

DISMANTLING THE PRIVATE ENFORCEMENT OF THE PRIVACY ACT OF 1974: *DOE V. CHAO*

*Haeji Hong, Esq.**

I. INTRODUCTION

What if our government released your social security number and your name to strangers without your consent?

Would you be outraged?

Would you feel violated?

Would you demand some type of remedy?

The social security number is one of the most valuable types of personal information that Americans possess in today's society. The ubiquitous nine-digit number ties each person to private, personal information such as his or her medical and insurance coverage, credit history, and governmental benefits and privileges such as a driver's license.¹ In this information age, Americans' greatest concern is the loss of privacy.² Disclosure of valuable personal information such as the social security number to strangers without the holder's consent is a

* J.D. from UC Davis in 1998. Currently clerking for Justice Harold F. See, Jr. of the Alabama Supreme Court. I would like to thank my family, Jongjoo Hong, Sunuk Hong, and Miji Hong for their support. I would also like to thank my friends, Julie R. Tuan, esq., James S. Kwon, esq., Chun T. Wright, esq., and John Palmerkern, esq. Their comments to this article, as well as their support, were invaluable.

1. *Preserving the Integrity of Social Security Numbers and Preventing Their Misuse by Terrorists and Identity Thieves: Joint Hearing Before the Subcomm. on Social Security of the Comm. on Ways and Means and the Subcomm. on Immigration, Border Security, and Claims of the House Comm. on the Judiciary*, 107th Cong. 11 (2002) (statement of James B. Lockart III, Deputy Commissioner of Social Security); UNITED STATES GENERAL ACCOUNTING OFFICE, SOCIAL SECURITY NUMBERS: GOVERNMENT BENEFITS FROM SSN USE BUT COULD PROVIDE BETTER SAFEGUARDS, GAO-02-352 at 2 (2002) [hereinafter GAO-02-352] (discussing the extent of government agencies' use of social security numbers), available at <http://www.gao.gov/new.items/d02352.pdf> (last visited Oct. 7, 2004).

2. See Gerald F. Seib, *Privacy Politics: Bush Maneuvers to the Right Spot*, WALL ST. J., June 27, 2001, available at 2001 WL-WSJ 2867878 (stating that the loss of personal privacy was the greatest concern among Americans according to a Wall St. Journal/NBC News poll).

significant violation of privacy and may cause real, significant harm. If the government made such a disclosure, reasonably, one would expect some type of remedy or compensation.

The Supreme Court disagreed. A divided Supreme Court recently decided in *Doe v. Chao*³ that the federal government's disclosure of the social security number, while constituting a violation of the Privacy Act of 1974 (the "Privacy Act"), was not enough to compensate the victim.⁴ After examining the civil remedy section of the Privacy Act, the Supreme Court ruled that the victim must also prove that he sustained actual damages before recovering the statutory minimum damage of \$1,000.⁵ This latest decision will greatly affect the enforcement of the Privacy Act by private citizens and reduce the effectiveness of the already much criticized Privacy Act.⁶

Congress enacted the Privacy Act to prevent the federal government from violating privacy rights of American citizens.⁷ Changing technology, i.e. computers, facilitated the government's collection and dissemination of private information and instigated

3. *Doe v. Chao*, 124 S. Ct. 1204 (2004).

4. *See id.* at 1206 and 1212 (holding that individuals adversely affected by a federal agency's violation of the Privacy Act of 1974 must prove actual damage to obtain the statutory award of \$1,000).

5. *See id.* at 1207-08.

6. PRIVACY PROT. STUDY COMM'N, PERSONAL PRIVACY IN AN INFORMATION SOCIETY 8 (1977) [hereinafter PERSONAL PRIVACY]; Steven A. Bercu, *Toward Universal Surveillance in an Information Age Economy: Can We Handle Treasury's New Police Technology?*, 34 JURIMETRICS J. 383, 425-26 (1994) (explaining that the Privacy Act's ineffectiveness stems from limited oversight, problems of the "routine use" exception, and general exemption for law enforcement agencies allow law enforcement network of FinCEN to operate relatively freely); William S. Challis & Ann Cavoukian, *The Case for a U.S. Privacy Commissioner: A Canadian Commissioner's Perspective*, 19 J. MARSHALL J. COMPUTER & INFO. L. 1, 9 (2000) (stating the Privacy Act's shortcomings include inconsistent application of privacy rules and lack of oversight and enforcement); Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy? An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 1000-01 (1991) (discussing the inadequacy of the civil remedies and barriers to access the courts); Paul M. Schwartz, *Privacy and Participation: Personal Information and Public Sector Regulation in the United States*, 80 IOWA L. REV. 553, 584-92 (1995) (criticizing the Privacy Act regarding the "routine use" exemption, computer matching, and transparency of data use). This article focuses only on the civil remedy provision of the Privacy Act. The Privacy Act has been heavily criticized regarding its scope, or lack thereof, in general, and many question whether the Privacy Act grants effective rights to individuals. This article does not endeavor to address the perceived structural flaws and limited scope of the Privacy Act. Instead, this article solely focuses on the civil remedy provision of the Privacy Act and its function as an effective enforcement mechanism of the rights set forth in the Privacy Act in light of the Supreme Court's decision in *Doe v. Chao*.

7. S. REP. NO. 93-1183, at 4-10 (1974), reprinted in JOINT COMM. ON GOV'T OPERATIONS, LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY, at 157-163 (1976) [hereinafter SOURCEBOOK]; H.R. REP. NO. 93-1416, at 2-10 (1974), reprinted in SOURCEBOOK, at 295-303. Coles, *supra* note 6, at 957-58.

congressional and executive concern for individual privacy.⁸ To protect against a new, rising privacy threat, the Privacy Act empowered individuals to safeguard personal information in several ways.⁹ Individuals can (1) determine what personal information has been collected by a federal agency,¹⁰ (2) verify the accuracy of such information,¹¹ (3) request corrections and amendments of inaccurate information,¹² and (4) request administrative review or bring a civil lawsuit.¹³ In order to effectuate the Privacy Act, Congress expected private citizens to enforce the Privacy Act by bringing civil actions against the government.¹⁴ Private enforcement of the Privacy Act could theoretically force governmental agencies to respect individuals' privacy and to adhere to the Privacy Act's mandate.¹⁵

This article argues that the Supreme Court's latest decision will effectively eradicate the only meaningful enforcement mechanism of the Privacy Act. Part II examines the history of the right to privacy and the legislative background to the Privacy Act.¹⁶ Part III reviews the Supreme Court's decision in *Doe v. Chao*.¹⁷ Part IV analyzes the Supreme Court's decision and explains the detrimental repercussions of *Doe v. Chao*.¹⁸ Finally, this article concludes by proposing legislative changes to the Privacy Act so that privacy rights can be enforced effectively.¹⁹

II. BACKGROUND

By the time Congress enacted the Privacy Act, the right to privacy was firmly entrenched in American legal rubrics. Most legal scholars

8. S. REP. NO. 93-1183, *supra* note 7, at 10, *reprinted in* SOURCEBOOK, *supra* note 7, at 163; H.R. REP. NO. 93-1416, *supra* note 7, at 4, *reprinted in* SOURCEBOOK, *supra* note 7, at 297.

9. 5 U.S.C. § 552a.

10. *Id.* § 552a(d)(1).

11. *Id.* § 552a(d)(2).

12. *Id.* § 552a(d)(3).

13. *Id.* § 552a(g)(1).

14. *See infra* notes 238-240 and accompanying text (discussing how Congress expected widespread private enforcement of the Privacy Act).

15. *See infra* notes 234-237 and accompanying text (discussing how private enforcement has been low). *See also* Coles, *supra* note 6, at 1000 (stating that incentives to bring a suit must be increased for effective private enforcement). As explained in footnote 6 of this article, this article does not attempt to address the issue of structural flaws and limited scope of the rights in the Privacy Act. *See supra* note 6 (explaining that this article does not attempt to address whether the Privacy Act is effective overall).

16. *See infra* Part II.

17. *See infra* Part III.

18. *See infra* Part IV.

19. *See infra* Part IV.D.

point to the seminal Harvard law review article, “The Right to Privacy” by Samuel D. Warren and Louis D. Brandeis, as the beginning of the right to privacy.²⁰ Warren and Brandeis declared the right to privacy as the “right to be let alone”²¹ and “the principle . . . of an inviolate personality.”²² Interestingly enough, the cause of Warren and Brandeis’ proclamation of the right to privacy was the rise of new technology and people’s abuse of such technology. More specifically, the media’s exploitations of the “sacred precincts of private and domestic life” with cameras and other mechanical devices perturbed Warren and Brandeis.²³ Such new acts of unethical behavior compelled Warren and Brandeis to eloquently articulate the existence of privacy rights.²⁴ Since then, technological innovations have prompted and shaped a parallel development of the right to privacy in common law and constitutional law to protect individuals against unanticipated intrusions.²⁵ The newest technological advancement — computers — pushed Congress into action in 1974, resulting in the passage of the Privacy Act.²⁶

A. *Development of the Right to Privacy*

1. Privacy Torts

The common law doctrine of the right to privacy began after an initial rejection of Warren and Brandeis’ theory of the existence of one’s right to privacy.²⁷ A public uproar followed a denial by the Court of

20. Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193 (1890); See Patricia Mell, *Seeking Shade in a Land of Perpetual Sunlight: Privacy as Property in the Electronic Wilderness*, 11 BERKELEY TECH. L.J. 1, 29-30 (1996) (discussing how although Warren and Brandeis did not first pronounce the right to privacy, they were first to recognize privacy as property and personal right); William L. Prosser, *Privacy*, 48 CAL. L. REV. 383, 384 (1960) (stating that Warren and Brandeis instigated a long line of law review discussions regarding the right to privacy).

21. Warren & Brandeis, *supra* note 20, at 193.

22. *Id.* at 205.

23. Prosser, *supra* note 20, at 383; Warren & Brandeis, *supra* note 20, at 195.

24. Prosser, *supra* note 20, at 383; Ken Gormley, *One Hundred Years of Privacy*, 1992 WIS. L. REV. 1335, 1348-52 (1992).

25. See *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001) (stating how the advance of technology affects the degree of privacy secured by the Fourth Amendment); see generally Gormley, *supra* note 24 (discussing privacy in the historical context with changing technology); Mell, *supra* note 20, at 12-13 (discussing history of technological innovation and how development of privacy right rose to counteract erosion of privacy caused by technological innovation).

26. 120 CONG. REC. 36,891 (1974) (remarks of Sen. Ervin), reprinted in SOURCEBOOK, *supra* note 7, at 769-70.

27. W. PAGE KEETON ET AL., PROSSER AND KEETON ON THE LAW OF TORTS 850 (W. Page Keeton ed., 5th ed. 1984); *Roberson v. Rochester Folding-Box Co.*, 171 N.Y. 538, 64 N.E. 442,

Appeals of New York in *Roberson v. Rochester Folding Box Co.* to recognize the right to privacy when a person's picture was used for advertisement without consent.²⁸ As a response, the New York legislature enacted a statute to create criminal and civil remedies against the use of any person's name or picture without his consent for advertisement.²⁹ Subsequently, in a similar case of misuse of an individual's name and picture, the Georgia Supreme Court repudiated the New York court's decision and embraced the right to privacy set forth by Warren and Brandeis in *Pavesich v. New England Life Ins. Co.*³⁰ A number of states followed Georgia's lead and the right to privacy gained firm authority and recognition in the First Restatement of Torts.³¹

Today, a majority of states recognize the existence of the common law right to privacy.³² According to Dean William L. Prosser³³ and the Second Restatement of Torts,³⁴ there are four forms of privacy intrusions. The right to privacy is invaded if one: (1) unreasonably intrudes upon an individual's seclusion,³⁵ (2) appropriates an individual's name or likeness,³⁶ (3) unreasonably publicizes an individual's private life;³⁷ or (4) unreasonably publicizes an individual to place him or her in a false light before the public.³⁸

According to the Second Restatement of Torts, a violation of the right to privacy entitles a person to recover damages for: "(a) the harm to his interest in privacy resulting from the invasion; (b) his mental distress proved to have been suffered if it is of a kind that normally results from such an invasion; and (c) special damage of which the invasion is a legal

544-556 (1902).

28. KEETON, *supra* note 27, at 850.

29. N.Y. Sess. Laws 1903, ch. 132, §§ 1-2, *amended by* N.Y. CIV. RIGHTS LAW, §§ 50-51 (McKinney 1909); KEETON, *supra* note 27, at 850-51. It is both a misdemeanor and a tort to "make use of the name, portrait or picture of any person for 'advertising purposes or for the purposes of trade' without his written consent." KEETON, *supra* note 27, at 850-51.

30. *Pavesich v. New England Life Ins. Co.*, 122 Ga. 190, 216-222, 50 S.E. 68, 79-81 (1905); KEETON, *supra* note 27, at 851.

