otherwise, Congress' experience with the CIA and the Department of State will be repeated and recommendations will go unheeded.²²³

Commentators have long favored the establishment of an independent enforcement agency.²²⁴ Unlike Congress and OMB, an independent Privacy Board is less likely to forsake individual privacy interests in favor of government interests in efficiency or information collection.²²⁵ As an independent authority, the Privacy Board will be more likely to succeed where Congress and OMB failed and to bring federal agencies into compliance with the Privacy Act.

VI. JUDICIAL ENFORCEMENT

A. Statutory and Procedural Barriers

The role of federal courts under the Privacy Act is limited.²²⁶ Federal court jurisdiction is restricted to four categories of violations: federal agency refusal to amend or to grant access to records, and federal agency failure to maintain records accurately or to comply with any other provision of the Privacy Act.²²⁷ This last category encompasses wrongful disclosure of personal information by a federal agency in violation of the routine use exemption.²²⁸

220. See, e.g., *An Overview*, *supra* note 11, at 327 (recognizing inevitable conflict between agency interests and privacy protection mechanisms imposed by Privacy Act); PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 518 (noting that conflict between agency information needs and limitations of Privacy Act presents great risk of improper disclosure); *supra* notes 138-41 (discussing conflict between federal agencies and Privacy Act).

221. See S. 3418, *supra* note 90, § 105(a), 120 CONG. REC. 36,918, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 342-43 (providing Privacy Commission with broad investigatory powers).

222. See S. REP. NO. 1183, *supra* note 37, at 23-27, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 176-80 (noting need for enforcement authority to ensure compliance).

223. See *supra* notes 199-208 and accompanying text (examining federal agency refusal to comply with congressional suggestions).

224. S. REP. NO. 1183, *supra* note 37, at 23, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 176; see also WHO CARES ABOUT PRIVACY?, *supra* note 158, at 36 (finding lack of Privacy Act oversight and need for increased representation of privacy interest, and recommending that Congress "consider alternatives to OMB as a privacy oversight agency").

225. See *supra* notes 138-41, 169-208 and accompanying text (finding conflict of interest in execution of Privacy Act in OMB and Congress).

226. See Privacy Act of 1974, 5 U.S.C. § 552a(g) (1988) (defining agency actions for which civil remedies are available).

227. *Id.* § 552a(g)(1)(A)-(g)(1)(D); see *supra* notes 80-83 and accompanying text (stating basis of jurisdiction and available judicial remedy).

228. Privacy Act of 1974, 5 U.S.C. § 552a(g)(1)(D) (1988); see *supra* note 61 (providing statutory language of routine use exemption) and notes 121-35 and accompanying text (re-

Claimants face formidable statutory and procedural barriers before a suit may be brought for wrongful disclosure in violation of the routine use exemption.²²⁹ Only the injured individual has standing to sue²³⁰ the federal agency responsible for the wrongful disclosure.²³¹ The individual bears the burden of proof²³² and has two years from the date of the wrongful disclosure to bring suit.²³³ The wrongful disclosure must be of personal information from a record²³⁴ contained in a system of records.²³⁵ In addition, the dis-

viewing legislative history of routine use exemption). See generally 2 J. O'REILLY, *supra* note 89, ch. 20.08 (examining scope and application of routine use exemption).

229. It should be noted, however, that exhaustion of administrative remedies is not a precondition to bringing a damages suit for wrongful disclosure. See, e.g., *Diederich v. Department of Army*, 878 F.2d 646, 647-48 (2d Cir. 1989) (finding damages suit under Privacy Act not barred by exhaustion doctrine); *Hubbard v. EPA*, 809 F.2d 1, 4 (D.C. Cir. 1986) (distinguishing section 552a(g)(1)(A) amending claims requiring exhaustion of remedies from section 552a(g)(4) damage claims not requiring exhaustion) (citing *Nagel v. Department of HEW*, 725 F.2d 1438, 1441 n.2 (D.C. Cir. 1984)); *Hewitt v. Grabicki*, 794 F.2d 1373, 1379 (9th Cir. 1986) (finding exhaustion of remedies not precondition for damages suit under Privacy Act).

230. Because injury and damages under the Privacy Act are individual, standing is limited to the person subject to adverse action. See 1 G. TRUBOW, *PRIVACY LAW & PRACTICE* 2-113 to -114 (1989) (recognizing associations denied right to represent member interests and unsuitability of class actions under Privacy Act); *Parks v. IRS*, 618 F.2d 677, 684-85 (10th Cir. 1980) (holding section 552a(g)(1) only provides for civil action brought by individual); see also *id.* (denying union standing to sue on behalf of adversely affected federal employees); *Dresser Indus., Inc. v. United States*, 596 F.2d 1231, 1237-38 (5th Cir. 1979) (refusing corporation standing to sue on employees' behalf), *cert. denied*, 444 U.S. 1044 (1980). But see *Parks*, 618 F.2d at 684-85 (recognizing possibility of association standing); *Hunt v. Washington State Advertising Comm'n*, 432 U.S. 333, 343 (1977) (holding associations have standing when members would otherwise have standing, interest is germane to association's purpose, and neither claims nor relief require participation of individual members of suit).

