University of Cincinnati Law Review

Volume 81 | Issue 3 Article 6

6-23-2013

Are You on the List? Dispelling the Myth of a Total Exemption from the Privacy Act's Civil Remedies in Shearson v. DHS

Maxim Brumbach
University of Cincinnati College of Law, brumbamg@mail.uc.edu

ARE YOU ON THE LIST? DISPELLING THE MYTH OF A TOTAL EXEMPTION FROM THE PRIVACY ACT'S CIVIL REMEDIES IN *SHEARSON V. DHS*

*Maxim Brumbach**

No one wants to be on the list.

I. INTRODUCTION

In the post-9/11 era, Americans have increasingly come to accept that collecting private information is necessary to national security.[1] Keeping the public safe undoubtedly requires the government to maintain lists of persons of interest and assess the threats such individuals pose to our national security. But what happens when something goes wrong?

Julia Shearson, a Harvard graduate and a prominent interfaith leader at the Council on American–Islamic Relations, found out exactly what can happen.[2] On a Sunday evening in January 2006, Ms. Shearson was returning from a road trip with her four-year-old daughter.[3] Their weekend getaway to Canada was drawing to a close as they crossed the Peace Bridge approaching Buffalo, New York.[4] What happened next was a traveler's nightmare. When Ms. Shearson handed her passport over to a U.S. Customs and Border Protection (CBP) agent, the agent's computer screen flashed red with the message "ARMED AND DANGEROUS."[5] Ms. Shearson was ordered out of her vehicle, handcuffed, and detained for questioning.[6] Her car was searched, and she was not allowed to call her family or an attorney.[7] After two and a half hours of questioning, Ms. Shearson was released without

* Associate Member, 2011–12 *University of Cincinnati Law Review*. This article was drafted in late 2011 and does not reflect the Supreme Court's holding in *F.A.A. v. Cooper*, 132 S. Ct. 1441 (2012), which is outside the scope of this Casenote.

1. *See* David Crary, *Post-9/11 Tradeoff: Security vs. Civil Lberties*, HOUSTON CHRON. (Nov. 22, 2011), http://www.chron.com/news/article/Post-9-11-tradeoff-Security-vs-civil-liberties-2277843.php#page-1.

2. Robert L. Smith, *Julia Shearson Tells How a Weekend Trip to Canada Became 5-year Fight for Rights*, CLEVELAND.COM (Jun. 4, 2011), http://blog.cleveland.com/metro/2011/06/julia_shearson_tells_how_a_wee.html. A native of Ohio who was raised Catholic and converted to Islam, Shearson helped open an office of the Council on American-Islamic Relations in Cleveland. *Id.*

3. *Id.*

4. *Id.*

5. *Id.* Shearson had no criminal record and had never owned a gun. *Id.*

6. *Id.*

7. *Id.*

explanation.[8]

After the incident, Ms. Shearson sought answers from the government but received only a few highly redacted documents in response. She filed a complaint in the U.S. District Court for the Northern District of Ohio under the Privacy Act and the Freedom of Information Act seeking access to her records, a declaration that the CBP report was inaccurate, and an injunction requiring its correction.[9] The district court ruled that the Department of Homeland Security (DHS) had exempted its system of records from the civil remedies provision of the Privacy Act, and Ms. Shearson's claims were dismissed.[10] On appeal, the Sixth Circuit vacated the dismissal of Shearson's claims for improper disclosure of information and for improper monitoring of activity protected by the First Amendment.[11] In reaching this decision, the court held that an agency may exempt its systems of records from civil liability only to the extent that the systems of records may be otherwise exempted from substantive provisions of the Privacy Act.[12]

Part II of this Casenote examines the validity of this interpretation related to the history and purpose of the Privacy Act. Part III considers the competing interpretations in previous cases involving the law enforcement exemption. Part IV analyzes the Sixth Circuit's decision in *Shearson v. DHS* and argues that the statute's language and underlying purpose support the court's narrow interpretation. Part V concludes that courts should follow the approach in *Shearson*, but Congress should pass legislation to protect privacy rights from encroachment by law enforcement agencies.