31. KEETON, *supra* note 27, at 851.

32. RESTATEMENT (SECOND) OF TORTS § 652A reporter's note (1977).

33. Prosser, *supra* note 20, at 389; Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153, 1188-89 (1997).

34. RESTATEMENT, *supra* note 32, §§ 652A-652I; Gindin, *supra* note 33, at 1188-89.

35. RESTATEMENT, *supra* note 32, §§ 652A(2)(a), 652B.

36. *Id.* §§ 652A(2)(b), 652C.

37. *Id.* §§ 652A(2)(c), 652D.

38. *Id.* §§ 652A(2)(d), 652E. *But see* Jerry Kang, *Information Privacy in Cyberspace Transactions*, 50 STAN. L. REV. 1193, 1202-03 (1998) (categorizing privacy in different "clusters" by physical space, ability to make decisions, and flow of information).

cause.”³⁹ One can recover damages for emotional distress, personal humiliation, and non-pecuniary loss if he proves actual harm.⁴⁰ The Second Restatement of Torts also postulates that damages may have to be proven and cannot be presumed for the privacy violations involving unreasonable publicity,⁴¹ given the Supreme Court’s decision regarding damages in a similar tort law, defamation law.⁴²

2. Constitutional Rights to Privacy

The right to privacy is not an explicitly enumerated constitutional right. Nevertheless, the Supreme Court has upheld the right to privacy as a constitutionally protected right in various cases.⁴³ The initial constitutional right to privacy arose in the context of birth control.⁴⁴ Once the Court articulated the constitutional right to privacy, the Court expanded the right to privacy in other contexts as well.⁴⁵ Although the Supreme Court has not yet decided on whether informational privacy is constitutionally protected, the Court may decide such privacy is warranted given today’s technology.

a. Fundamental Privacy Rights

The Supreme Court first pronounced the constitutional right to privacy in *Griswold v. State of Connecticut*.⁴⁶ *Griswold* involved a

39. RESTATEMENT, *supra* note 32, § 652H.

40. *Id.* § 652H cmt. b and c.

41. *Id.* § 652H cmt. c.

42. See *Gertz v. Robert Welch, Inc.*, 418 U.S. 323, 349-50 (1974) (holding that recovery for defamation must be for actual injury and cannot be for presumed or punitive damage when liability is not based on a showing of knowledge of falsity or reckless disregard for the truth).

43. See *Griswold v. State of Connecticut*, 381 U.S. 479, 484-86 (1965) (finding that state birth control law violated constitutional right to marital privacy); *Roe v. Wade*, 410 U.S. 113, 152-54 (1973) (finding that the prohibition of abortion violated constitutional right to privacy regarding abortion decisions, but that this right was not unqualified); *Katz v. United States*, 389 U.S. 347, 353, 359 (1967) (finding that the Fourth Amendment protects individuals against unreasonable searches and seizures or unauthorized electronic surveillance); *Kyllo v. United States*, 533 U.S. 27, 33-34, 40 (2001) (finding that privacy secured by the Fourth Amendment changes with the advance of technology and that the unauthorized thermal imaging of home violated the expectations of privacy guaranteed by the Fourth Amendment); see also *Whalen v. Roe*, 429 U.S. 589, 605 (1977) (discussing in dicta the threat to privacy in the collection of personal information in computerized data banks).

44. *Griswold*, 381 U.S. at 485-86.

45. See *Kyllo*, 533 U.S. at 33-34, 40 (holding that the unauthorized thermal imaging of the home violated the right to privacy guaranteed by the Fourth Amendment); *Katz*, 389 U.S. at 353, 359 (holding that unauthorized electronic surveillance violated the right to privacy).

46. 381 U.S. 479 (1965).

Connecticut statute that prohibited the use of any birth control.⁴⁷ Although the right to privacy was not explicitly enumerated in the Bill of Rights, the Supreme Court clearly wanted to justify the constitutionality of marital privacy.⁴⁸ The Court was openly disgusted by the idea that the state could search private marital bedrooms for violations of the statute at issue.⁴⁹ To breathe life into the right to privacy, the Court examined various Bill of Rights cases. The Court observed that in many cases, certain associational rights emanated from the Bill of Rights but were not explicitly mentioned in the Bill of Rights.⁵⁰ Likewise, the Court found that zones of privacy can and do exist from the emanations of the guarantees in the penumbras of the First, Third, Fourth, Fifth, and Ninth Amendments.⁵¹

Subsequently, the Supreme Court addressed the constitutional right to privacy again in *Roe v. Wade*.⁵² In *Roe*, the Court addressed whether a Texas anti-abortion statute violated a woman's right to privacy.⁵³ The Court once again acknowledged that the right to privacy is not explicitly protected by the Constitution, but reiterated the constitutionality of the right of personal privacy.⁵⁴ In examining past cases, the Court found that the right of personal privacy includes only rights that can be deemed "fundamental" or "implicit in the concept of ordered liberty," and generally relates to activities associated with marriage.⁵⁵ Thus, the Court struck down the Texas anti-abortion law and found that a woman's decision to terminate a pregnancy is within the right of personal privacy.⁵⁶

47. *Griswold*, 381 U.S. at 480. The defendants and appellants gave information and advice to a married couple on the use of contraceptives. *Id.* They were found guilty as accessories under Section 54-196 of the General Statutes of Connecticut (1958 rev.) that allows criminal charges to be brought against those who assist another to commit any offense. *Id.*

48. *Griswold*, 381 U.S. at 485-86. The Supreme Court declared that marital privacy was "a right to privacy older than the Bill of Rights." *Id.* at 486.

49. *Id.* at 485-86.

50. *Id.* at 482-83. For example, the freedom of association is not explicitly guaranteed by the First Amendment but is protected as a peripheral First Amendment right. *Id.* at 483.

51. *Id.* at 484; *see also* *Roe v. Wade*, 410 U.S. 113, 152 (1973).

52. 410 U.S. 113 (1973).

53. *Id.* at 117-19.

54. *Id.* at 152.

55. *Id.*

56. *Id.* at 154, 162-64. However, a woman's right to have an abortion is not absolute and is balanced against the state's interest in protecting the woman's health and the potential human life. *Id.* at 162-63.

b. The Fourth Amendment and Privacy Rights

Having established the constitutionality of the fundamental right to privacy, the Supreme Court turned to the Fourth Amendment to further develop privacy rights in other contexts.⁵⁷ The Fourth Amendment prohibits unreasonable searches and seizures⁵⁸ and protects individuals' privacy from governmental intrusion.⁵⁹ As advanced technology heightened the government's surveillance capabilities, the Supreme Court faced cases on whether privacy rights should be adjusted accordingly.⁶⁰ Two notable cases are *Olmstead v. United States*⁶¹ and *Katz v. United States*.⁶²

The Supreme Court initially ruled that wire tapping a telephone line was not a search or seizure that required a warrant in *Olmstead v. United States*.⁶³ Noting that previous search and seizure cases dealt with physical invasions, the Court reasoned that telephone lines that extend beyond a home were outside the scope of Fourth Amendment protection.⁶⁴ Justice Brandeis, in his famous dissent, argued that the interpretation of the Fourth Amendment must adapt with technology and that Fourth Amendment privacy violations can occur without physical seizures.⁶⁵

Thirty-nine years later, the Supreme Court adopted Justice Brandeis' view and overruled *Olmstead* in *Katz v. United States*.⁶⁶ In *Katz v. United States*, law enforcement used advanced electronic equipment to eavesdrop and record telephone conversations conducted in a public telephone booth by the petitioner.⁶⁷ The Court found that such electronic surveillance violated privacy rights and protections afforded by the Fourth Amendment.⁶⁸ Instead of focusing on whether a

57. *Katz v. United States*, 389 U.S. 347 (1967).

58. U.S. CONST. amend. IV. The Fourth Amendment provides "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." *Id.*

59. Gindin, *supra* note 33, at 1185.

60. *See Katz v. United States*, 389 U.S. 347 (1967); *Olmstead v. United States*, 277 U.S. 438 (1928), *overruled in part by Katz v. United States*, 389 U.S. 347 (1967).

61. 277 U.S. 438 (1928).

62. 389 U.S. 347 (1967).

63. *Olmstead*, 277 U.S. at 466.

64. *Id.* at 464-66.

65. *Id.* at 477-78 (Brandeis, J., dissenting).

66. *Katz*, 389 U.S. at 353.

67. *Id.* at 348.

68. *Id.* at 353.

physical trespass occurred, the initial inquiry should focus on whether both an actual and reasonable expectation of privacy existed.⁶⁹ Furthermore, the Court clarified that the Fourth Amendment “protects people, not places . . . [,and what a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”⁷⁰

B. Informational Privacy

Technological advances are not intrinsically evil. Unfortunately, people abuse technological advances by finding new means to invade on one’s privacy. Therefore, such occasions create new interests for which privacy protection is necessary. Today, the computer’s ability to amass vast amounts of information has created a “market” in which personal information is a traded commodity.⁷¹ However, the computer’s concomitant ability to rapidly collect and disseminate personal information raises privacy concerns.⁷² The Supreme Court has not yet addressed whether informational privacy should also receive constitutional protection. However, the Supreme Court in *Whalen v. Roe* acknowledged that individuals may have privacy interests in personal information.⁷³

Whalen involved a New York statute that required doctors to forward copies of patients’ records regarding the prescription of certain drugs to the state so that the state could maintain a centralized computer file.⁷⁴ Although the statute prohibited the public disclosure of the patients’ identity, patients and physicians initiated the lawsuit to protect the privacy of patient information.⁷⁵ The Supreme Court upheld the constitutionality of the statute, holding that two types of privacy interests, disclosure of personal information and independence in decisional ability, were not impaired.⁷⁶ However, the Court noted that it was aware of threats to privacy created by unnecessary accumulation of personal information by the government in computer data banks and the unwarranted disclosure of such accumulated private information.⁷⁷

69. *Id.* at 361 (Harlan, J., concurring).

70. *Id.* at 351.

71. See Francis S. Chlapowski, Note, *The Constitutional Protection of Informational Privacy*, 71 B.U. L. REV. 133, 158-59 (1991); Mell, *supra* note 20, at 12-13.

72. Chlapowski, *supra* note 71, at 133, 158.

73. *Whalen v. Roe*, 429 U.S. 589, 605 (1977).

74. *Id.* at 591, 593-95.

75. *Id.* at 594-95.

76. *Id.* at 598-604.

77. *Id.* at 605-06. The Supreme Court stated:

Privacy torts and the constitutional right to privacy have developed on an ad-hoc basis in various contexts over time.⁷⁸ While the Supreme Court may address the need for constitutional protection of informational privacy,⁷⁹ without the right case, the Supreme Court may never decide the issue.⁸⁰ To remove some of the uncertainty, Congress enacted the Privacy Act to address concerns regarding the federal government's invasion of individuals' privacy.⁸¹

C. *The Privacy Act*

During the 1970's, the public grew alarmed over the federal government's increasing use of computers to collect, maintain, and use personal information.⁸² In response, Congress passed the Privacy Act.

A final word about issues we have not decided. 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. The right to collect and use such data for public purposes is typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures. Recognizing that in some circumstances that duty arguably has its roots in the Constitution, nevertheless New York's statutory scheme, and its implementing administrative procedures, evidence a proper concern with, and protection of, the individual's interest in privacy. We therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data - whether intentional or unintentional - or by a system that did not contain comparable security provisions. We simply hold that this record does not establish an invasion of any right or liberty protected by the Fourteenth Amendment.

Id.

78. See *supra* note 27-77 and accompanying text; Frederick Z. Lodge, Note, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 *FORDHAM L. REV.* 611, 613-14, 617-18 (1984).

79. The Supreme Court recently noted that the right to privacy guaranteed by the Fourth Amendment must adapt with the technological advances. *Kyllo v. United States*, 533 U.S. 27, 33-34 (2001).

80. Lodge, *supra* note 78, at 618 (noting uncertainty in the scope of right to privacy).

81. S. REP. NO. 93-1183, *supra* note 7, at 1, 6, reprinted in SOURCEBOOK, *supra* note 7, at 154, 159; 120 CONG. REC. 36,902-03 (1974) (remarks by Sen. Jackson), reprinted in SOURCEBOOK, *supra* note 7, at 800; Lodge, *supra* note 78, at 618. Congress found that it must act to protect individuals' privacy by regulating the federal agencies' use of personal information. The Privacy Act of 1974, Pub. L. No. 93-579, § 2(A)(5), 88 Stat. 1896 (1974).

82. S. REP. NO. 93-1183, *supra* note 7, at 1, 6, 11, reprinted in SOURCEBOOK, *supra* note 7, at 154, 159, 164; 120 CONG. REC. 36,893-94 (1974) (remarks by Sen. Percy), reprinted in SOURCEBOOK, *supra* note 7, at 776-78; *id.* at 36,900-03 (remarks by Sen. Nelson and Sen. Jackson), reprinted in SOURCEBOOK, *supra* note 7, at 794-801. Congress found that the privacy of individuals was affected by federal agencies' accumulation and use of personal information. The Privacy Act of 1974, Pub. L. No. 93-579, § 2(A)(1), 88 Stat. 1896 (1974).