231. See, e.g., *Connolly v. Comptroller of the Currency*, 876 F.2d 1209, 1215 (5th Cir. 1989) (holding no cause of action against individuals for violations of Privacy Act); *Brown-Bey v. United States*, 720 F.2d 467, 469 (7th Cir. 1983) (stating Privacy Act claims properly dismissed when prison inmate sued individuals rather than agency); *Wren v. Harris*, 675 F.2d 1144, 1148 n.8 (10th Cir. 1982) (noting that Privacy Act authorizes civil action only against agency); see also *Saint Michael's Convalescent Hosp. v. California*, 643 F.2d 1369, 1373 (9th Cir. 1981) (finding no cause of action against state agencies under Privacy Act); *Irwin Memorial Blood Bank of the San Francisco Medical Soc'y v. American Nat'l Red Cross*, 640 F.2d 1051, 1057-58 (9th Cir. 1981) (holding no action lies against independent entity).

232. See *Johnston v. Horne*, 875 F.2d 1415, 1422 (9th Cir. 1989) (citing *Edison v. Department of Army*, 672 F.2d 840, 842 (11th Cir. 1982) in support of requirement that complaining party bears burden of proving violation).

233. Privacy Act of 1974, 5 U.S.C. § 552a(g)(5) (1988). Where the "agency has materially and willfully misrepresented any information required under this section 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 two year statute of limitations is extended to "any time within two years after discovery by the individual of the misrepresentation." *Id.*; see *Diliberti v. United States*, 817 F.2d 1259, 1262-64 (7th Cir. 1987) (finding failure to file action within statute of limitations deprived federal court of subject matter jurisdiction).

234. Privacy Act of 1974, 5 U.S.C. § 552a(a)(4) (1988); see *supra* note 41 (providing definition of record).

In keeping with its legislative origins, the definition of record has been broadly interpreted: The definition of . . . "Record" . . . has been expanded to assure the intent that a record can include as little as one descriptive item about an individual and that such records may incorporate but not be limited to information about an individual's edu-

cation, financial transactions, medical history, criminal or employment records, and that they may contain his name, or the identifying number, symbol, or other identifying marks, particularly assigned to the individual, such as a finger or voice print, or a photograph.

Analysis of Compromise Amendments, *supra* note 39, at 40,883, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 993. *See generally* 2 J. O'REILLY, *supra* note 89, ch. 20.06 (examining scope of record definition).

Courts generally have adhered to an expansive definition of "record." *See, e.g.*, *Chapman v. NASA* (*Chapman I*), 682 F.2d 526, 528-29 (5th Cir. 1982) (holding private notes taken by federal agency employer of meetings with employee reflecting employee job performance later incorporated into personnel file constituted records under Privacy Act), *cert. denied*, 469 U.S. 1038 (1984). OMB Guidelines, however, distinguish between federal agency records and records privately maintained by agency employees over which the agency exercises no control; the latter records fall outside the scope of the Privacy Act. OMB Guidelines, *supra* note 124, at 28,952, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 1028. Courts considering the distinction have held that private records are not subject to the restrictions of the Privacy Act. *See Bowyer v. Department of Air Force*, 804 F.2d 428, 431 (7th Cir. 1986) (finding supervisor's private notes not subject to Privacy Act requirements unless used by federal agency in decisions concerning employee status) (citing *Boyd v. Secretary of Navy*, 709 F.2d 684, 686 (11th Cir. 1983), *cert. denied*, 464 U.S. 1043 (1984)); *Chapman I*, 682 F.2d at 529 (recognizing private notes used to refresh memory but not involved in decision making process as outside scope of Privacy Act).

235. Privacy Act of 1974, 5 U.S.C. § 552a(a)(5) (1988); *see supra* note 43 (providing definition of "system of records"). *See generally* 2 J. O'REILLY, *supra* note 89, ch. 20.07 (examining nature and scope of system of records definition).

A system of records consists of records under federal agency control that are retrievable by reference to a personal identifier. Privacy Act of 1974, 5 U.S.C. § 552a(a)(5) (1988); *see OMB Guidelines*, *supra* note 124, at 28,952, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 1027 (examining requirements of systems of records). In contrast to the broad interpretation given to records, courts have narrowly interpreted system of records. *See Savarese v. Department of HEW*, 479 F. Supp. 304, 307-09 (N.D. Ga. 1979) (granting summary judgment when disclosed information was located in system of records, but not retrieved from system of records at time of disclosure), *aff'd mem. sub nom. Savarese v. Harris*, 620 F.2d 298 (5th Cir. 1980), *cert. denied*, 449 U.S. 1078 (1981); *Smierka v. Department of Treasury*, 447 F. Supp. 221, 228-29 (D.D.C. 1978) (finding daily investigative reports prepared as summaries of work not within scope of Privacy Act), *remanded on other grounds*, 604 F.2d 698 (D.C. Cir. 1979).