II. BACKGROUND

In the early 1970's, America was faced with a problem: considering the government's rapidly growing collection of personal data, how should citizens be protected from inaccuracies of records and misuse of personal data?[13] This problem grew out of several technological

8. *Id.*

9. Complaint, Shearson v. U.S. Dep't of Homeland Sec., (N.D. Ohio Jun. 15, 2006) (No. 106 CV 1478), 2006 WL 2315107 [hereinafter Complaint]. The court also became frustrated with documents from the agency that were too greatly redacted to read or understand. *See* Shearson v. U.S. Dept. of Homeland Sec., No. 1:06 CV 1478, 2008 WL 928487, at *5 (N.D. Ohio Apr. 4, 2008) ("The Court is greatly disturbed at the inordinate amount of redactions present in the government's brief. Other than a general overview of the exemptions claimed, there is no other readable material.").

10. Shearson v. U.S. Dept. of Homeland Sec., No. 106 CV 1478, 2007 WL 764026, at *12–13 (N.D. Ohio Mar. 9, 2007) *rev'd on reconsideration*, No. 1:06 CV 1478, 2008 WL 928487 (N.D. Ohio Apr. 4, 2008).

11. Shearson v. U.S. Dept. of Homeland Sec., 638 F.3d 498, 499 (6th Cir. 2011).

12. *Id.* at 504.

13. *See* President Richard Nixon, *Radio Address About the American Right of Privacy*, *February*

advances, including the development of the computer[14] and the rise of consumer credit cards.[15] In addition to these developments, the Watergate scandal sparked fear about secret records the government kept.[16] In this tumultuous political climate, President Nixon called for immediate action and created the Domestic Council Committee on the Right of Privacy to develop comprehensive recommendations for new legislation.[17] Congress acted swiftly to draft a law that would protect individual privacy from government encroachment, ultimately leading to the passage of the Privacy Act.[18]

The first subpart of this Part discusses the legislative development of the Privacy Act (the Act). The next two subparts discuss specifically the development of the law enforcement exemption and the civil remedies provision. The final subpart explains the structure of the Act, with an emphasis on the law enforcement and civil remedies provisions.

A. The Legislative Development of the Privacy Act

When Senator Sam Ervin, Jr. introduced an early version of the Privacy Act to the Senate, he said, "[T]he appetite of government and private organizations for information about individuals threatens to usurp the right to privacy which I have long felt to be among the most basic of our civil liberties as a free people."[19] Senator Ervin and other legislators conducted investigations, concluding that many government agencies maintained huge files of information without specific guidelines about their maintenance.[20] Some of these databases were

23, 1974, AM. PRESIDENCY PROJECT (Feb. 23, 1974), http://www.presidency.ucsb.edu/ws/?pid=4364 ("Though well-intentioned, Government bureaucracies seem to thrive on collecting additional information. That information is now stored in over 7,000 Government computers. Collection of new information will always be necessary. But there must also be reasonable limits on what is collected and how it is used.").

14. *See id.* ("With the advent of the computer in the 1960's, this data gathering process has become a big business in the United States—over $20 billion a year—and the names of over 150 million Americans are now in computer banks scattered across the country.").

15. *See* Robin Stein, *The Ascendancy of the Credit Card Industry*, PBS: FRONTLINE (Nov. 23, 2004), http://www.pbs.org/wgbh/pages/frontline/shows/credit/more/rise.html.

16. *See* 120 CONG. REC. S6741 (daily ed. May 1, 1974) (remarks of Sen. Ervin), *reprinted in* COMM. ON GOV'T OPERATIONS, U.S. SENATE AND COMM. ON GOV'T OPERATIONS, U. S. H.R., LEGIS. HISTORY OF THE PRIVACY ACT OF 1974, S. 3418 (PUBLIC LAW 93-579), SOURCE BOOK ON PRIVACY at 4 [hereinafter SOURCE BOOK] ("If we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens.").

17. Nixon, *supra* note 13.

18. *See* 120 CONG. REC. S6741 (daily ed. May 1, 1974) (remarks of Sen. Ervin), *reprinted in* SOURCE BOOK, *supra* note 16, at 5–6; Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896-1905 (1974).

19. 120 CONG. REC. S6741 (daily ed. May 1, 1974) (remarks of Sen. Ervin), *reprinted in* SOURCE BOOK, *supra* note 16, at 3–4.