The legislative history and congressional hearings regarding the Privacy Act reflect several concerns. Congress was concerned about the inherent dangers of the growing ease of electronic surveillance capabilities and the vast amount of information gathered about individuals in computer data banks.⁸³ With the growing ease of collecting information, Congress also feared that the government gathered unnecessary, personal information simply because it could.⁸⁴ Congress worried that such collected data could potentially lead to the abuse of power and transform America into an “Orwellian” society.⁸⁵ The Privacy Act of 1974 was meant to combat these concerns and curb the federal government’s informational privacy intrusions.⁸⁶

1. Overview of the Privacy Act

Based on the five principles of the “Code of Fair Information Practice” set forth in the report published in July 1973 by the Department of Health, Education and Welfare,⁸⁷ the Privacy Act

83. 120 CONG. REC. 36,902-03 (1974) (remarks by Sen. Jackson), *reprinted in* SOURCEBOOK, *supra* note 7, at 800-01; Major John F. Joyce, *Article: The Privacy Act: A Sword and a Shield But Sometimes Neither*, 99 MIL. L. REV. 113, 118-19 (1983). The Privacy Protection Commission charged with studying the application of the Privacy Act reported in its 1977 report of the accelerating trend on the accumulation of more information about an individual. PERSONAL PRIVACY, *supra* note 6, at 8.

84. S. REP. NO. 93-1183, *supra* note 7, at 11-13, *reprinted in* SOURCEBOOK, *supra* note 7, at 164-66; Joyce, *supra* note 83, at 119-20. For example, Congress noted that the army kept unnecessary information about civilians’ attitude toward government policies and created blacklists. S. REP. NO. 93-1183, *supra* note 7, at 13-14, *reprinted in* SOURCEBOOK, *supra* note 7, at 166. The Army had very few or no directives to guide their actions. *Id.* at 14, *reprinted in* SOURCEBOOK, *supra* note 7, at 167. The Army gathered irrelevant information such as personal finances, psychiatric diagnosis, and medical records and maintained them in computers. *Id.*, *reprinted in* SOURCEBOOK, *supra* note 7, at 167.

85. See 120 CONG. REC. 36,647 (1974) (remarks of Rep. Alexander), *reprinted in* SOURCEBOOK, *supra* note 7, at 893; *id.* at 36,651 (remarks of Rep. Biaggi), *reprinted in* SOURCEBOOK, *supra* note 7, at 904; Joyce, *supra* note 83, at 119-20; see also PERSONAL PRIVACY, *supra* note 6, at 8 (stating that record keeping allows organizations and government agencies to possibly monitor individuals).

86. S. REP. NO. 93-1183, *supra* note 7, at 1, 6, *reprinted in* SOURCEBOOK, *supra* note 7, at 154, 159; 120 CONG. REC. 36,902-03 (1974) (remarks by Sen. Jackson), *reprinted in* SOURCEBOOK, *supra* note 7, at 800; Lodge, *supra* note 78, at 618. Because of time pressures, the House and the Senate quickly reached a compromise bill through a series of informal meetings held by the committee leaders. Joyce, *supra* note 83, at 122-23. Consequently, no committee report exists to explain the legislative intent behind many key provisions of the bill as adopted. *Id.* at 123.

87. See S. REP. NO. 93-1183, *supra* note 7, at 8-9, *reprinted in* SOURCEBOOK, *supra* note 7, at 161-62; Joyce, *supra* note 83, at 119. The five principles of the “Code of Fair Information Practice” are:

There must be no personal data record-keeping systems whose very existence is secret.

There must be a way for an individual to find out what information about him is in a

embodies the following eight privacy principles:⁸⁸

There shall be no personal-data record-keeping system whose very existence is secret and there shall be a policy of openness about an organization's personal-data record-keeping policies, practices, and systems. (The Openness Principle)

An individual about whom information is maintained by a record-keeping organization in individually identifiable form shall have a right to see and copy that information. (The Individual Access Principle)

An individual about whom information is maintained by a record-keeping organization shall have a right to correct or amend the substance of that information. (The Individual Participation Principle)

There shall be limits on the types of information an organization may collect about an individual, as well as certain requirements with respect to the manner in which it collects such information. (The Collection Limitation Principle)

There shall be limits on the internal uses of information about an individual within a record-keeping organization. (The Use Limitation Principle)

There shall be limits on the external disclosures of information about an individual a record-keeping organization may make. (The Disclosures Limitation Principle)

A record-keeping organization shall bear an affirmative responsibility for establishing reasonable and proper information management policies and practices which assure that its collection, maintenance, use, and dissemination of information about an individual is necessary and lawful and the information itself is current and accurate. (The

record and how it is used.

There must be a way for an individual to prevent information about him that was obtained for one purpose from being used or made available for other purposes without his consent.

There must be a way for an individual to correct or amend a record of identifiable information about him.

Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take precautions to prevent misuse of the data.

S. REP. NO. 93-1183, *supra* note 7, at 9, *reprinted in* SOURCEBOOK, *supra* note 7, at 162.

88. PERSONAL PRIVACY, *supra* note 6, at 501.

Information Management Principle)

A record-keeping organization shall be accountable for its personal-data record-keeping policies, practices, and systems. (The Accountability Principle)⁸⁹

At the same time, the Privacy Act also attempts to balance the government's legitimate interest to function efficiently.⁹⁰ To do so, the Privacy Act prohibits federal government agencies' abilities to disclose, maintain, collect, and use information, but contains several exemptions.⁹¹

To address privacy concerns, a federal agency may not disclose any records unless the disclosure is made because of a written request by, or with a written consent from, the individual to whom the record pertains.⁹² An agency must also ascertain the accuracy of all records before releasing information.⁹³ A detailed accounting of disclosures must be kept so that the agency can forward any corrections or amendments to the released information.⁹⁴ An individual has a right to access his own records maintained by an agency and to correct or amend inaccuracies.⁹⁵ Additionally, an agency must maintain information relevant to the agency's purpose only.⁹⁶ If "information may result in adverse determination about an individual's rights, benefits, and privileges under Federal programs," then the agency must make every practical effort to collect information directly from the affected individual.⁹⁷ Finally, an agency must provide the appropriate means of security and confidentiality of the records to protect the privacy of the individuals.⁹⁸

These rights and privacy protections are balanced against the government's need to function efficiently.⁹⁹ Thus, the restrictions set forth are only applicable if the "records" are maintained in a "system of

89. *Id.* at 501-502. These principles are not attributable to any specific Congressional statement but are gleaned by the Privacy Commission. *Id.* at 502.

90. H.R. REP. NO. 93-1416, *supra* note 7, at 4, *reprinted in* SOURCEBOOK, *supra* note 7, at 297.

91. 5 U.S.C. § 552a(b)-(f) (2004).

92. *Id.* § 552a(b).

93. *Id.* § 552a(e)(6).

94. *Id.* § 552a(c).

95. *Id.* § 552a(d).

96. *Id.* § 552a(e)(1).

97. 5 U.S.C. § 552a(e)(2).

98. *Id.* § 552a(e)(10).

99. H.R. REP. NO. 93-1416, *supra* note 7, at 4, *reprinted in* SOURCEBOOK, *supra* note 7, at 297.

records.”¹⁰⁰ Additionally, the Privacy Act applies only to federal “agencies.”¹⁰¹ Furthermore, the heart of the Privacy Act, the non-disclosure requirement of individuals’ records, contains twelve exceptions that allow agencies to disclose records without the individual’s consent.¹⁰²

To prevent the federal government’s usurpation of exemptions and to guarantee the effectiveness of the rights afforded by the Privacy Act, Congress included a civil enforcement provision.¹⁰³ An individual may enforce the Privacy Act by bringing a civil action against an agency in a district court.¹⁰⁴ In addition to providing specific action and injunction as remedies,¹⁰⁵ the Privacy Act also allows successful plaintiffs to recover monetary damages.¹⁰⁶ This is the provision that the Supreme Court interpreted in *Doe v. Chao*.¹⁰⁷ Therefore, the provision warrants a

100. 5 U.S.C. § 552a(b), (c), (d), (e). *Id.* § 552a(a) lists definitions of terms used in the Privacy Act. Among the terms defined are “record” and “system of records.” *Id.* § 552a(a)(4)-(5). A “record” means:

any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transaction, 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. § 552a(a)(4) A “system of records” means “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.* at § 552(a)(5). Because of the advanced electronic searching capabilities that exist today, many have criticized that the agencies are maintaining significant amounts of records outside of the technical definition of “system of records.” Julianne M. Sullivan, Comment, *Will the Privacy Act of 1974 Still Hold Up in 2004? How Advancing Technology Has Created a Need for Change in the “System of Records” Analysis*, 39 CAL. W. L. REV. 395, 398-99, 402-05 (2003). For example, it is possible to retrieve records of an individual by searching for criteria unrelated to an individual’s identifying name or number, such as somebody else’s name. *Id.* at 403-04.

101. 5 U.S.C. § 552a(a)(1). See PERSONAL PRIVACY, *supra* note 6, at 497-99 (recommending that the Privacy Act should not expand to include organizations outside the federal government).

102. 5 U.S.C. § 552a(b)(1)-(12). Unfortunately, the liberal use of these “routine exceptions,” has eroded much of the strength of the non-disclosure requirement. Coles, *supra* note 6, at 978-83. Particularly, data matching of computer records to find individuals in more than one data base was routinely conducted under the “routine exception.” Schwartz, *supra* note 6, at 587-88. To protect individuals’ privacy against data matching, Congress passed a major amendment to the Privacy Act in 1988, the Computer Matching and Privacy Protection Act. Computer Matching and Privacy Protections Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507 (1988). The Computer Matching and Privacy Protection Act provides little substantive guidance, however, and procedural requirements set by the act may not completely eradicate privacy violations from data matching. Schwartz, *supra* note 6, at 588-89.

103. 5 U.S.C. § 552a(g).

104. *Id.* § 552a(g)(1)(D).

105. *Id.* § 552a(g)(2)(A)-(B).

106. *Id.* § 552a(g)(4).

107. *Doe v. Chao*, 124 S. Ct. 1204, 1208-10 (2004).

closer review of the language, legislative history, and subsequent interpretations and guidelines.

2. Damages Section: 5 U.S.C. §552a(g)(4) Statutory Language

Section 552a(g)(4) of the Privacy Act addresses the circumstances under which, and the amount of, damages that may be recoverable.¹⁰⁸ Section 552a(g)(4) first defines when the United States is liable for damages.¹⁰⁹ For the federal government to be liable, a plaintiff must prove an “adverse” effect on the plaintiff and an “intentional or willful” action by the agency.¹¹⁰ Stated another way, the plaintiff must prove that he suffered an “adverse” effect because the agency “intentionally or willfully:”¹¹¹ (1) failed to maintain records of the individual with the accuracy, relevance, timeliness, and completeness that was necessary to determine the qualifications, character, rights, or opportunities of, or benefits to, the individual based on such records;¹¹² or (2) failed to comply with any other provisions of the Privacy Act.¹¹³ Once the plaintiff proves these elements, then Subsections 552a(g)(4)(A) and (B) specify the recoverable amount of damages:¹¹⁴

(g)(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States

108. 5 U.S.C. § 552a(g)(4), (4)(A)-(B).

109. *Id.* § 552a(g)(4).

110. *Id.*

111. *Id.* § 552a(g)(1)(C)-(D), (g)(4). The damage section of the civil remedy provision of the Privacy Act provides that:

Whenever an agency . . .

(g)(1)(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, . . .

(g)(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and the costs of the action together with reasonable attorney fees as determined by the court.

Id.

112. *Id.* §552a(g)(1)(C), (g)(4).

113. 5 U.S.C. § 552a(g)(1)(D), (g)(4).

114. *Id.* § 552a(g)(4)(A)-(B).

shall be liable to the individual in an amount equal to the sum of—

actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

the costs of the action together with reasonable attorney fees as determined by the court.¹¹⁵

The majority in the Supreme Court decided that the language in Subsection 552a(g)(4)(A) requires a plaintiff to prove that he sustained actual damages before recovering the statutory minimum damage of \$1,000. A review of the legislative history concerning Section 552a(g)(4) is helpful in determining whether the Supreme Court accurately interpreted the damage section.

a. Legislative History

Both Democrats and Republicans agreed that privacy was a significant issue that required Congress to act quickly.¹¹⁶ However, because of Congress' swift passage of the Privacy Act, there are no detailed legislative comments or committee reports to explain many of the key provisions of the Privacy Act.¹¹⁷ Despite the paucity of legislative comments on the bill that was actually passed, one can glean some legislative intent from the changes made to the original versions of the Privacy Act. Because of the immense bipartisan interest, the Senate and House of Representatives each introduced its own version of the privacy bill.¹¹⁸ The Privacy Act that Congress eventually passed reflects a compromise between the Senate's and House's version of the Privacy Act.¹¹⁹ In fact, one of the key compromises made between the Senate

115. *Id.*

116. S. REP. NO. 93-1183, *supra* note 7, at 10, *reprinted in* SOURCEBOOK, *supra* note 7, at 163.

117. Joyce, *supra* note 83, at 122-23. Because of time pressures, the House and the Senate quickly reached a compromise bill through a series of informal meetings by the committee leaders. *Id.* at 123. Consequently, no committee report exists to explain the legislative intent behind many key provisions of the bill as adopted. *Id.*

118. S. 3418, 93d Cong., 2d Sess. (May 1, 1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 9-28; H.R. 16,373, 93d Cong., 2d Sess. (August 12, 1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 239-257.