The requirement that the records be under federal agency control is designed to establish accountability and to distinguish agency records from private records. OMB Guidelines, *supra* note 124, at 28,952, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 1027. The "retrieved by" language in the definition of system of records acknowledges that records may exist containing personal information which do not fall within a system of records because they are not retrievable by a personal identifier. *Id.* at 28,952, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 1028.

Only records actually retrievable by a personal identifier, not those potentially retrievable, are protected by the Privacy Act. *Id.* This distinction has led one commentator to write: "[t]hus, the method used to retrieve a record rather than its substantive content determines its coverage under the Privacy Act." Ehrlke, *supra* note 1, at 831. Moreover, federal agencies are under no affirmative duty to place records within a system of records. *See, e.g.*, *Manuel v. Veterans Admin. Hosp.*, 857 F.2d 1112, 1119 (6th Cir. 1988) (declining to adopt contention that Privacy Act places duty on agency to place records in system of records), *cert. denied*, 489 U.S. 1055 (1989); *Wren v. Heckler*, 744 F.2d 86, 89 (10th Cir. 1984) (refusing to recognize duty of agency to place information in system of records); *Savarese*, 479 F. Supp. at 306 (finding that agency is not required to place information into records upon request nor to remove records upon request).

The possibility for abuse of the system of records language was aptly recognized by the United States Court of Appeals for the Sixth Circuit:

[T]he Privacy Act, in its current state, permits the situation whereby an employee may be deprived of his or her rights when an agency, or its custodian of records, purposely or with malice misdirects or prevents information from getting into the

closure must be willful or intentional,²³⁶ and cause²³⁷ the individual

system of records. This Court [recognizes] . . . that there are gaps in the Privacy Act. . . . The potential for abuse obviously does exist. *Manuel*, 857 F.2d at 1120. Nevertheless, the Sixth Circuit declined to take action, concluding that it was "the responsibility of Congress to fill in these gaps within the Privacy Act and clarify those areas and situations in which records must be placed within the agency's system of records." *Id.* The Study Commission also criticized the system of records language, finding it frustrated the purpose of the Privacy Act by permitting personal information to be held by agencies which was inaccessible to the individual. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 503-04. The Study Commission concluded that

the system-of-records definition has two limitations. First, it undermines the [Privacy] Act's objective of allowing an individual to have access to the records an agency maintains about him, and second, by serving as the activating, or "on/off switch" for the [Privacy] Act's other provisions, it unnecessarily limits the [Privacy] Act's scope. To solve this problem without placing an unreasonable burden on the agencies, the Commission believes the [Privacy] Act's definition of a systems of records should be abandoned and its definition of a record amended.

Id. (emphasis in original).

236. Privacy Act of 1974, 5 U.S.C. § 552a(g)(4) (1988).

The "willful or intentional" standard of proof was the product of a compromise reached between competing Senate and House versions. *See supra* note 113 (examining compromise standards of proof). "On a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct, . . . [the willful or intentional standard is to be viewed] as only somewhat greater than gross negligence." *Analysis of Compromise Amendments*, *supra* note 39, at 40,882, reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 990. Applying the intentional or willful burden of proof, courts have split on the standard's requirements. Some courts have required more than gross negligence. *See, e.g., Johnston v. Horne*, 875 F.2d 1415, 1422 (9th Cir. 1989) (requiring more than gross negligence, but declining to define gross negligence); *Andrews v. Veterans Admin. of the United States*, 838 F.2d 418, 425 (10th Cir.) (requiring conduct exhibiting more than gross negligence, and at minimum, reckless behavior), *cert. denied*, 488 U.S. 817 (1988); *Moskiewicz v. Department of Agric.*, 791 F.2d 561, 564 (7th Cir. 1986) (requiring conduct of "reckless behavior and/or knowing violations of the [Privacy] Act" for meeting greater than gross negligence). Other courts have found gross negligence sufficient. *See Chapman v. National Aeronautics & Space Admin. (Chapman II)*, 736 F.2d 238, 243 (5th Cir.) (per curiam) (likening gross negligence to willfulness), *cert. denied*, 469 U.S. 1038 (1984); *Albright v. United States (Albright II)*, 732 F.2d 181, 189 n.25 (D.C. Cir. 1984) (noting liability for violations caused by gross negligence). Still other alternative definitions of willful or intentional have been advanced. *See, e.g., Laningham v. Department of Navy*, 813 F.2d 1236, 1242 (D.C. Cir. 1987) (defining intentional or willful as conduct "so patently egregious and unlawful 'that anyone undertaking the conduct should have known it unlawful'") (quoting *Wisdom v. Department of Housing & Urban Dev.*, 713 F.2d 422, 425 (8th Cir. 1983), *cert. denied*, 465 U.S. 1021 (1984)); *Chapman II*, 736 F.2d at 243 (requiring evidence of "unlawful intent" or "ulterior motive"); *Albright II*, 732 F.2d at 189 (defining willful or intentional as "committing the act without grounds for believing it to be lawful, or by flagrantly disregarding others' rights under the [Privacy] Act").