20. *See* Sam J. Ervin, Jr., *The First Amendment: A Living Thought in the Computer Age*, 4

"blacklists," encompassing unverified and outdated information.[21] In many cases, different government agencies freely shared lists and records.[22] According to Senator Ervin, people throughout the country were "concerned that through a computer error they may be denied basic fairness and due process of law with respect to benefits and privileges for which they have applied."[23] Senator Ervin illustrated this problem in a 1972 article, recounting the story of the mayor of San Francisco who was accused of involvement with organized crime based on investigative records that were improperly released to journalists.[24]

Senator Ervin was not alone in his view; legislators had received reports that, in light of new data systems being built, failing to set limits on their operation would seriously jeopardize the security of citizens' personal information.[25] Such systems would be extremely costly to upgrade or replace after their initial implementation.[26] Additionally, the government's General Services Administration had proposed a massive centralized database of personal information called FEDNET.[27] Legislators were concerned that the law could not keep up with the fast pace at which technology was evolving.

In the wake of the Watergate scandal, many politicians were also nervous about the power that the government could wield through its data collection.[28] Congress was concerned about unauthorized

COLUM. HUM. RTS. L. REV. 13, 15–18 (1972). The Senate Subcommittee on Constitutional Rights had untaken a survey of government agencies about their use of databases. *Id.* at 17. In many cases, the Subcommittee had trouble getting responses from agencies or received "evasive and misleading" reports. *Id.* at 18.

21. *Id.* at 19. According to Sen. Ervin, these "blacklists" contained "masses of irrelevant, outdated or even incorrect investigative information based solely on personalities, behavior and beliefs." *Id.*

22. *Id.* at 21–22.

23. *Id* at 23. In his article, Sen. Ervin provides numerous examples, including several accounts of citizens being denied employment based on arrest records disclosed by the F.B.I. *Id.* at 24–35.

24. *Id.* at 28.

25. S. REP. NO. 93-1183, at 7, *reprinted in* SOURCE BOOK, *supra* note 16, at 160 (citing testimony of Dr. Alan F. Westin).

26. *Id.* ("[T]hese systems may become so large, so expensive, and so vital to so many Americans that public opinion will be put to a terrible choice—serious interruption of services or installation of citizen-rights measures.").

27. *Id.* at 10–11, *reprinted in* SOURCE BOOK, *supra* note 16, at 163–64. Concerned about the project, the Vice-Presdent said that the government must "consider the fallout hazards of FEDNET to traditional freedoms." *Id.*

28. *Id.* at 11, *reprinted in* SOURCE BOOK, *supra* note 16, at 164 ("The revelations before the Select Committee to Investigate Presidential Campaign Activities concerning policies and practices of promoting the illegal gathering, use or disclosure of information on Americans who disagreed with governmental policies were cited by almost all witnesses as additional reasons for immediate congressional action on . . . privacy legislation."); *see also* H.R. REP. NO. 93-1416, at 8–9, *reprinted in* SOURCE BOOK, *supra* note 16, at 301–02.

wiretapping and the existence of secret White House enemy lists.[29] President Nixon commented that government knowledge about citizens "brings with it an awesome potential for harm as well as good—and an equally awesome responsibility on those who have that knowledge."[30]

As the Senate Committee on Government Operations reported, the Privacy Act was designed to "promote accountability, responsibility, legislative oversight and open government with respect to the use of computer technology."[31] Among its several purposes, the Act was meant to prevent "illegal, unwise, overbroad investigation and record surveillance of law-abiding citizens."[32] In drafting the initial bill, the Government Operations Committee relied on several sources, including a report from the Department of Health, Education and Welfare that recommended creating a Code of Fair Information Practice based on five core principles[33]: (1) there must be no personal data record-keeping systems whose very existence is secret; (2) there must be a way for individuals to find out what information about them is in a record and how it is used; (3) there must be a way for an individual to prevent information collected for one purpose to be used for another, incongruent purpose, unless there is consent; (4) there must be a way for an individual to correct or amend a record of identifiable information; and (5) any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for its intended use and must take precautions to prevent misuse of the data.[34]

With these concerns in mind, both houses of Congress introduced bills to protect individual privacy.[35] In general, the Senate bill placed stricter requirements on government agencies than the House bill did.[36] The Senate's bill included a Privacy Protection Commission with broad oversight responsibilities, while the House version included a study commission with primarily an advisory role.[37] In several ways, the Senate bill required agencies to maintain records only to the extent necessary to accomplish their purpose.[38] Conversely, the House bill

29. H.R. REP. NO. 93-1416, at 8–9, *reprinted in* SOURCE BOOK, *supra* note 16, at 301–02.

30. Nixon, *supra* note 13.

31. S. REP. NO. 93-1183, at 1, *reprinted in* SOURCE BOOK, *supra* note 16, at 154.

32. *Id*.