119. 120 CONG. REC. 40,405-13 (1974) (Analysis of House and Senate Compromise Amendments to the Federal Privacy Act), *reprinted in* SOURCEBOOK, *supra* note 7, at 858-77; *Id.* at 40,881-86 (Analysis of House and Senate Compromise Amendments to the Federal Privacy Act), *reprinted in* SOURCEBOOK, *supra* note 7, at 985-1001.

and the House related to the damages section of the Privacy Act.¹²⁰

The Senate was interested in providing strong enforcement and remedy provisions for individuals.¹²¹ The Senate's original version of the Privacy Act allowed individuals to recover actual and punitive damages, when appropriate, for any violation of the privacy bill.¹²² The Senate, then, revised the provision to drop the punitive damages remedy but allowed individuals to recover actual and general damages, in an amount no less than \$1,000, upon a showing of an agency's negligence.¹²³ The Senate never fully debated whether it intended individuals to prove damages in order to recover the statutory minimum of \$1,000 in any of the debates or hearings.¹²⁴ However, the Senate's memorandum during the Congressional debate indicates that Congress intended the \$1,000 statutory minimum recovery to be liquidated damages.¹²⁵ Therefore, the Senate most likely never intended individuals to prove actual damages before allowing recovery of the

120. 120 CONG. REC. 40,406-07 (1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 861-62; *id.* at 40,882, *reprinted in* SOURCEBOOK, *supra* note 7, at 989-90.

121. S. REP. NO. 93-1183, *supra* note 7, at 82-83, *reprinted in* SOURCEBOOK, *supra* note 7, at 235-36.

122. 120 CONG. REC. 12,649 (1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 27. The original Senate version as introduced by Senator Ervin stated:

304(b)Any person who violates the provisions of this Act, or any rule, regulation, or order issued thereunder, shall be liable to any person aggrieved thereby in an amount equal to the sum of—

any actual damages sustained by an individual;

punitive damages where appropriate;

in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

Id.

123. S. 3418, 93d Cong., 2d Sess. (as amended November 21, 1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 371. The revised Senate version of the act stated:

303(c)The United States shall be liable for the actions or omissions of any officer or employee of the Government who violates the provisions of this Act, or any rule, regulation, or order issued thereunder in the same manner and to the same extent as a private individual under like circumstances to any person aggrieved thereby in an amount equal to the sum of—

any actual and general damages sustained by any person but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

in the case of any successful action to enforce any liability under this section, the costs of the action together with reasonable attorney's fees as determined by the court.

Id.

124. *See* 120 CONG. REC. 36,885-36,921 (1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 763-838.

125. *Id.* at 36,891, *reprinted in* SOURCEBOOK, *supra* note 7, at 768. The amendment was made to allow "an individual suing under the Act . . . to recover both actual and general damages and . . . [include] a provision for liquidated damages of say \$1,000 into the assessed against the agency for a violation of the Act." *Id.*

statutory minimum of \$1,000.

On the other hand, the House, while concerned about remedy provisions for individuals, was more concerned about the scope of the government's liability.¹²⁶ The House's original version allowed an individual suffering from some "adverse" effect from an agency's violation of the act to recover punitive or actual damages, depending on the agency's level of intent.¹²⁷ The revised version adopted by the House, like the Senate, dropped the punitive damages provision. However, while the Senate's version only required an agency's negligence to find liability, the House allowed an individual to recover actual damages only if the agency's violation of the act was "willful, arbitrary, or capricious."¹²⁸

126. *Id.* at 36,659-60 (remarks of Rep. McCloskey, Rep. Fascell, and Rep. Erlenborn), reprinted in SOURCEBOOK, *supra* note 7, at 922-24.

127. H.R. 16,393, 93d Cong., 2d Sess. (August 12, 1974), reprinted in SOURCEBOOK, *supra* note 7, at 249-51. The original version stated that:

(f)(1) Whenever any agency (A) refuses to comply with an individual request under subsection (d)(1) of this section, (B) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to such individual's qualifications, character, rights, opportunities, or benefits that may be made on the basis of such records and consequently makes such a determination which is adverse to the individual, or (C) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual, such individual may bring a civil action against such agency . . .

In any suit brought pursuant to the provisions of subsection (f)(1) in which the court determines—

(A) that the agency's refusal or failure has been willful, the agency shall be liable to the individual in an amount equal to the sum of—

(i) actual damages sustained by the individual as a result of such refusal or failure; punitive damages allowed by the court; and

the costs of the action together with reasonable attorney's fees as determined by the court; or

(B) that the agency's refusal or failure has been negligent, the agency shall be liable to the individual in an amount equal to the sum of—

(i) any actual damages sustained by the individual as a result of such refusal or failure; and

(ii) the costs of the action together with reasonable attorney's fees as determined by the court.

Id.

128. H.R. 16,373, 93d Cong., 2d Sess. (as amended October 2, 1974), reprinted in SOURCEBOOK, *supra* note 7, at 288 and in H.R. REP. NO. 93-1416, *supra* note 7, at 31-32, reprinted in SOURCEBOOK, *supra* note 7, at 324-25. Thus, the revised House version retained other provisions of the remedy section but revised the amount of damage section to:

(3) In any suit brought under the provisions of subsection (g)(1)(B) and (C) of this section in which the court determines that the agency acted in a manner which was willful, arbitrary, or capricious, the United States shall be liable to the individual in an amount equal to the sum of—

The debate among the Congressmen regarding the elimination of the punitive damage section reveals concerns on the adequacy of the remedy and the government's exposure to potentially high liability.¹²⁹ Several Congressmen expressed concerns over the removal of the punitive damages provision because they believed that proving actual damages would be difficult.¹³⁰ Thus, many believed that actual damages alone would be an inadequate remedy.¹³¹ In fact, the House of Representatives debated whether to amend the bill to re-insert the punitive damage section when the agency acted in a "willful, capricious, and arbitrary" manner.¹³² The debate evinces that the House understood proving that an agency's violation was "willful, capricious, and arbitrary" would be difficult, but also feared that excessive liability could exceed the government's budgetary constraints.¹³³

The damages provision of the finalized Privacy Act reflects a compromise between the Senate and the House on the extent of the government's liability.¹³⁴ The extent of the government's liability depends on (1) the level of intent required to hold an agency liable and (2) the measure of damages allowed for recovery.¹³⁵ The Senate and the House compromised on both of these factors.¹³⁶ The Privacy Act's requirement to hold an agency liable for "intentional or willful" conduct is a lower level of intent required than the House's version of "willful, arbitrary or capricious" intent requirement but is a higher level of intent requirement than the Senate's version of negligent requirement.¹³⁷ By keeping the Senate's \$1,000 minimum recovery language, the finalized

-
- (A) actual damages sustained by the individual as a result of the refusal or failure; and
(B) the costs of the action together with reasonable attorney fees as determined by the court.

Id.

129. See *infra* notes 130-33.

130. H.R. REP. NO. 93-1416, *supra* note 7, at 38, *reprinted in* SOURCEBOOK, *supra* note 7, at 330.

131. *Id.*

132. 120 CONG. REC. 36,658-60 (1974) (remarks of Rep. Fascell, Rep. McCloskey, Rep. Eckhardt, and Rep. Erlenborn), *reprinted in* SOURCEBOOK, *supra* note 7, at 919-24.

133. *Id.* at 36,659-60 (remarks of Rep. Fascell and Rep. Erlenborn), *reprinted in* SOURCEBOOK, *supra* note 7, at 923.

134. Compare S. 3418, 93d Cong., 2d Sess. (as amended November 21, 1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 371 with H.R. 16,373, 93d Cong., 2d Sess. (as amended October 2, 1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 288.

135. See *infra* notes 136-138.

136. Compare S. 3418, 93d Cong., 2d Sess. (as amended November 21, 1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 371 with H.R. 16,373, 93d Cong., 2d Sess. (as amended October 2, 1974), *reprinted in* SOURCEBOOK, *supra* note 7, at 288.

137. 120 CONG. REC. 40,406 (1974) (Analysis of House and Senate Compromise Amendments to the Federal Privacy Act), *reprinted in* SOURCEBOOK, *supra* note 7, at 862.

Privacy Act also allows for damages greater than the House's version of "actual damages" recovery, but allows less than the Senate's previous version, which had provided for "general damages" as well.¹³⁸

The analysis of the compromised damages provision submitted by the House and the Senate does not explicitly address whether Congress intended individuals to prove actual damages before recovering the statutory minimum of \$1,000.¹³⁹ However, interpretations by two entities following the passage of the Privacy Act are helpful on this issue.¹⁴⁰ Congress charged the Privacy Protection Study Commission (the "Commission") to study and recommend changes to the Privacy Act and the Office of Management and Budget (the "OMB") to oversee and create guidelines in implementing the Privacy Act.¹⁴¹ Following the passage of the Privacy Act, the Commission published a report and the OMB released guidelines, on the damages provision of the Privacy Act.¹⁴²

b. Subsequent Studies, Recommendations, and Guidelines

Congress established the Commission to serve for two years to examine certain issues concerning the Privacy Act, including whether the government should be liable for general damages resulting from a willful or intentional violation of the Privacy Act.¹⁴³ The Commission did not explicitly address whether individuals must prove "actual damages" in order to recover the statutory minimum damage of \$1,000. What the Commission did recommend, however, implied that the Commission did not believe individuals had to prove "actual damages" in order to recover the statutory minimum damage of \$1,000.¹⁴⁴

The Commission first addressed the standing requirement of the individual in Section 552a(g)(4) before addressing recoverable

138. See S. 3418, 93d Cong., 2d Sess. (as amended November 21, 1974), reprinted in SOURCEBOOK, *supra* note 7, at 371; H.R. 16,373, 93d Cong., 2d Sess. (as amended October 2, 1974), reprinted in SOURCEBOOK, *supra* note 7, at 288.

139. *Id.* at 40,406, reprinted in SOURCEBOOK, *supra* note 7, at 861-62; *id.* at 40,882, reprinted in SOURCEBOOK, *supra* note 7, at 989-90.

140. See *infra* notes 141-162.

141. The Privacy Act of 1974, Pub. L. No. 93-579, §§ 5, 6, 88 Stat. 1896 (1974).

142. *But see* Baker v. Dep't of Navy, 814 F.2d 1381, 1383 (9th Cir. 1987) (stating that although OMB guidelines are not binding on the courts, courts look to the guidelines for guidance); Zeller v. United States, 467 F. Supp. 487, 497 (D.C.N.Y. 1979) (stating that OMB guidelines are not binding on the courts).

143. The Privacy Act of 1974, Pub. L. No. 93-579, § 5(c)(2)(B)(iii), 88 Stat. 1896, 1905 (1974).

144. PERSONAL PRIVACY, *supra* note 6, at 529-32.

damages.¹⁴⁵ According to the Commission, Section 552a(g)(4) required an individual to prove his standing by showing that he suffered “actual injury” or “adverse effect” before he could recover any damages.¹⁴⁶ The Commission found that civil remedies were ineffective, in part, because of the difficulty in proving individuals’ standing or showing an “actual injury.”¹⁴⁷ The Commission recommended enforcing compliance with the Privacy Act and allowing individuals’ standing to bring lawsuits without requiring individuals to show an “injury or adverse effect.”¹⁴⁸ If the Commission believed that a standing requirement of “actual injury” was too difficult to prove, surely the Commission would have also addressed the difficulty of proving “actual damages” itself for recovery of the statutory minimum of \$1,000. The House certainly addressed the difficulty of proving “actual damages.”¹⁴⁹ Yet, the Commission did not address, or even recommend, eliminating proof of “actual damages” for recovery of statutory minimum.

Nor did the Commission fail to discuss Section 552a(g)(4)(A) or the “actual damages” provision of the civil remedies. Because of Congress’ specific mandate to the Commission to examine whether to include “general damages” provision, the Commission provided a thoughtful analysis of the meaning of the term “actual damages.”¹⁵⁰ The Commission found that the term “actual damages” was synonymous with the term “special damages” as used in defamation cases to allow recovery for pecuniary losses only.¹⁵¹ In light of the limited amount of recovery and in the interest of balancing individuals’ privacy protection and the public purse, the Commission recommended amending the “actual damages” provision.¹⁵² The Commission recommended replacing the term “actual damages” with the term “special damages and general damages,” with certain restrictions.¹⁵³ The limits set on the “general damages” would allow the minimal recovery of \$1,000, but no more than \$10,000 in excess of any special damages.¹⁵⁴

The Commission’s recommendations show that the Commission

145. *Id.* at 529.

146. *Id.*

147. *Id.*

148. *Id.*

149. *See supra* notes 130-133 and accompanying text (discussing the debate in the House regarding the elimination of punitive damage provision and adequacy of the actual damage as remedy).