Failure to meet the intentional or willful standard results in a complete bar to suit under the Privacy Act. The willful or intentional requirement has prevented numerous individuals from seeking redress for injuries suffered as a result of federal agency violations of the Privacy Act. *See, e.g., Andrews*, 838 F.2d at 424 (stating no remedy for Privacy Act violation absent showing of willful or intentional agency action); *Wisdom*, 713 F.2d at 424 (finding no liability where federal agency disclosure of inaccurate records was pursuant to its unchallenged regulations); *Perry v. Block*, 684 F.2d 121, 129 (D.C. Cir. 1982) (finding no "willful or deliberate" violation of Privacy Act where federal agency response to request for records was confused and delayed).

237. A causal connection between the adverse effect and alleged violation must be established. *See Albright v. United States (Albright II)*, 732 F.2d 181, 186-88 (D.C. Cir. 1984) (upholding lower court finding of no evidence of causal connection between violation and adverse effect in section 552a(g)(1)(D) claim); *Edison v. Department of Army*, 672 F.2d 840, 845-46 (11th Cir. 1982) (interpreting section 552a(g)(4) to require showing that allegedly erroneous records were proximate cause of adverse determinations); *see also Bruce v. United*

to suffer an adverse effect.²³⁸ If successful, the court may award actual damages, court costs, and attorney fees.²³⁹ Failure to surmount any one of these obstacles, however, is adequate grounds for

States, 621 F.2d 914, 917 n.9 (8th Cir. 1980) (questioning in *dicta* whether causation could be proved).

238. Privacy Act of 1974, 5 U.S.C. § 552a(g)(1)(D) (1988).

The "adverse effect" language was adopted from the House bill. H.R. 16,373, *supra* note 90, § 552a(g)(1)(C), 120 CONG. REC. 36,654, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 287. The Senate bill used similar language, granting standing to any "aggrieved person." S. 3418, *supra* note 90, § 303(b), (c), 120 CONG. REC. 36,921, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 371. The Senate language was designed to "afford the widest possible standing." S. REP. NO. 1183, *supra* note 37, at 83, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 236.

Courts have generally interpreted the adverse effect requirement broadly, in keeping with the language of the Senate bill. *See Parks v. IRS*, 618 F.2d 677, 682-83 (10th Cir. 1980) (interpreting adverse effect standing requirement broadly based on legislative history of Senate bill); *see also* Project, *supra* note 15, at 1328-29 (finding conflicting congressional intent, but recommending broad interpretation to fulfill purpose of civil remedies provision). Nevertheless, claims are frequently dismissed for failure to establish an adverse effect. *See Hewitt v. Grabicki*, 794 F.2d 1373, 1379 (9th Cir. 1986) (dismissing damages suit for absence of adverse action); *Harper v. United States*, 423 F. Supp. 192, 196-97 (D.S.C. 1976) (failing to find adverse effect as result of disclosed information). *But see Albright v. United States* (Albright II), 732 F.2d 181, 186 (D.C. Cir. 1984) (recognizing that emotional trauma alone is sufficient adverse effect, provided adequate showing of causation); *Parks*, 618 F.2d at 683 (finding mental distress and embarrassment actionable adverse effect).

239. Privacy Act of 1974, 5 U.S.C. § 552a(g)(4)(A), (B) (1988). *See generally* Note, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 *FORDHAM L. REV.* 611, 619-22 (1984) (examining remedial provisions of Privacy Act).

The award of court costs and attorney fees is mandatory in a successful damages suit, but otherwise discretionary. *See Analysis of Compromise Amendments*, *supra* note 39, at 40,882, *reprinted in* SOURCE BOOK ON PRIVACY, *supra* note 8, at 990. In a successful suit for damages, the Privacy Act provides that recoverable actual damages shall not be less than \$1000. Privacy Act of 1974, 5 U.S.C. § 552a(g)(4)(A) (1988). Absent statutory or legislative guidance, the courts have split on the extent of actual damages recoverable for wrongful disclosure. *Compare Fitzpatrick v. IRS*, 665 F.2d 327, 331 (11th Cir. 1982) (restricting actual damages to pecuniary damages, denying recovery for mental injuries, loss of reputation, and embarrassment) *and* *Albright v. United States* (Albright I), 558 F. Supp. 260, 264 (D.D.C. 1982) (limiting actual damages to out-of-pocket expenses), *aff'd*, 732 F.2d 181 (D.C. Cir. 1984) *with Parks v. IRS*, 618 F.2d 677, 680 (10th Cir. 1980) (seeking recovery for psychological injuries) *and Johnson v. Department of Treasury*, 700 F.2d 971, 983-86 (5th Cir. 1983) (defining actual damages to include damages for physical and mental injury where supported by competent evidence); *see also* 1 G. TRUBOW, *supra* note 230, at 2-118 to -120 (examining split in courts over scope of actual damages).