33. *Id.* at 8–9, *reprinted in* SOURCE BOOK, *supra* note 16, at 161–62.

34. *Id.* at 9, *reprinted in* SOURCE BOOK, *supra* note 16, at 162.

35. S. 3418, 93rd Cong. § 203 (1974); H.R. 16373, 93rd Cong. (1974).

36. *See* Doe v. Chao, 540 U.S. 614, 622–23 (2004); Tijerina v. Walters, 821 F.2d 789, 799 (D.C. Cir. 1987).

37. 120 CONG. REC. 40405 (1974); *reprinted in* SOURCE BOOK, *supra* note 16, at 860–61 (explaining House version of the bill).

38. *See id.* at 40406, *reprinted in* SOURCE BOOK, *supra* note 16, at 861.

added limitations on the bill's reach including the "routine use" exception that allowed agencies regularly to share certain personal information, such as payroll data.[39] With a tense political climate and great pressure to take action, legislators worked a compromise between the two bills in the closing months of 1974.[40]

B. Development of the Law Enforcement Exemption

While the Privacy Act was arguably rushed through the legislature, one of the most debated issues was the extent to which national security and law enforcement agencies should be exempted from the terms of the law.[41] Legislators recognized from the very beginning that national security and law enforcement efforts could be undermined if the public was granted access to sensitive agency records.[42] Legislators in both houses of Congress sought to safeguard the work of agencies like the Central Intelligence Agency (CIA) and the Justice Department by creating exemptions, while balancing theses interests against the individual rights that the Privacy Act would secure.[43]

The Senate created a narrow exemption in its version of the bill designed to limit public access to sensitive records.[44] The Senate bill did not create a blanket exemption for law enforcement agencies, but instead allowed exemptions only for specific systems of records.[45] Under a revised version of the bill, law enforcement records were

39. REP. OF THE COMM. ON GOV'T OPERATIONS, 120 CONG. REC. 40405–06 (Dec. 17, 1974), *reprinted in* SOURCE BOOK, *supra* note 16, at 859.

40. *See* 120 CONG. REC. 40410–11 (Dec. 17, 1974) (remarks of Sen. Hruska), *reprinted in* SOURCE BOOK, *supra* note 16, at 871–72.

41. 120 CONG. REC. 36960 (Nov. 21, 1974) (remarks of Rep. Abzug), *reprinted in* SOURCE BOOK, *supra* note 16, at 938–39.

42. *Id.* at 36960 (remarks of Rep. Erlenborn), *reprinted at* SOURCE BOOK, *supra* note 16, at 939–40.

43. *Compare* S. REP. NO. 93-1183, at 3, *reprinted in* SOURCE BOOK, *supra* note 16, at 156, *with* H.R. 16373 § 2(i) *reprinted in* SOURCE BOOK, *supra* note 16, at 252–53.

44. S. 3418, 93rd Cong. § 202 (1974) (as introduced, May 1, 1974), *reprinted in* SOURCE BOOK, *supra* note 16, at 23. This section provided:

> The provisions of this title shall not apply to personal information systems—
>
> (1) to the extent that information in such systems is maintained by a Federal agency, and the head of that agency determines that the release of the information would seriously damage national defense;
>
> (2) which are part of active criminal investigatory files compiled by Federal, State, or local law enforcement organizations, except where such files have been maintained for a period longer than is necessary to commence criminal prosecution; or
>
> (3) maintained by the press and news media, except information relating to employees of such organizations.

Id.

45. *See id.*

exempted only from provisions for individual access to records, inquiry into the source of records, and certain limits on the dissemination of records.[46] In some cases, however, an agency head would have to show that access to a system of records would "seriously damage or impede the purpose for which the information is maintained."[47] The Senate bill also included a Privacy Protection Commission with a significant oversight and investigatory role in these determinations.[48]

The House of Representatives designed a much broader general exemption that exempted certain records from nearly all requirements of the bill.[49] The general exemptions applied to all systems of records the CIA maintained, and most systems maintained "by an agency or component thereof which perform as its principal function any activity pertaining to the enforcement of criminal laws."[50] The exempted systems of records would be subject only to the requirement of publishing a name and description of the system.[51]