150. PERSONAL PRIVACY, *supra* note 6, at 530-32.

151. *Id.* at 530.

152. *Id.* at 531.

153. *Id.* at 530.

154. *Id.* at 531.

carefully and thoroughly considered the effects and consequences of the damage provision. Thus, the conspicuous lack of analysis on the issue of requiring proof of “actual damages” for recovery of the statutory minimum of \$1,000 strongly intimates that the Commission did not interpret the Privacy Act to require such proof from individuals.

The OMB, on the other hand, explicitly stated that the Privacy Act does not require individuals to prove “actual damages” in order to recover the statutory minimum of \$1,000.¹⁵⁵ Congress conferred more permanent responsibilities to the OMB; Congress directed the OMB to (1) create guidelines and regulations for agencies to implement the Privacy Act; and (2) assist and oversee the implementation.¹⁵⁶ Accordingly, the OMB issued its first Privacy Act Guidelines on July 9, 1975, just six months after the passage of the Privacy Act.¹⁵⁷ With respect to the civil remedy provision, the OMB interpreted that:

When the court finds that an agency has acted willfully or intentionally in violation of the Act in such a manner as to have an adverse effect upon the individual, the United States will be required to pay:

Actual damages or \$1,000, whichever is greater; and

Court costs and attorney fees.¹⁵⁸

Although the OMB has amended its Privacy Act Guidelines numerous times over the past 30 years, significantly, the OMB never altered its interpretation of the civil remedy provision.¹⁵⁹ Thus, the

155. See *infra* notes 157-160 and accompanying text.

156. The Privacy Act of 1974, Pub. L. No. 93-579, § 6, 88 Stat. 1896, 1905 (1974). The Privacy Act stated that:

§ 6. The Office of Management and Budget shall—
develop guidelines and regulations for the use of agencies in implementing the provisions of Section 552a of Title 5, United States Code, as added by Section 3 of this Act; and provide continuing assistance to and oversight of the implementation of the provisions of such section by agencies.

Id.

157. Office of Management and Budget, Privacy Act Guidelines, 40 Fed. Reg. 28,949 (1975) [hereinafter OMB GUIDELINES].

158. *Id.* at 28970. Although OMB Guidelines are not binding on the courts, courts give deference to the guidelines in interpreting the Privacy Act. *Baker v. Dep’t of Navy*, 814 F.2d 1381, 1383 (9th Cir. 1987) (stating that although OMB guidelines are not binding on the courts, courts look to the guidelines for guidance and citing case that stated courts defer to the guidelines).

159. See 40 Fed. Reg. at 56,741, 44 Fed. Reg. 23,138 (1979); 47 Fed. Reg. 21,656 (1982); 48 Fed. Reg. 15,556 (1983); 49 Fed. Reg. 12,338 (1984); 50 Fed. Reg. 52,738 (1985); 52 Fed. Reg. 12,990 (1987); 54 Fed. Reg. 25,821 (1989); 58 Fed. Reg. 36,075 (1993); 59 Fed. Reg. 37,914 (1994); 61 Fed. Reg. 6,435 (1996); *Doe v. Chao*, 124 S. Ct. 1204, 1216 (2004) (Ginsburg, J., dissenting).

OMB believed that the Privacy Act requires only proof of a “willful or intentional” violation coupled with an “adverse effect” on an individual for the individual to recover the statutory minimum of \$1,000.¹⁶⁰ Because the OMB’s principal responsibility is to interpret the Privacy Act to guide the agencies, the OMB’s interpretation should be viewed with great significance.¹⁶¹ In fact, prior to *Doe v. Chao*, the majority of circuits adopted the OMB’s interpretation that individuals may recover the statutory minimum damage of \$1,000 after proving an “adverse effect” from the agency’s “intentional or willful” violation of the Privacy Act.¹⁶²

The Privacy Act’s plain language, legislative history, the Commission’s recommendation, the OMB’s interpretation, and the interpretation adopted by a majority of the circuits all clearly pointed to allowing individuals to recover the statutory minimum damage of \$1,000 without requiring proof of actual damages. Then, in February 2004, a divided Supreme Court drastically altered this course.

160. *But see Doe*, 124 S. Ct. at 1216, n. 2 (Ginsburg, J., dissenting). Justice Ginsburg in her dissent noted that the government communicated informally with an unnamed OMB official who stated that the OMB does not believe individuals are allowed the statutory minimum of \$1,000 recovery without sustaining actual damages. *Id.* However, such informal OMB communication “cannot override OMB’s contemporaneous, long-published construction of §552a(g)(4).” *Id.*

161. *Baker*, 814 F.2d at 1383 (9th Cir. 1987) (stating that although the OMB guidelines are not binding on the courts, courts look to the guidelines for guidance and citing case that stated courts defer to the guidelines).

162. *See Orekoya v. Mooney*, 330 F.3d 1, 8 (1st Cir. 2003), *overruled in part by Doe v. Chao*, 124 S. Ct. 1204 (2004) (stating that the majority adopted the OMB’s interpretation and the First Circuit adopts the majority interpretation); *Doe v. Chao*, 306 F.3d 170, 189 (4th Cir. 2002) (Michael, J., dissenting) (stating that the majority interprets no proof of actual damage for the statutory minimum recovery of \$1,000 and citing various cases); *Wilborn v. Dep’t of Health and Human Serv.*, 49 F.3d 597, 603 (9th Cir. 1995), *overruled in part by Doe v. Chao*, 124 S. Ct. 1204 (2004) (holding that plaintiff with no provable damages is allowed the statutory damage of \$1,000); *Quinn v. Stone*, 978 F.2d 126, 131, 135 (3d Cir. 1992) (discussing an adverse effect as a causal standing requirement but omitting proof of actual damages as a requirement to recover damages); *Waters v. Thornburgh*, 888 F.2d 870, 872 (D.C. Cir. 1989), *overruled in part by Doe v. Chao*, 124 S. Ct. 1204 (2004) (stating that plaintiff is “entitled to the greater of \$1,000 or the actual damages sustained” if plaintiff establishes “intentional or willful” violation and “adverse effect” on the plaintiff); *Johnson v. Dep’t of Treasury*, 700 F.2d 971, 977 n.12 (5th Cir. 1983), *overruled in part by Doe v. Chao*, 124 S. Ct. 1204 (2004) (stating that statutory minimum of \$1,000 is obviously recoverable without provable damage); *Fitzpatrick v. IRS*, 665 F.2d 327, 330-31 (11th Cir. 1982), *overruled in part by Doe v. Chao*, 124 S. Ct. 1204 (2004) (stating that plaintiffs that suffered injury with no provable damage could still recover \$1,000); *Parks v. IRS*, 618 F.2d 677, 683 (10th Cir. 1980) (stating that plaintiff states claim for statutory minimum of \$1,000 by showing intentional or willful violation of the Privacy Act and suffered adverse effect). *But see Hudson v. Reno*, 130 F.3d 1193, 1207 (6th Cir. 1997) (stating that plaintiff cannot recover because of failure to show actual damages), *overruled in part by*, *Pollard v. E. I. du Pont de Nemours & Co.*, 532 U.S. 843 (2001).

III. *DOE V. CHAO*: ALTERING THE COURSE

Justice Souter wrote for the majority in the Supreme Court in *Doe v. Chao*,¹⁶³ and Justice Ginsburg wrote the main dissenting opinion, with Justices Stevens and Breyer joining her dissent.¹⁶⁴ The Court's decision marks a fundamental shift in the ability of individuals to recover the statutory minimum damage of \$1,000 under the Privacy Act. The facts of the case are straightforward, and the only issue addressed by the Court is whether a plaintiff must prove actual damages to recover the minimal statutory award of \$1,000.¹⁶⁵

In *Doe v. Chao*, the petitioner, Buck Doe, was one of many individuals who filed for benefits under the Black Lung Benefits Act with the Office of Workers' Compensation Programs (the "Labor Agency").¹⁶⁶ Doe disclosed his social security number in his application form.¹⁶⁷ The Labor Agency used Doe's and other black lung claimants' social security numbers to identify the claims on "multi-captioned" notices of hearings. Because the notices were sent to numerous parties, such as other claimants, other claimants' employers, and other attorneys, the Labor Agency violated the Privacy Act's non-disclosure requirement by releasing Doe's social security number without his permission to third parties.¹⁶⁸ Thereafter, Doe and six other claimants sued the Department of Labor for violation of the Privacy Act.¹⁶⁹ The District Court entered judgment against all plaintiffs, except against Doe.¹⁷⁰ In Doe's case, the District Court granted Doe's motion for summary judgment based on his uncontroverted evidence of emotional distress and awarded him the statutory minimum damage of \$1,000.¹⁷¹

A divided Fourth Circuit panel reversed the summary judgment awarded to Doe.¹⁷² The Fourth Circuit held that a plaintiff must prove actual damages arising from an agency's violation in order to recover the

163. *Doe v. Chao*, 124 S. Ct. 1204, 1206 (2004).

164. *Id.* at 1213 (Ginsburg, J., dissenting).

165. *Id.* at 1206. Both parties agreed that the Department of Labor's violation was "willful or intentional" and that the petitioner suffered an "adverse effect" from the violation. *Id.* at 1213.

166. *Id.* at 1206.

167. *Id.*

168. *Id.*; 5 U.S.C. § 552a(b).

169. *Doe*, 124 S. Ct. at 1206.

170. *Id.* at 1207. The District Court also denied class certification sought by plaintiffs for all claimants since the enactment of the Privacy Act. *Id.* at 1206-07. The Department of Labor stipulated to stop publishing social security numbers of the claimants for future notices, and cross-motions for summary judgments followed. *Id.*

171. *Id.* at 1207.

172. *Doe*, 124 S. Ct. at 1207. The Fourth Circuit also affirmed in part to hold that the Department of Labor should be awarded summary judgment against all plaintiffs. *Id.*

statutory minimum damage of \$1,000.¹⁷³ The Fourth Circuit further found that Doe's conclusory allegations of emotional distress did not rise to a triable issue of fact on proving actual damages.¹⁷⁴ Doe petitioned for review, and the Supreme Court granted certiorari to affirm the Fourth Circuit's decision.¹⁷⁵

Doe took the position that any plaintiff adversely affected by an agency's intentional or willful violation is entitled to the statutory minimum damage of \$1,000.¹⁷⁶ The Department of Labor argued that a plaintiff must also prove some actual damage to recover the statutory minimum.¹⁷⁷ The Supreme Court began the analysis with the text of the applicable Privacy Act provision.¹⁷⁸ Specifically, the Court concentrated on Subsection 552a(g)(4)(A).¹⁷⁹ Section 552a(g)(4) provides:

(g)(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.¹⁸⁰

The Court noted that looking backward from the point of the \$1,000 statutory minimum, the \$1,000 award is limited to the "person entitled to recovery."¹⁸¹ The Court reasoned that "person entitled to recovery" must refer immediately back to the preceding phrase "actual damages sustained" to define the elements necessary for a class of persons eligible for the statutory minimum award of \$1,000.¹⁸² Thus, the Court ruled that a plaintiff must prove: (1) intentional or willful violation; (2) adverse effect on the individual; and (3) actual damages before the

173. *Id.*

174. *Id.*

175. *Id.*

176. *Id.* at 1208.

177. *Doe*, 124 S. Ct. at 1208.

178. *Id.*

179. *Id.*

180. 5 U.S.C. § 552a(g)(4).

181. *Doe*, 124 S. Ct. at 1208.

182. *Id.*

plaintiff can recover the statutory minimum damage of \$1,000.¹⁸³

The majority in the Court also provided additional justification for rejecting Doe's interpretation of the damage provision of the Privacy Act.¹⁸⁴ First, the Court stated that Doe's statutory reading creates tension.¹⁸⁵ The Court reasoned that Doe's interpretation treats the willful or intentional act as the last element necessary to find the government liable.¹⁸⁶ The Court argued that such an interpretation ignores the fact that liability is qualified by enumerated damages.¹⁸⁷

Second, the majority pointed out that Doe's position contradicts traditional tort recovery, which requires a wrongful act, causation, and proof of some harm.¹⁸⁸ The Court conceded that the Privacy Act's claim may be more analogous to privacy torts, which presumes "general damages."¹⁸⁹ However, the Court observed that although Congress included a "general damage" provision in earlier drafts of the privacy bill, Congress deleted the provision in the final bill.¹⁹⁰ Therefore, the Court concluded that the deliberate elimination precludes awarding presumed damages and compels interpretation of "person entitled to recovery" to include the requirement of proof of "actual damages."¹⁹¹

Justice Ginsburg disagreed with the Court's reasoning.¹⁹² After

183. *Id.* at 1208, 1212.

184. *Id.* at 1208-10.

185. *Id.* at 1208-09.

186. *Id.* at 1209.

187. *Doe*, 124 S. Ct. at 1209. The Court later also noted that Doe's interpretation would leave a conditional guarantee with no purpose in the statute. *Id.* at 1210.

188. *Id.* at 1209.

189. *Id.*

190. *Id.* at 1209-10.