Courts have interpreted the remedial provisions of the Privacy Act as exclusive, and have been unwilling to extend injunctive relief for wrongful disclosure. *See, e.g., Doe v. Stephens*, 851 F.2d 1457, 1463 (D.C. Cir. 1988) (denying requested injunctive relief for return of medical records, exclusion of information from grand jury, and ban on disclosure by United States Attorney and staff); *Hastings v. Judicial Conference of the United States*, 770 F.2d 1093, 1104 (D.C. Cir. 1985) (refusing declaratory and injunctive relief as contrary to statutory language), *cert. denied*, 477 U.S. 904 (1986); *Parks*, 618 F.2d at 684 (finding improper implying broad right to injunctive relief). *But see Florida Medical Ass'n v. Department of HEW*, 479 F. Supp. 1291, 1299 n.8 (M.D. Fla.) (permitting injunctive relief against agency disclosure of personal records on ground that section 552a(g)(1)(D) confers general grant of jurisdiction to issue injunctive and declaratory relief), *vacated and remanded*, 601 F.2d 199 (5th Cir. 1979). At least one court has attempted to rectify the inadequacy of relief for wrongful disclosure by recognizing an implied private cause of action arising out of constitutional violations. *See Doe v. United States Civil Serv. Comm'n*, 483 F. Supp. 539, 565 (S.D.N.Y. 1980) (finding private cause of action warranted because Privacy Act afforded incomplete relief). Available remedial relief severely limits the ability of injured parties to be made whole and restricts relief to after-

dismissal.²⁴⁰

B. Notice Test and Compatibility Test

Only if the plaintiff overcomes these statutory and procedural barriers will the court reach the issue of wrongful disclosure. When determining whether disclosure of personal information is proper under the routine use exemption, courts consider the routine use notice published in the *Federal Register*, as well as the purposes for which the information was collected and disclosed.²⁴¹ Courts have generally relied upon two tests, the notice test and the compatibility test, when determining whether disclosure is proper under the routine use exemption. The notice test focuses on whether the disclosure falls within the explicit language of the routine use notice published in the *Federal Register*.²⁴² The compatibility test examines whether the disclosure is "compatible" with the purpose for which the information was collected.²⁴³

the-fact recovery of damages. See *Haase v. Sessions*, 893 F.2d 370, 374 (D.C. Cir. 1990) (explaining that Privacy Act provides for injunctive relief in only two specific situations).

240. See, e.g., *Diliberti v. United States*, 817 F.2d 1259, 1262 (7th Cir. 1987) (holding failure to file suit within two years deprives federal court of subject matter jurisdiction); *Hewitt v. Grabicki*, 794 F.2d 1373, 1379 (9th Cir. 1986) (dismissing damages suit for lack of adverse action); *Hanley v. Department of Justice*, 623 F.2d 1138, 1139 (6th Cir. 1980) (barring action under Privacy Act when records not within system of records); *Mervin v. Federal Trade Comm'n*, 591 F.2d 821, 827 (D.C. Cir. 1978) (affirming judgment against plaintiff for failure to prove agency did not amend records in response to request).

241. Privacy Act of 1974, 5 U.S.C. § 552a(a)(7) (1988); see *supra* note 61 (providing statutory definition of routine use); *supra* notes 121-35 and accompanying text (discussing legislative history of routine use exemption).

242. For applications of the notice test, see *Swenson v. United States Postal Serv.*, 890 F.2d 1075, 1078 (9th Cir. 1989) (narrowly interpreting routine use for disclosure to congressional office in response to congressional inquiry made at request of individual as inapplicable when individual did not request information); *Federal Labor Relations Auth. v. Department of Treasury*, 884 F.2d 1446, 1456 (D.C. Cir. 1989) (relying on *amicus* brief's interpretation of relevant language in routine use to find disclosure not pursuant to routine use), *cert. denied*, 110 S. Ct. 864 (1990); *Doe v. DiGenova*, 779 F.2d 74, 86-87 (D.C. Cir. 1985) (finding routine use for referral of records to law enforcement officials only when records themselves indicate violation of law and routine use published after disclosure); *Doe v. Naval Air Station*, 768 F.2d 1229, 1231-32 (11th Cir. 1985) (holding disclosure of vehicle registration information to law enforcement agencies not covered by administrative routine uses); *Parks v. IRS*, 618 F.2d 677, 681-82 (10th Cir. 1980) (finding no routine use in disclosure of information about not participating in savings bond program or soliciting such sales when such use not established through notice and comment rulemaking).