A group of legislators led by Representative Bella Abzug, chair of the Government Information and Individual Rights Subcommittee, argued for a more limited law enforcement exemption.[52] In Rep. Abzug's view, exemptions from the bill were "justified only in the face of overwhelming societal interests."[53] She emphasized defining the exemptions "in specific terms related to the use of records rather than to the agency maintaining them."[54] Accordingly, Rep. Abzug proposed amendments to eliminate the general exemptions for the CIA and the Secret Service, arguing that "[a] blanket exemption for any agency . . . has no place in the bill."[55] Despite Rep. Abzug's proposals, the exemptions were left in the bill that was sent to the Senate.[56]

In light of the disparate versions of the law enforcement exemption,

---

46. S. 3418, 93rd Cong. § 203 (1974) (as passed by Senate, Nov. 21, 1974), *reprinted in* SOURCE BOOK, *supra* note 16, at 361–63.

47. *See id.*

48. *Id.* § 103, *reprinted in* SOURCE BOOK, *supra* note 16, at 338–41. The Commission was to investigate and report violations of the Act, review new data systems proposed by agencies, and make recommendations about implementing the Act and developing future legislation. *Id*.

49. Privacy Act of 1974, H.R. 16373 § 2(i), 93rd Cong. (1974) (as introduced), *reprinted in* SOURCE BOOK, *supra* note 16, at 252–53.

50. *Id*. The Act goes on to specify that the exemption applies only to those systems of records maintained for law enforcement purposes, including investigation, prosecution, confinement, etc. *Id.*

51. *Id.* § 2(e)(1)–(3), *reprinted in* SOURCE BOOK, *supra* note 16, at 247–48.

52. 120 CONG. REC. 36960 (remarks of Rep. Abzug), *reprinted in* SOURCE BOOK, *supra* note 16, at 938.

53. H.R. REP. NO. 93-1416, at 17 (1974) (additional views of Rep. Abzug), *reprinted in* SOURCE BOOK, *supra* note 16, at 329.

54. *Id.*, *reprinted in* SOURCE BOOK, *supra* note 16, at 330.

55. 120 CONG. REC. 36960 (remarks of Rep. Abzug), *reprinted in* SOURCE BOOK, *supra* note 16, at 941.

56. *See id.* at 36960, *reprinted in* SOURCE BOOK, *supra* note 16, at 943.

legislators soon reached a compromise in a further amended version of the bill that returned to the Senate floor.[57] With these revisions in place, Senator Roman Hruska argued that the compromise did not effectively address the issue of national security and law enforcement records.[58] Senator Hruska, fearing that further change would drag out the process, proposed to deal with such records through separate legislation.[59] Under pressure to act before the end of the legislative session, however, the Senate and the House both approved the compromise version virtually unaltered.[60] The compromise version, substantively the same as the Act stands today, kept the House's broad general exemption framework but added numerous sections to the list of non-exemptible provisions.[61]

C. Development of the Civil Remedies Provision

Embracing many of the same policy concerns as the law enforcement exemption, the civil remedies provision similarly required a major compromise between the two versions of the bill.[62] The Senate version provided for strong civil enforcement, originally allowing plaintiffs to recover actual and punitive damages.[63] The House bill, on the other hand, sought to limit the scope of government liability.[64] While the Senate version required the plaintiff to prove only negligence, the House version required proof that a violation was "willful, capricious, and arbitrary."[65] Ultimately, legislators compromised on a standard of "willful or intentional" conduct, but added a statutory minimum of $1,000 in damages.[66]

Significantly, the Supreme Court has construed the damages provision narrowly to limit recovery to actual damages proven by the plaintiff.[67] Thus, while Congress arguably intended to create a type of

57. *See id.*

58. 120 CONG. REC. 36905–07 (remarks of Sen. Hruska), *reprinted in* SOURCE BOOK, *supra* note 16, at 809–11.

59. *Id.*

60. 120 CONG. REC. 40885–86, *reprinted in* SOURCE BOOK, *supra* note 16, at 998–1001. The principle difference involved the Senate's Privacy Commission. To reach a compromise with the House, the amended bill included a study commission with a much lesser role than originally contemplated by the Senate. *See id.*

61. *Compare* Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896-1905 (1974), *with* 5 U.S.C. § 552a (2006).

62. *See* Haeji Hong, *Dismantling the Private Enforcement of the Privacy Act of 1974:* Doe v. Chao, 38 AKRON L. REV. 71, 86–87 (2005).