191. *Doe*, 124 S. Ct. at 1209-10. The Court also addressed three other issues raised by Doe. *Id.* at 1210. First, the Court disregarded Doe's argument that it is illogical for a victim who suffered an adverse effect from an intentional or willful violation of an agency without also suffering actual damages. *Id.* Because the "adverse effect" serves to identify a plaintiff who satisfies the causation and standing requirements, the Court posited that it is possible to have only enough injury to bring an action without actual damages. *Id.* at 1211. Doe also raised the oddity in guaranteeing a minimal presumed damage to plaintiffs who can prove some actual damages. *Doe*, 124 S. Ct. at 1211. The Court responded that such a requirement is not peculiar because such a remedial scheme already exists for defamation torts; plaintiffs in certain defamation suits could only recover presumed damages by proving some pecuniary loss. *Id.* Lastly, Doe pointed out two other statutes with remedial provisions similar to the Privacy Act that support his interpretation of the Privacy Act. *Id.* at 1212. The Court discounted analogies to one of the statutes because of the lack of the phrasing "entitled to recovery." *Id.* Furthermore, the Court refused to review the legislative history of the statutes citing the unreliability of the subsequent legislative history outside of the statute at issue. *Id.*

192. *Doe*, 124 S. Ct. at 1213-21 (Ginsburg, J., dissenting). Justice Stevens and Justice Breyer joined Justice Ginsburg's dissent. *Id.* at 1213. Justice Breyer also wrote a short, separate dissent, to emphasize that Justice Ginsburg's interpretation would not increase the government's exposure to

reviewing the statutory construct of the civil remedy provision, Justice Ginsburg argued that the Court should have adopted the prevailing interpretation that individuals are not required to prove actual damages to recover the statutory minimum damage of \$1,000.¹⁹³ Justice Ginsburg advanced several reasons for rejecting the majority's interpretation.¹⁹⁴

First, Justice Ginsburg argued that the plain language of the statute does not support the Court's interpretation.¹⁹⁵ Justice Ginsburg pointed out that proper construction of the statute requires a review of the placement of terms in the statute.¹⁹⁶ The terms "actual damages" and "person entitled to relief" appear in the text after conditions necessary to find agency's liability.¹⁹⁷ Justice Ginsburg explained that if Congress intended individuals to prove actual damages to recover the statutory minimum damage of \$1,000, the statute would have been written to include "in no case shall a person who proves such damages . . . receive less than \$1,000."¹⁹⁸ Moreover, Justice Ginsburg criticized the majority's statutory interpretation because it left several terms superfluous and failed to give effect to every word and clause.¹⁹⁹ Justice Ginsburg gave examples to illustrate her criticism.²⁰⁰ She argued that the majority's interpretation would render the term "shall be liable" to "may be liable," and the "adverse effect" element would be eliminated by the majority's requirement that a plaintiff must prove "actual damages" in order to recover the statutory minimum.²⁰¹ Additionally, Justice Ginsburg pointed out that the prevailing view of the court of appeals and the OMB's interpretation support the interpretation that the \$1,000 recovery is independent from proof of actual damages.²⁰²

Additionally, Justice Ginsburg argued that the purpose and legislative history of the Privacy Act support her interpretation.²⁰³ Because Privacy Act violations often result in emotional harm only, Justice Ginsburg argued that Congress intended individuals to recover for "any damages."²⁰⁴ Thus, Justice Ginsburg reasoned that the \$1,000

liability. *Id.* at 1221 (Breyer, J., dissenting).

193. *Id.* at 1215 (Ginsburg, J., dissenting).

194. *See id.* at 1213-21.

195. *Id.* at 1213.

196. *Doe*, 124 S. Ct. at 1213.

197. *Id.* at 1214.

198. *Id.*

199. *Id.* at 1214-15.

200. *Id.*

201. *Id.* at 1215.

202. *Doe*, 124 S. Ct. at 1215-16.

203. *Id.* at 1216.

204. *Id.*

statutory damage award was meant to give individuals incentives to enforce the Privacy Act by allowing recovery for “non-pocketbook harm.”²⁰⁵

IV. ANALYSIS OF *DOE V. CHAO*

The Supreme Court’s narrow construction of the Privacy Act will force individuals to overcome unrealistic hurdles. The majority contorted the statute and the legislative history to reach a result that restricts individuals from effectively enforcing the Privacy Act.²⁰⁶ On the other hand, the dissent’s straightforward statutory construction is consistent with the purpose of the Privacy Act.²⁰⁷ The Court’s restrictive interpretation is especially disturbing because the Court, in effect, held that individuals have no remedy for the government’s unlawful disclosure of a person’s social security number.²⁰⁸ But if individuals have no effective remedy, who will enforce the Privacy Act? Historically, the government has proven itself to be a poor enforcer of the Privacy Act.²⁰⁹ Thus, the Court’s ruling in *Doe v. Chao* decimates the likelihood of future enforcement of the Privacy Act.

A. Statutory Interpretation and Legislative History Support the Dissent’s Interpretation

The interpretation of the damage section of the Privacy Act begins with the plain language of the statute itself.²¹⁰ Therefore, we begin with an analysis of the plain language of the statute and the Court’s

205. *Doe*, 124 S. Ct. at 1218-19. Justice Ginsburg also observed that fears of exposing the government to disproportionate liability never materialized in nearly 30 years of the enforcement of the Privacy Act. *Id.* at 1217-18. Justice Ginsburg also criticized the majority’s interpretation because it forces individuals to manufacture provable, albeit small, actual damages such as a \$10 fee paid to obtain a credit report. *Id.* at 1217. Finally, Justice Ginsburg argued that other privacy statutes include similar civil remedy provisions and have been interpreted to allow the statutory minimum recovery without proving actual damages. *Id.* at 1219-20.

206. *See Doe*, 124 S. Ct. at 1206-12.

207. *See id.* at 1213-21 (Ginsburg, J., dissenting).

208. *See id.* at 1206-07 (discussing how *Doe* brought an action for an agency’s disclosure of his social security number to third parties without his permission and how *Doe* must prove actual damages before recovering the \$1,000 statutory minimum); *see also supra* notes 166-191 and accompanying text.

209. *See infra* notes 242-267 and accompanying text (discussing how the government fails to protect privacy and the lack of incentives for the government to protect privacy).

210. *See Ardestani v. Immigration and Naturalization Serv.*, 502 U.S. 129, 135 (1991) (stating that the actual language of the statute is the starting point in statutory interpretation); *Kaiser Aluminum & Chem. Corp. v. Bonjorno et al.*, 494 U.S. 827, 835 (1990) (stating same).

interpretation of the damages provision.²¹¹ The applicable Section 552a(g)(4) states as follows:

(g)(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.²¹²

The Court clearly wanted to support the Department of Labor's interpretation and twisted a straightforward statutory construction in order to do so. The majority achieved its result by starting from the last clause of Subsection 552a(g)(4)(A) and stressing the importance of linking "entitled to recovery" to the immediately preceding clause of "actual damages sustained."²¹³ The most natural way to read a statute, however, is to start from the beginning of the statute and to place all the words in their context.²¹⁴ If the Court interpreted Section 552a(g)(4) from the beginning, the Court would see that Section 552a(g)(4) ends with the clause "the United States shall be liable to the individual in an amount equal to the sum of" before the provision separates into Subsections (A) and (B).²¹⁵ The most natural interpretation of this clause is that the clause preceding "shall be liable" defines conditions in which the government may be found liable. Naturally, one would also expect to read the measure of damages following the clause "shall be liable . . . in an amount equal to the sum of." As expected, following this clause, the provision starts two new Subsections, (A) and (B), that

211. See *Doe*, 124 S. Ct. at 1208.

212. 5 U.S.C. § 552a(g)(4).

213. *Doe*, 124 S. Ct. at 1208; see also *supra* notes 181-183 and accompanying text.

214. See generally *Nat'l Labor Relations Bd. v. Ky. River Cmty. Care, Inc.*, 532 U.S. 706 (2001) (analyzing statutory interpretation by reviewing the structure of the National Labor Relations Act); *Davis v. Mich. Dep't of Treasury*, 489 U.S. 803, 809 (1989) (stating that language in a statute must be read in context and in place of the overall statutory scheme).

215. 5 U.S.C. § 552a(g)(4). The Section begins as follows:

(g)(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

Id.

define measure of damages—actual and statutory minimal damages in Subsection (A) and the costs of action and reasonable attorney fees in Subsection (B).²¹⁶

In particular, Subsection (A) provides recovery for actual damages, “but in no case shall a person entitled to recovery receive less than the sum of \$1,000.”²¹⁷ Because Subsection (A) is most naturally read only as a clause for the measure of damage in the overall statutory scheme of Section 552a(g)(4), the clause in Subsection (A) should be interpreted to allow either (1) actual damages, or if actual damages are diminutive or non-existent, (2) \$1,000. By stressing the importance of the “entitled to recovery” clause more than the overall statutory scheme, the majority neglected the “shall be liable” clause that signals the beginning of the measure of damages Subsections. In fact, as Justice Ginsburg cogently articulated in her dissent, the majority’s interpretation alters the words “shall be liable” effectively into “may be liable.”²¹⁸

More importantly, the majority completely failed to focus on the appropriate legislative history regarding the statutory minimum damage of \$1,000.²¹⁹ In reviewing the legislative history, the majority emphasized the elimination of the presumed “general damages” provision.²²⁰ Instead, the majority should have addressed the significance of the inclusion of the \$1,000 damage amount as a compromise provision to the various provisions submitted by the Senate and the House.²²¹ As the majority accurately observed, the previous Senate version of the remedy provision included both “actual” and “general” damages but deleted the “general damages” in the final privacy bill.²²² However, the deletion of the “general damages” provision is not relevant for purposes of construing whether the \$1,000

216. *Id.* § 552a(g)(4). Subsections 552a(g)(4)(A) and (B) are as follows:

(g)(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

Id.

217. *Id.* § 552(a)(g)(4)(A).

218. *Doe*, 124 S. Ct. at 1215 (Ginsburg, J., dissenting).

219. *See id.* at 1208.

220. *Id.* at 1209-10.

221. *Id.*

222. *Id.* at 1210; S. 3418, 93d Cong., 2d Sess. (as amended November 21, 1974), reprinted in SOURCEBOOK, *supra* note 7, at 371; *see also supra* notes 123-125 and accompanying text.

statutory damage award requires proof of actual damages. The relevant drafting and legislative history are how the \$1,000 statutory minimum provision was included in the Privacy Act.²²³ The original version proposed by the Senate did not include the \$1,000 statutory minimum language.²²⁴ In amending the Senate's original version, the Senate included the \$1,000 statutory minimum language which ultimately survived and was incorporated into the Privacy Act.²²⁵ What the majority overlooked is that the Senate had included the \$1,000 statutory minimum language as a liquidated damage provision when amending the original Senate version of the privacy bill.²²⁶ No legislative history exists to dispute that this is not a liquidated damage provision in the current Privacy Act.

Congress typically does not require proof of actual damages for plaintiffs to recover statutory liquidated damages.²²⁷ This is because a liquidated damage provision traditionally exists to specifically address the uncertainty and difficulty involved in proving actual damages.²²⁸ A liquidated damage provision is especially useful when real but intangible damages arise from violations.²²⁹ Because of the difficulty in assessing actual damages, a liquidated damages provision removes uncertainty by fixing a reasonable monetary sum.²³⁰ In other words, plaintiffs only need to prove that a breach or violation occurred, and proof of actual damages is unnecessary to recover liquidated damages.²³¹

223. See *Doe*, 124 S. Ct. at 1209-10.

224. See *supra* note 122 and accompanying text.

225. *Doe*, 124 S. Ct. at 1209-10; S. 3418, 93d Cong., 2d Sess. (as amended November 21, 1974), reprinted in SOURCEBOOK, *supra* note 7, at 371.

226. 120 CONG. REC. 36,891 (1974), reprinted in SOURCEBOOK, *supra* note 7, at 768; see also *supra* note 125 and accompanying text. The Senate explained the inclusion of \$1,000 provision in its amended bill to allow "an individual . . . to recover . . . for liquidated damages of say \$1,000 into the assessed against the agency for a violation of the Act." 120 CONG. REC. 36,891 (1974), reprinted in SOURCEBOOK, *supra* note 7, at 768.

227. See e.g. *Perrone v. Gen. Motors Acceptance Corp.*, 232 F.3d 433, 436 (5th Cir. 2000). In interpreting the actual damage provision of the Consumer Leasing Act, the Fifth Circuit stated that statutory damage provision of the Consumer Leasing Act was meant to encourage private enforcement when no actual damages exist. *Id.* Additionally, statutory damages complement actual damage provision in the Consumer Leasing Act because statutory damages exist for cases where violations are small or difficult to ascertain. *Id.* See also Jeff Sovern, *The Jewel of Their Souls; Preventing Identity Theft Through Loss Allocation Rules*, 64 U. PITT L. REV. 343, 385 (2003) (stating that Fair Debt Collection Practices Act provides for statutory damages of up to \$1,000 when consumers cannot establish actual damages).