243. For applications of the compatibility test, see *Swenson v. United States Postal Serv.*, 890 F.2d 1075, 1078 (9th Cir. 1989) (adopting *Britt* test and finding disclosure in response to congressional inquiry concerning alleged undercounting of rural mail routes incompatible with purpose for collection, which was performance of routine personnel functions) (citing *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 549-50 (3d Cir. 1989)); *Doe v. Stephens*, 851 F.2d 1457, 1466-67 (D.C. Cir. 1988) (holding agency cannot simply promulgate routine uses to avoid non-consensual disclosure provision of Privacy Act); *Andrews v. Veteran's Admin. of the United States*, 613 F. Supp. 1404, 1413 (D. Wyo. 1985) (holding that enacted agency regulations must be consistent with purposes of Privacy Act and that inconsistent regulations are invalid and cannot justify release of covered information), *rev'd*, 838 F.2d 418 (10th Cir.), *cert. denied*, 488 U.S. 817 (1988).

The United States Court of Appeals for the District of Columbia Circuit applied the notice test in *Tijerina v. Walters*.²⁴⁴ Tijerina, a Texas bar applicant, brought suit against the Administrator of Veterans' Affairs for making an unsolicited disclosure of personal information to the Texas Board of Law Examiners (Board).²⁴⁵ During a random audit of Veterans' Administration Home Loan Guaranty applications conducted by the Veterans' Administration (VA), a discrepancy was discovered in Tijerina's file which was referred to the VA's Office of Inspector General (OIG).²⁴⁶ In the course of its investigation, OIG learned that Tijerina intended to take the Texas bar examination.²⁴⁷ Some time after OIG declined to prosecute Tijerina, a Deputy Inspector General wrote an unsolicited letter to the Board, informing the Board that OIG had investigated Tijerina and concluded that he had falsified a document in connection with his VA loan.²⁴⁸

The VA argued that the disclosure was protected by two routine uses published in the *Federal Register*.²⁴⁹ Interpreting the routine uses narrowly, the court rejected the VA's argument, and held that neither routine use justified the disclosure.²⁵⁰ The court found that OIG's disclosure based on suspicions of possible violations did not qualify under the routine use allowing disclosure where "a suspected violation or reasonably imminent violation of law" was anticipated.²⁵¹ Similarly, the court held that the routine use requiring disclosure in response to a request for information was inapplicable, because the Board had not "requested" the information.²⁵²

In *Britt v. Naval Investigative Service*,²⁵³ the United States Court of Appeals for the Third Circuit modified the notice test by requiring that the routine use published in the *Federal Register* provide adequate notice of the nature and purpose of the disclosure.²⁵⁴ *Britt* involved the unsolicited disclosure of a Naval Investigative Service

244. 821 F.2d 789 (D.C. Cir. 1987).

245. *Tijerina v. Walters*, 821 F.2d 789, 791 (D.C. Cir. 1987).

246. *Id.*

247. *Id.*

248. *Id.*

249. *Id.* at 793. One routine use permitted "disclosure of information relevant to a suspected violation or reasonably imminent violation of law to another agency charged with investigating the violation," while the other permitted "the VA to respond to an official request of a state agency by disclosing information relevant to that agency's decision whether to issue a license to an individual." *Id.*

250. *Id.* at 798.

251. *Id.*

252. *Id.*

253. 886 F.2d 544 (3d Cir. 1989).

254. *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 548 (3d Cir. 1989) (observing that Congress intended *Federal Register* to provide meaningful public notice of purpose of releasing information).

(NIS) report to Britt's employer, the Immigration and Naturalization Service.²⁵⁵ The court examined the routine use published in the *Federal Register* and found it to be overly broad.²⁵⁶ The court concluded that Britt received inadequate notice of the disclosure and its purpose.²⁵⁷ Rather than decide the case on these grounds, however, the court turned to the issue of compatibility.²⁵⁸

Applying the compatibility test, the Third Circuit rejected NIS's argument that disclosure need merely relate to the routine use published in the *Federal Register*.²⁵⁹ Drawing on the legislative history of the Privacy Act, the court required a dual inquiry into the purpose of collecting the personal information and the purpose of disclosure.²⁶⁰ Applying the compatibility test to the facts, the court held that the disclosure was incompatible with the purpose for which the information was collected.²⁶¹ The court explained that "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and its purpose in disclosing the information."²⁶²

In *Covert v. Harrington*,²⁶³ the United States Court of Appeals for the Ninth Circuit recognized the interrelationship between the statutory definition of routine use,²⁶⁴ the routine use exemption,²⁶⁵ the

255. *Id.* at 546.