63. *Id.* at 87.

64. *Id.* at 88.

65. *Id.*

66. *See* Hong, *supra* note 62, at 89–90.

67. Doe v. Chao, 540 U.S. 614, 627 (2004).

presumed damages, the provision has not been interpreted to do so.[68] The policies that underlie the debate on government liability are too vast to discuss here, but it is sufficient to say the narrow construction of the Privacy Act's civil remedies significantly limits the power of private enforcement.[69]

D. The Structure of the Privacy Act

In general, the Privacy Act lists numerous duties imposed on government agencies that limit the way they can collect, store, and transmit private information.[70] The subsections place specific requirements upon the way an agency maintains its records.[71] Most of these requirements, however, do not apply to law enforcement databases due to the law enforcement and routine use exemptions.[72]

When the Act was drafted, Congress understood the need for certain government databases to be exempt from provisions of the Act because some databases involve sensitive law enforcement and national security information.[73] Subsection (j) of the Act provides a general exemption for databases the CIA maintains, and provides exemptions for other agencies that principally perform activities "pertaining to the enforcement of criminal laws."[74] If an agency promulgates appropriate regulations including the reason for the exemption, then a system of records may be exempted from most of the Act's provisions.[75] However, subsection (j) lists specific sections from which a law enforcement system of records may not be exempted.[76] These non-exemptible sections form a core of requirements that apply to all government databases. Under these requirements, an agency must:

68. *Id.*; *see also* Hong, *supra* note 62, at 100–01.

69. Hong, *supra* note 62, at 102–03; *see also* Alex Kardon, *Damages Under the Privacy Act: Sovereign Immunity and a Call for Legislative Reform*, 34 HARV. J.L. & PUB. POL'Y 705, 758–59 (2011).

70. *See* 5 U.S.C. § 552a (2006).

71. *Id.*

72. *Id.* § 552a(j)–(k); *see also infra* note 74.

73. *See* S. REP. NO. 93-1183, at 74–75, *reprinted in* SOURCE BOOK, *supra* note 16, at 227–28; H.R. REP NO. 93-1416, at 3–4, *reprinted in* SOURCE BOOK, *supra* note 16, at 296–97.

74. 5 U.S.C. § 552a(j) (2006). This subsection provides, "The head of any agency may promulgate rules . . . to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is—(1) maintained by the Central Intelligence Agency; or (2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including [information concerning any stage of investigation, arrest, charging, disposition, sentencing or parole]." *Id.*

75. *Id.*; *see also* Ryan v. Dep't of Justice, 595 F.2d 954, 957 (4th Cir. 1979).

76. 5 U.S.C. § 552a(j).

(1) disclose a record only as specifically provided by subsection (b) of the statute−such disclosure is generally limited by the reason for the disclosure, i.e., law enforcement records may be disclosed for other law enforcement purposes;[77]
(2) account for disclosure and keep the accounting on file for five years;
(3) publish a description of each system of records in the federal register;
(4) make reasonable efforts to assure that disseminated records are "accurate, complete, timely, and relevant" to the agency's purpose;
(5) maintain no record of First Amendment activity except as authorized, including when pertinent to and within the scope of law enforcement;
(6) establish rules and security safeguards to protect confidentiality; and
(7) publish any new use of data 30 days in advance of such use.[78]

An agency also cannot exempt itself from the criminal penalties provision of the Act.[79]

To enforce the duties described in the Act, the civil remedies provision covers four specific situations listed under subsection (g). These situations include when an agency (1) determines not to amend records, (2) refuses access to records, (3) fails to maintain accurate records, and (4) fails to adhere to other provisions of the Act and causes an adverse effect (the "catch-all" provision).[80] The first two remedy provisions apply to parts of the Act that are within the scope of the law enforcement exemption.[81] The remaining accuracy and catch-all remedies have been the subject of some debate among litigants since these remedies may be used to enforce rights guaranteed by the non-exemptible parts of the Act.[82] Because these subsections are not mentioned among the non-exemptible sections listed under the law enforcement exemption, courts have struggled to determine whether the exemption provision allows an agency to escape liability related to the accuracy and catch-all provisions.[83]

77. *Id.* § 552a(b). The section permits, in pertinent part, disclosure (1) "to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties"; (2) "for a routine use as defined in subsection (a)(7)"; (3) "to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request"; and (4) under certain other circumstances required by law. *Id.*

78. *See id.* § 552a(j), (b), (c)(1)–(2), (e)(4)(A)–(F), (e)(6)–(7), (e)(9)–(10), and (e)(11).