228. ELAINE W. SHOBEN ET AL., REMEDIES 398-99 (3d ed. 2002).

229. DAN B. DOBBS, HANDBOOK ON THE LAW OF REMEDIES § 12.5, at 821 (1973).

230. SHOBEN, *supra* note 228, at 398.

231. See *McCarthy v. Tally*, 297 P.2d 981, 987 (Cal. 1956) (stating that plaintiffs only need to prove damage would have been difficult to ascertain at time of contract, agreed sum for damages

Thus, because Congress intended the Privacy Act's civil remedy provision of \$1,000 to be a liquidated damage provision,²³² Congress never intended individuals to prove actual damages in order to recover the \$1,000 statutory minimum. Unfortunately, the majority missed the significance of the liquidated damage provision by focusing instead on the issue of presumed general damages.²³³ As a consequence, the Court obliterated the liquidated damage mechanism of the Privacy Act and established a statutory interpretation that will cause enforcement problems.

B. Effect of the Doe v. Chao Decision

Doe v. Chao effectively dismantled the private enforcement mechanism of the Privacy Act. As it stands, the private enforcement rate of the Privacy Act is already extremely low. For the past 30 years, individuals have brought very few civil actions against government agencies.²³⁴ Without transparency of the government's activities, individuals are simply unaware of their privacy rights and the existence of records kept by government agencies.²³⁵ Even if individuals were to bring lawsuits, plaintiffs must prove two required elements for recovery, an "intentional and willful" level of culpability and an "adverse effect" suffered by the individual.²³⁶ Courts have already construed both terms restrictively, creating barriers to recovery and discouraging individuals from bringing enforcement actions under the Privacy Act.²³⁷ By requiring proof of actual damages to recover the \$1,000 statutory minimum, the Supreme Court raised the barriers created by lower courts

was reasonable, and that breach occurred). The California Supreme Court held that actual damage is not necessary to recover liquidated damage. *Id.* But see DOBBS, *supra* note 229, at 822 (noting that some cases held that plaintiffs must prove some actual damages but such cases are in the minority).

232. See *supra* note 226 and accompanying text.

233. See *Doe*, 124 S. Ct. at 1209-11.

234. See OFFICE OF INFORMATION AND PRIVACY, U.S. DEPARTMENT OF JUSTICE, FREEDOM OF INFORMATION CASE LIST 321-91 (1998) [hereinafter CASE LIST] (listing cases brought under the Privacy Act as of 1998); OFFICE OF MANAGEMENT AND BUDGET, FIFTH ANNUAL REPORT OF THE PRESIDENT ON THE IMPLEMENTATION OF THE PRIVACY ACT OF 1974 14 (1979) [hereinafter 1979 PRESIDENT REPORT] (stating that through 1978, only a few privacy litigations arose with approximately 40 suits being filed each year, and that in 1979 the number of cases increased to 123); LODGE, *supra* note 78, at 633 n.132 (stating how the Department of Justice identified only 60 reported cases brought under the Privacy Act that included damage claims as of 1983).

235. 1979 PRESIDENT REPORT, *supra* note 234, at 10.

236. *Doe*, 124 S.Ct. at 1219 n.5 (Ginsburg, J., dissenting), *id.* at 1221 (Breyer, J., dissenting); Lodge, *supra* note 78, at 632-33.

237. *Doe*, 124 S.Ct. at 1219 n.5 (Ginsburg, J., dissenting), *id.* at 1221 (Breyer, J., dissenting); Lodge, *supra* note 78, at 633.

to a formidable height, and in all likelihood, killed all enforcement incentives.

C. Need for Enforcement of the Privacy Act

Congress included the civil remedy provision to encourage private enforcement of the Privacy Act.²³⁸ Recognizing that federal agencies have little incentives to enforce the Privacy Act,²³⁹ Congress intended to provide incentives for the “widest possible citizen enforcement.”²⁴⁰ The values of privacy traditionally included avoiding embarrassment, building intimacy, avoiding misuse, and encouraging innovation.²⁴¹ Today, individuals need even more privacy protection of information to protect valuable information such as an individual’s identity. To do so, there must be a mechanism to enable the enforcement of the Privacy Act to guarantee such protection. Unfortunately, *Doe v. Chao* effectively eradicates this mechanism for enforcement and has dealt a significant blow to the protection of private information in our society.

1. Lack of Incentives to Protect Privacy and Privacy Violations

Our government, the largest collector of information, generally does not protect personal privacy and makes little efforts to follow the requirements of the Privacy Act.²⁴²

In 1993, the U.S. General Accounting Office (the “GAO”) found that the FBI’s own audit revealed repeated misuse of the agency’s largest internal database, the National Crime Information Center.²⁴³ The GAO reported inconsistent compliance with the Privacy Act by government agencies, finding a compliance rate ranging from 100 percent for some requirements to 70 percent for others.²⁴⁴ Additionally,

238. 120 CONG. REC. 36,892 (1974) (remarks of Sen. Ervin), *reprinted in* SOURCEBOOK, *supra* note 7, at 772; *id.* at 36,644 (remarks of Rep. Moorhead), *reprinted in* SOURCEBOOK, *supra* note 7, at 884.

239. *Id.* at 36,645 (remarks of Rep. Abzug), *reprinted in* SOURCEBOOK, *supra* note 7, at 887.

240. S. REP. NO. 93-1183, *supra* note 7, at 83, *reprinted in* SOURCEBOOK, *supra* note 7, at 236.

241. Kang, *supra* note 38, at 1212-14 (listing purposes and values of privacy as “avoiding embarrassment,” “constructing intimacy,” and “averting misuse”); Jay Weiser, *Measure of Damages for Violation of Property Rules: Breach of Confidentiality*, 9 U. CHI. L. SCH. ROUNDTABLE 75, 82 (2002) (discussing how privacy allows experimentation leading to new social developments).

242. Chlapowski, *supra* note 71, at 133-34.

243. Glenn R. Simpson, *Big Brother-in-Law: If the FBI Hopes to Get the Goods on You, It May Ask ChoicePoint*, WALL ST. J., Apr. 13, 2001, at A1.

244. UNITED STATES GENERAL ACCOUNTING OFFICE, PRIVACY ACT: OMB LEADERSHIP NEEDED TO IMPROVE AGENCY COMPLIANCE, GAO-03-304 at 14 (2003) [hereinafter GAO-03-304].

today, where 70 percent of the agencies' records contain electronic records²⁴⁵ and cybercrimes are expected to increase,²⁴⁶ the government's computer-security efforts are so dismal that the House recently gave a "D-minus" grade.²⁴⁷

It is no wonder that the government fails to vigilantly protect our privacy rights. The OMB, the only central agency empowered by Congress to oversee implementation of the Privacy Act, devotes little resources and assigns low priority to Privacy Act compliance.²⁴⁸ Because of the OMB's lack of strong oversight, agencies in turn assign a low priority to Privacy Act compliance.²⁴⁹ Additionally, agencies maintaining public records view their primary responsibility in maintaining the integrity of records, not in protecting the privacy of individuals.²⁵⁰ Thus, if an agency maintaining public records receives documents with an individual's social security number, the agency simply allows the entire document, with the social security number, to be available for public viewing.²⁵¹ In sum, government agencies fail to protect personal privacy because they have no incentives to protect privacy, and no strong centralized enforcement agent exists to compel agencies to protect our privacy rights.²⁵²

The government's lax attitude toward safeguarding individuals' right to privacy in personal information is especially disturbing today because the government collects voluminous amounts of personal information.²⁵³ In some instances, an agency maintains information on as many as 290 million people.²⁵⁴ For such a large number of people,

245. GAO-03-304, *supra* note 244, at 13.

246. See generally Thomas Fedorek, *Computers + Connectivity = New Opportunities for Criminals and Delimmas for Investigators*, 76 N.Y. ST. B.J. 10 (Feb. 2004) (discussing how the connectivity of computers create new opportunities for criminals, describing new types of cybercrimes, and predicting an increase in certain types of cybercrimes).

247. Simpson, *supra* note 243, at A1. See also GAO-02-352, *supra* note 1, at 29-30 (reporting significant information security weaknesses and that federal agencies lack information security programs required by legislation).

248. GAO-03-304, *supra* note 244, at 26; Lynn Chuang Kramer, Comment, *Private Eyes Are Watching You: Consumer Online Privacy Protection—Lessons From Home and Abroad*, 37 TEX. INT'L L.J. 387, 414 (2002) (stating that the Office of Management and Budget had little interest in issuing guidelines on the Privacy Act).

249. GAO-03-304, *supra* note 244, at 26.

250. GAO-02-352, *supra* note 1, at 38.

251. *Id.*

252. Kramer, *supra* note 248, at 414.

253. UNITED STATES GENERAL ACCOUNTING OFFICE, INFORMATION MANAGEMENT: SELECTED AGENCIES' HANDLING OF PERSONAL INFORMATION, GAO-02-1058 at 17 (2002) [hereinafter GAO-02-1058].

254. GAO-03-304, *supra* note 244, at 13. The median number of people maintained in the system of records is about 3,500, but the number ranges from 5 people to 290 million people. *Id.*

agencies collect (1) personal identifying information such as a social security number, the name, phone number, driver's license number, address, and even e-mail address of an individual and (2) other non-identifying information such as an individual's birth date, physical description, occupation, net worth, criminal record, credit history, and salary.²⁵⁵ Of the information collected, agencies most often use the social security number to retrieve personal information²⁵⁶ because of the widespread use of the social security number as an accurate and reliable identifier for individuals.²⁵⁷

The combination of the colossal amount of personal information and the lack of incentives to protect individuals' privacy is causing abuse and violations of our right to privacy by the government. In some instances, the government intentionally violates the right to privacy to profit from the sale of individuals' personal information.²⁵⁸ For example, the United States Postal Service regularly sells information obtained from "change of address cards" to private companies, including credit reporting agencies and direct selling marketers.²⁵⁹ In other instances, government agencies simply share information with private

255. GAO-02-1058, *supra* note 253, at 19. Agencies collect enormous amounts of personal information about an individual, his or her spouse, children, dependents, and parents. *Id.* The GAO, in its 2002 report, identified three types of information collected by certain agencies: personal identifiers, demographic data, and financial/legal data. *Id.* The personal identifier information includes the legal name, maiden name, aliases, home phone number, business phone number, social security number, driver's license number, alien registration number, legal address, and e-mail address of an individual. *Id.* Demographic data includes the date of birth, place of birth, citizenship, marital status, date of marriage/divorce, number in household, education level, occupation, gender, and physical attributes such as height and eye color of an individual. *Id.* Financial/legal data includes the salary, investments, net worth, credit history, child support, bankruptcy, criminal record, drug convictions, and litigations of an individual. *Id.*

256. GAO-03-304, *supra* note 242, at 13. Social security numbers are used for tax identification, employment records, law enforcement records, court records, driver records, child support records, professional licenses, student loans, and other uses such as veteran benefits. Flavio L. Komuves, *We've Got Your Number: An Overview of Legislation and Decisions to Control the Use of Social Security Numbers as Personal Identifiers*, 16 J. MARSHALL J. COMPUTER & INFO. L. 529, 540-49 (1998).

257. GAO-02-352, *supra* note 1, at 6. President Franklin D. Roosevelt issued an Executive Order in 1943 that required all federal agencies to use social security numbers exclusively to identify individuals. *Id.* Thereafter, federal agencies and private entities dramatically increased their reliance on social security numbers as the primary identifying number for individuals. *Id.*

258. Mark E. Budnitz, *Privacy Protection for Consumer Transactions in Electronic Commerce: Why Self-Regulation is Inadequate*, 49 S.C. L. REV. 847, 855 (1998) (discussing government violations of the right to privacy).

259. Budnitz, *supra* note 256, at 855-56 (stating that United States Postal Service receives \$80,000 per year for the sale of information from change of address cards). State governments also sell information to raise revenue for the states. *See id.* at 855. For example, Illinois receives \$10 million annually from the sale of public records. *Id.*

companies without realizing that such actions are in violation of the Privacy Act. For example, the state of Hawaii contracted a private company to issue speeding tickets using traffic cameras.²⁶⁰ To issue speeding tickets, however, Hawaiian state and city agencies gave the private company access to individuals' driver's license numbers, which also happen to be the individuals' social security numbers.²⁶¹ The access constituted a violation of the Privacy Act because agencies must disclose all intended uses of the social security numbers to individuals at the time agencies obtain the information from the individuals.²⁶² At other times, government agencies intentionally take actions that violate the spirit of the Privacy Act, but are not technically violations of the Privacy Act.²⁶³ For example, the FBI, IRS, and numerous federal agencies currently purchase millions of dollars worth of personal data from private companies that provide commercial look-up services.²⁶⁴ These commercial companies specialize in what government agencies cannot do — glean, sort, and organize data on individuals to compile a master information file.²⁶⁵ By indexing and matching information from various sources, private companies collect credit information, names, aliases, addresses, motor-vehicle information, real property records, traffic records, bankruptcy filings, and other information under an individual's social security number.²⁶⁶ Although Congress enacted the Privacy Act to prevent federal agencies from gathering data irrelevant for agencies' purposes, federal agencies circumvent the Privacy Act by employing private companies to gather extraneous data.²⁶⁷

2. Government's Privacy Violation: An Invitation for Identity Theft

Today, where information is a valuable commodity, government

260. Mike Leidemann, *Lawsuit Targets Camera Tickets*, HONOLULU ADVERT., April 3, 2002, available at 2002 WL 24193802; *ACLU Sues State Over Traffic Camera Vans for Violating Privacy Laws*, A.P. Wires, April 2, 2002 [hereinafter AP WIRE 2002].