256. The notice published in the *Federal Register* read:

ROUTINE USES OF RECORDS MAINTAINED IN THE SYSTEM, INCLUDING CATEGORIES OF USERS AND THE PURPOSES OF SUCH USES:

To other investigative units (federal, state or local) from whom the investigation was conducted, or who are engaged in criminal investigative and intelligence activities; federal regulatory agencies with investigative units.

Id. at 547 (quoting 50 Fed. Reg. 22,802-03 (1985)).

257. *Id.* at 548. The court recognized that the notice was adequate for disclosures to "other investigative units," but that the notice for "federal regulatory agencies with investigative units" gave no statement of purpose for which the information could be released. *Id.* at 547-48.

258. *Id.*

259. *Id.* at 549.

260. *Id.* The court's analysis is in keeping with the Study Commission's recommendation that "the compatible-purpose test of the routine use exemption should be augmented by a test for consistency with the conditions or reasonable expectations of uses and disclosure under which the information was provided, collected or obtained." PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 519.

261. *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 550 (3d Cir. 1989).

262. *Id.* at 549-50.

263. 876 F.2d 751 (9th Cir. 1989).

264. Privacy Act of 1974, 5 U.S.C. § 552a(a)(7) (1988); *see supra* note 61 (providing statutory language of routine use definition).

265. Privacy Act of 1974, 5 U.S.C. § 552a(b)(3) (1988); *see supra* note 61 (providing statutory language of routine use exemption); *supra* notes 121-35 and accompanying text (discussing legislative history of routine use exemption).

routine use notice published in the *Federal Register*,²⁶⁶ and the routine use notice²⁶⁷ provided at the time of information collection.²⁶⁸ Employees of the Hanford Nuclear Reservation brought suit, claiming that unlawful disclosure of their personnel security files by the Department of Energy (DOE) to the DOE Inspector General and the United States Department of Justice resulted in their criminal prosecution.²⁶⁹ The court declined to apply a compatibility test.²⁷⁰ Instead, the court held the disclosure unlawful on the grounds that it was contrary to the routine use notice provided to the employees on the form used to collect the disclosed information.²⁷¹ The court explained that this notice, like the notice appearing in the *Federal Register*, was an integral part of the statutory scheme of the Privacy Act and could not be ignored.²⁷² Both notice requirements were designed to let individuals know why and for what purpose personal information was requested of them.²⁷³

Judicial enforcement of the notice and compatibility tests has successfully prevented some abuses of the routine use exemption by federal agencies. Moreover, both tests advance objectives of the Privacy Act. Both tests enable individuals to determine what personal information is collected and disclosed by federal agencies and to ensure that the purpose for which personal information is used is consistent with the purpose for which it is collected.²⁷⁴ By interpreting routine use notices narrowly, courts encourage federal agencies to provide complete and accurate notification of the purposes for which collected information will be used.²⁷⁵ The compati-

266. Privacy Act of 1974, 5 U.S.C. § 552a(e)(4)(D) (1988); see *supra* note 71 (providing statutory language of notice requirement).

267. Privacy Act of 1974, 5 U.S.C. § 552a(e)(3)(C) (1988). Section (e)(3)(C) requires that every agency "inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual . . . the routine uses which can be made of the information, as published" in the *Federal Register*. *Id.*

268. *Covert v. Harrington*, 876 F.2d 751, 755-56 (9th Cir. 1989) (holding that agency's failure to inform plaintiff that information would be used for law enforcement purposes violates section 552a(e)(3)(C)).

269. *Id.* at 752.

270. *Id.* at 755.

271. *Id.* at 755-76.

272. *Id.* at 756. In reaching this statutory interpretation, the Ninth Circuit noted that its decision was consistent with that of the First Circuit, which had decided a similar issue. *Id.* (citing and quoting *Usher v. Secretary of Health & Human Servs.*, 721 F.2d 854, 856 (1st Cir. 1983) (finding no statutory reason for agency noncompliance with notice requirement)).

273. *Covert v. Harrington*, 876 F.2d 751, 756 (9th Cir. 1989).

274. See Privacy Act of 1974, 5 U.S.C. § 552a (1988) (Congressional Findings and Statement of Purpose).

275. See *Analysis of Compromise Amendments*, *supra* note 39, at 40,881 (cautioning agencies "to think out in advance what uses it will make of information"), reprinted in *SOURCE BOOK ON PRIVACY*, *supra* note 8, at 987-88.

bility test restricts attempts by federal agencies to circumvent the Privacy Act through the publication of broadly worded routine use notices. Enforcing the compatibility requirement prevents federal agencies from using information for purposes unrelated to those for which the information was collected. Finally, decisions such as *Cov-vert* and *Britt* encourage strict compliance with the notice requirements of the Privacy Act.

Unfortunately, courts are seldom able to apply these tests because they do not reach the issue of wrongful disclosure. Statutory and procedural barriers prevent ready access to the courts.²⁷⁶ Indeed, these obstacles frequently act as a complete bar to private enforcement and recovery under the Privacy Act.²⁷⁷ In its final report, the Study Commission recognized the inadequacy of civil remedies under the Privacy Act, stating that the enormous number of record systems, the expense and time in bringing an action, and the requirement of willful or intentional behavior make enforcement by the individual impracticable.²⁷⁸ The Study Commission noted that "[t]he circumstances in which an individual can bring suit, his possible reward for doing so, and the instances in which a court can order an agency into compliance with the [Privacy] Act are all too limited to provide an effective accountability mechanism."²⁷⁹ The Study Commission's observations are particularly troubling given the significance both the Senate and House placed on private enforcement.²⁸⁰

C. Recommendations for Judicial Enforcement

If private enforcement is to be an effective check against federal agency abuse, the incentives for bringing suit must be increased. The Privacy Act should be amended to provide injunctive relief for

276. See *supra* notes 226-40 and accompanying text (discussing formidable barriers to suit under Privacy Act); Ehlke, *supra* note 1, at 841 (concluding lack of litigation under Privacy Act is, in part, result of "ineffective remedial scheme"); 2 J. O'REILLY, *supra* note 89, ch. 22.04 (examining severe restrictions on access to civil remedies).

277. See 2 J. O'REILLY, *supra* note 89, ch. 22.04, at 22-17 (noting individual surmounting barriers has "won a rare victory").

278. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 529.

279. *Id.*

280. See S. REP. NO. 1183, *supra* note 37, at 16, 82-83, (encouraging widest possible civil enforcement and recognizing need for it given lack of alternative independent administrative enforcement body), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 169, 235-36; H.R. REP. NO. 1416, *supra* note 8, at 15 (relying on "constant vigilance" of individuals supported by "legal redress" to combat abuse by federal agencies), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 308. Courts have recognized the need to encourage private enforcement as well. See *Parks v. IRS*, 618 F.2d 677, 685 (10th Cir. 1980) (finding congressional purpose to encourage "self-help enforcement" in order to realize goals of Privacy Act).

all violations.²⁸¹ Injunctive relief would allow individuals to retrieve personal information wrongfully disclosed and to prevent its further dissemination. Also, recovery of actual damages should not be limited to pecuniary harm.²⁸² The injury suffered by an individual whose privacy has been invaded is personal in nature. Actual damages should reflect the personal, as well as the economic, harm suffered.²⁸³

Access to the courts must be facilitated as well. The standard of proof should be lowered in recognition of the fact that injuries suffered are rarely intentional.²⁸⁴ In addition, the distinction between record and system of records should be replaced with a definition less susceptible to manipulation.²⁸⁵ Unless Congress acts to remove these barriers or to limit their restrictive effect, the benefits of judicial enforcement will remain unrealized.

CONCLUSION

The Privacy Act of 1974 attempts to strike a balance between the government's need to gather and to use personal information and the individual's need to exercise control over that information. The balance, however, has never been achieved. Instead, the Privacy Act has favored the government's desire for information at the expense of individual privacy. Nowhere is this bias more evident than in the routine use exemption.

Adopted to facilitate orderly government conduct, the routine use exemption has been misused by federal agencies to disclose personal information without individual consent. OMB, federal agency, and congressional oversight have failed to effectively prevent abuse of the exemption. Nor have the courts, constrained by the language of the Privacy Act, been able to provide adequate relief

281. See Project, *supra* note 15, at 1331 (advocating adoption of injunctive relief for all violations).

282. See *id.* (arguing damages should not be limited if congressional goals are to be achieved).

283. See *supra* note 118 (examining limited remedial relief for wrongful disclosure under Privacy Act). Having reviewed the remedial provisions of the Privacy Act, the Study Commission concluded that Congress had intended to limit actual damages to recovery of "clear economic loss," but recommended that recovery be broadened to include general damages. PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 530.

284. See S. REP. NO. 1183, *supra* note 37, at 24 (recognizing threat of invasion of personal privacy comes from inadvertent action), reprinted in SOURCE BOOK ON PRIVACY, *supra* note 8, at 177; see also *An Overview*, *supra* note 11, at 325 (recognizing intentional or willful standard as greatest deterrent to suit under Privacy Act).

285. See PRIVACY PROTECTION STUDY COMMISSION, *supra* note 111, at 503-04 (finding that distinction between record and system of records frustrates purpose of Privacy Act); *A Constitutional Analysis*, *supra* note 29, at 149 (noting susceptibility of records definition to manipulation).

to injured individuals. Left unchecked, federal agencies, motivated by institutional priorities, have continued to abuse the routine use exemption.

Although an important first step, the Privacy Act has not achieved its goal of safeguarding individual privacy. Congress recognized the importance of the right to individual privacy in personal information, but failed to provide adequately for its protection. Until Congress addresses weaknesses in the Privacy Act such as the routine use exemption, individual privacy will remain subject to unchecked government intrusion.