261. Leidemann, *supra* note 258; AP WIRE 2002, *supra* note 258.

262. The Privacy Act of 1974, Pub. L. No. 93-579, § 7, 88 Stat 1896 (1974); Leidemann, *supra* note 258.

263. Glenn R. Simpson, *U.S. Agencies Tap Outside Data Source*, WALL ST. J., April 13, 2001, at A1, available at 2001 WL-WSJ 2860297 (discussing government agencies' intentional actions which violate the Privacy Act).

264. Simpson, *supra* note 261, at A1. The Justice Department paid \$8,000,000 to buy data from ChoicePoint in 2000, and the IRS signed a multiyear contract worth up to \$12,000,000 with ChoicePoint. *Id.* ChoicePoint alone has at least 35 federal agencies as customers. *Id.*

265. *Id.*

266. *Id.*

267. *Id.*

agencies' violation of the Privacy Act, especially the unlawful disclosure of social security numbers, will increase social and economic harm to individuals.²⁶⁸ Like it or not, the social security number is the universal identifier for individuals.²⁶⁹ Because of the widespread use of the social security number as an identifier by the government and private companies, individuals' complete financial, medical, credit, and other vital information is linked to the social security number.²⁷⁰ Not surprisingly, the social security number is also the key information stolen and used by identity thieves to commit identity theft.²⁷¹

Identity theft is rising each year,²⁷² and the total cost associated with identity theft reported in year 2002 alone is staggering — approximately \$47.6 billion to businesses and \$5.0 billion to individuals.²⁷³ However, of the approximately 27 million Americans affected by identity theft during the period of 1998-2003,²⁷⁴ most victims did not incur out-of-pocket losses.²⁷⁵ Instead, most victims suffered significant non-monetary harm. Victims generally attribute a significant loss of time spent on resolving problems caused by identity theft as the most common non-monetary harm, with figures ranging anywhere from an average of 30 hours to 600 hours.²⁷⁶ Problems range from bounced

268. Mell, *supra* note 20, at 12-13 (stating that information has become a valuable commodity instead of ancillary resource).

269. See Daniel J. Solove, *Identity Theft, Privacy, and the Architecture of Vulnerability*, 54 HASTINGS L.J. 1227, 1253 (2003) (stating that the social security number is a de facto identifier).

270. GAO-02-352, *supra* note 1, at 3-8; Solove, *supra* note 267, at 1252-54.

271. GAO-02-352, *supra* note 1, at 9; Solove, *supra* note 267, at 1252. With the social security number, a person can “open and close accounts, change addresses, obtain loans, access personal information, make financial transactions, and more.” Solove, *supra* note 267, at 1253.

272. See CONSUMER SENTINEL, IDENTITY THEFT DATA CLEARINGHOUSE, FEDERAL TRADE COMM'N, NATIONAL AND STATE TRENDS IN FRAUD & IDENTITY THEFT: JANUARY – DECEMBER 2003 3-4 (2004) (stating that complaints received by Federal Trade Commission (“FTC”) increased from 2002) [hereinafter FTC 2004 REPORT]; Synovate, Federal Trade Comm'n, Federal Trade Commission – Identity Theft Survey Report 18 (2003) (stating that identity theft crimes are on the rise, and identity theft report increased 41% from 2002) [hereinafter FTC 2003 SURVEY]; UNITED STATES GENERAL ACCOUNTING OFFICE, IDENTITY THEFT: PREVALENCE AND COST APPEAR TO BE GROWING, GAO-02-363 at 4 (2002) (indicating increase in identity theft alerts received by consumer reporting agencies) [hereinafter GAO-02-363].

273. FTC 2003 SURVEY, *supra* note 270, at 7.

274. *Id.* at 12.

275. *Id.* at 43. Approximately 63% of the victims incurred no monetary losses. *Id.*

276. LINDA & JAY FOLEY, IDENTITY THEFT RESOURCE CENTER, IDENTITY THEFT: THE AFTERMATH 2003, A COMPREHENSIVE STUDY TO UNDERSTAND THE IMPACT OF IDENTITY THEFT ON KNOWN VICTIMS 24 (2003), available at <http://www.idtheftcenter.org/idaftermath.pdf> (last visited Oct. 10, 2004) [hereinafter ID RESOURCE 2003 STUDY]; FTC 2003 SURVEY, *supra* note 270, at 7. The figures on the number of hours spent by victims vary by reports and surveys. The FTC reported victims spent approximately 297 million total hours, with an average of 30 hours per victim in 2002. FTC 2003 SURVEY, *supra* note 270, at 7. The Identity Theft Resource Center

checks, loan denials, credit card application rejections, debt collection harassment, insurance rejections, and the shut down of utilities.²⁷⁷ Victims can also be mistaken as the subject of civil lawsuits or criminal investigations, arrests, or convictions.²⁷⁸ Given the severity of these non-monetary problems, victims are clearly justified in feeling personally violated and suffering from severe emotional distress.²⁷⁹ In fact, such non-monetary harm, although difficult to quantify, may cause more damage to identity theft victims than quantifiable monetary loss.²⁸⁰ Unfortunately, identity theft will likely increase over the years with the growth of online technologies²⁸¹ because a majority of government agencies use electronic records containing the social security number.²⁸² Such records are generally stored and processed in computers that are linked to other computers.²⁸³

The government's illegal or careless disclosure of the social security number to third parties, for any reason, is similar to leaving one's front door wide open – inviting thieves to steal. Because of limited resources and the difficulty in tracing identity thieves, law enforcement rarely catches identity thieves.²⁸⁴ This problem is compounded because most identity theft victims do not find out that their identities have been stolen until long after the theft has begun.²⁸⁵

surveyed a group of known identity theft victims and found victims spent an average of 600 hours. ID RESOURCE 2003 STUDY at 24.

277. GAO-02-363, *supra* note 270, at 9; FTC 2003 SURVEY, *supra* note 270, at 47-48.

278. GAO-02-363, *supra* note 270, at 9; FTC 2003 SURVEY, *supra* note 270, at 47-48.

279. See GAO-02-363, *supra* note 270, at 9 (stating that victims often feel “personally violated” and may potentially suffer severe emotional harm).

280. See ID RESOURCE 2003 STUDY, *supra* note 274, at 35 (stating that victim's sense of frustration, anger, insecurity, and helplessness linger over time and such psychological impacts may have far worse consequences for victims than financial costs).

281. GAO-02-363, *supra* note 270, at 13; Harry A. Valetk, *Mastering the Dark Arts of Cyberspace: A Quest for Sound Internet Safety Policies*, 2004 STAN. TECH. L. REV. 2, 11 (2004).

282. GAO-02-352, *supra* note 1, at 27 (stating how 90 percent of the surveyed agencies use both hard and electronic records containing the social security numbers to conduct activities, and that many employ computers linked to computer networks when using electronic records).

283. *Id.*

284. See UNITED STATES GENERAL ACCOUNTING OFFICE, IDENTITY THEFT: GREATER AWARENESS AND USE OF EXISTING DATA ARE NEEDED, GAO-02-766 17-18 (2002) (finding that law enforcement agencies have insufficient resources to investigate and prosecute and that identity theft cases often end without an arrest) [hereinafter GAO-02-766]. It also does not help that because of longer than usual efforts needed to solve identity theft crimes and relatively minimal punishment even if successful, law enforcements have no incentives to vigorously pursue identity theft crimes. *Id.* One survey found that the chance of catching an identity thief is only one in 700. *How Many Identity Theft Victims Are There? What IS the Impact on Victims?*, Privacy Rights Clearinghouse (2003), available at <http://www.privacyrights.org/ar/idthefts-surveys.htm> (posted September 8, 2003 and last visited May 8, 2004).

285. Solove, *supra* note 267, at 1248. Victims usually learn of the identity theft about one year

Thus, at the present time, safeguarding the social security number and other identifying information to prevent identity theft is more effective than relying on law enforcement to catch identity thieves. Therefore, government agencies must take stringent proactive measures, now more than ever, to protect the privacy of individuals' personal information.

3. The Importance of Private Enforcement of the Privacy Act

To do so, government agencies should follow the Privacy Act and the guidelines of the Privacy Act more vigorously. Unfortunately, given the government's lack of incentives and the low priority on protecting the right of privacy, the Privacy Act is only effective if government agencies are compelled to follow it. To prevent substantial harm, such as identity theft, individuals must be able to bring actions to enforce the government's protection of individuals' informational privacy before substantial damages arise. By swiftly bringing actions when illegal disclosures initially occur and forcing the government to pay the statutory minimum damage amount, individuals can compel government agencies to protect privacy more effectively and proactively.

Individuals are appropriate enforcers of the Privacy Act because individuals have more at stake. As discussed above, if the government fails to comply with the Privacy Act, individuals, not the government, suffer the consequence. Thus, it makes sense to give incentives for individuals to shoulder the responsibility of monitoring government activities and in bringing actions against the government to enforce the Privacy Act. With the *Doe v. Chao* decision, however, individuals have little to no incentive to bring actions to compel government agencies to follow the Privacy Act before individuals incur substantial harm. With no incentives to bring actions, the private enforcement mechanism of the Privacy Act is effectively eliminated.

D. Legislative Recommendation

Congress must once again act to ensure the protection of individuals' privacy by giving incentives for individuals to bring civil actions against the government. At a minimum, Congress should amend the civil damages provision to clarify that individuals need not prove actual damages to recover the statutory minimum damage. For private enforcement to be truly effective, however, Congress should amend the damages provision to do more.

Congress feared exorbitant costs and liability stemming from the enforcement of the Privacy Act, but such fears never materialized.²⁸⁶ Before the Privacy Act passed, the OMB estimated a total of \$300-\$400 million to implement the Privacy Act in 1974.²⁸⁷ The actual cost of implementation in the first year proved to be substantially less – approximately \$66 million.²⁸⁸ Additionally, the private enforcement rate for the last 30 years has been low.²⁸⁹ Given the significant consequences that can arise from violations under the Privacy Act and the relatively low liability incurred by the government to date, Congress should increase the amount of recoverable damages.

Congress should increase the measure of damages in three ways. First, the minimum statutory liquidated damages should be increased from \$1,000 to \$10,000. The increased statutory minimum damage amount is substantial enough to deter the government from violating the right to privacy and to encourage individuals to monitor and sue the government for violations of the Privacy Act. Second, the damage provision should include presumed general damages. The presumed general damage doctrine, an exception in tort law, has been justified in areas of law when certainty of injury and difficulty of proving such injury exist.²⁹⁰ Emotional damages individuals suffer and the difficulty of proving such injury from the government's privacy violation certainly justify inclusion of presumed general damages in the damages provision of the Privacy Act. Lastly, Congress should add a punitive damages provision for repeated or continued violations by agencies to encourage the government to immediately rectify violations. The punitive damage provision would not apply to any first time violation by the government. By only penalizing the government for repeated or continued violations, the government would not be exposed to astronomical liability. However, punitive damages will deter agencies from ignoring or assigning low priorities to privacy violations.

The increased measure of damages as recommended above will provide the proper incentives for individuals to bring actions to enforce the Privacy Act. However, the recommended measure of damages should only be awarded once an individual proves an "adverse effect" to

286. *Doe v. Chao*, 124 S.Ct. 1204, 1217-18 (2004) (Ginsburg, J., dissenting) (pointing out that courts have not allowed class certification and runaway liability and that government has not experienced enormous recoveries).

287. PERSONAL PRIVACY, *supra* note 6, at 500.

288. *Id.*

289. *See supra* notes 232-235 and accompanying text (discussing low private enforcement rate and factors contributing to low private enforcement rate).

290. *Dun & Bradstreet, Inc. v. Greenmoss Builders, Inc.*, 472 U.S. 749, 760 (1985).

the individual and an “intentional and willful” level of culpability by the government. Since courts’ restrictive interpretations made these elements difficult to prove, individuals would be deterred from bringing frivolous lawsuits. Therefore, the increased measure of damages would allow individuals to recover only for meritorious actions.

V. CONCLUSION

Informational privacy is vital in today’s society. The Privacy Act of 1974 attempts to protect individuals’ privacy from governmental intrusions. The effectiveness of the Privacy Act, however, lies in the ability of individuals to bring enforcement actions against the government. Unfortunately, the Supreme Court’s recent decision in *Doe v. Chao* obliterates the incentives necessary for individuals to bring enforcement actions against the government under the Privacy Act. Therefore, Congress should once again take legislative action to provide incentives for individuals to compel the government’s compliance with safeguarding individuals’ rights to privacy and to effectuate the Privacy Act.