79. *Id.*; *id.* § 552a(i). This section provides for a fine of up to $5,000 for (1) willfully, improperly disclosing information; (2) willfully maintaining a system of records without notice; or (3) willfully requesting or obtaining a record under false pretenses. *Id.*

80. *Id.* § 552a(g); *see also* Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 502 (6th Cir. 2011) (quoting Doe v. Chao, 540 U.S. 614, 618–19 (2004)).

81. *See Shearson*, 638 F.3d at 502; Doe v. F.B.I., 936 F.2d 1346, 1352 (D.C. Cir. 1991).

82. *E.g.*, *Shearson*, 638 F.3d at 502–03.

83. *See id.*

III. CASE LAW ON THE LAW ENFORCEMENT EXEMPTION

Two interpretations of the Privacy Act's law enforcement exemption have emerged. Under the first interpretation, some courts have held that an agency may exempt a system of records from civil remedies entirely.[84] Under the second interpretation, other courts have concluded that an agency may exempt a system of records from civil remedies only to the extent that the Act's other substantive provisions are exemptible.[85]

A. The "Complete Exemption" Interpretation

One of the first cases to test the Privacy Act's law enforcement exemptions was *Ryan v. Department of Justice*.[86] In *Ryan*, the Fourth Circuit reasoned that, but for a procedural failure, the Justice Department could have exempted its system of records from subsection (g) completely.[87] The plaintiff, an FBI security officer, alleged that the Justice Department had wrongfully disclosed information to the Washington Post about his work.[88] He sought access to a memorandum concerning him, as well as damages for the alleged wrongful disclosure.[89] The court held that the FBI had appropriately exempted the system containing the memo from the Act's mandatory access provision in subsection (d).[90] The court explained that the Privacy Act requires an agency to promulgate rules stating both the exemption and the reason for such exemption.[91] Examining the Justice Department's regulations, the court concluded that the agency had provided a rationale pertaining only to subsection (d) of the Act.[92] The agency had, therefore, exempted its records only from that specific subsection.[93] Nonetheless, the court stated that the agency "had the authority to exempt [the system of records] from the application of all the civil remedies."[94]

In 1986, a pair of appellate cases endorsed the same reasoning as *Ryan*.[95] In *Kimberlin v. U.S. Department of Justice*, the Seventh Circuit

84. *See id.*
85. *See id.*
86. Ryan v. Dep't of Justice, 595 F.2d 954, 954 (4th Cir. 1979).
87. *Id.* at 958.
88. *Id.* at 955.
89. *Id.*
90. *Id.* at 957–58.
91. Ryan v. Dep't of Justice, 595 F.2d 954, 957 (4th Cir. 1979).
92. *Id.* at 958.
93. *Id.*
94. *Id.*
95. *See* Kimberlin v. U.S. Dep't of Justice, 788 F.2d 434 (7th Cir. 1986); Alexander v. United

considered an inmate's wrongful disclosure claim and ultimately found that the disclosure was proper under a separate routine use exception in subsection (b).[96] In a footnote, however, the court echoed the Fourth's Circuit's view that systems of records can be exempted from subsection (g).[97] As in *Ryan*, the statement was not necessary to the court's dismissing the plaintiff's claims.[98]

Soon after the *Kimberlin* decision, the Ninth Circuit finally applied the complete exemption interpretation to bar a plaintiff's Privacy Act claim.[99] In *Alexander v. United States*, the plaintiff alleged that he had been terminated from his job as a security officer because the FBI failed to maintain accurate records on his rap sheet.[100] According to the plaintiff, his record contained information about two arrests that a court had ordered expunged.[101] Upon considering the plaintiff's Privacy Act claims, the court held that the FBI had properly promulgated regulations to exempt its Identification Division Records System from the civil remedies provision.[102] The exemption from the provision was necessary, according to the FBI's regulations, because subsection (g) "concern[s] an individual's access to records" and "the vast majority of records in this system concern local arrests which it would be inappropriate for the FBI to undertake to correct."[103] Further, the court stated that the law enforcement exemption "expressly prohibits suits against an agency for passing inaccurate information to a third party, if appropriate regulations have been issued."[104] The court provided no additional analysis of the statute's language or purpose in reaching this conclusion.[105]

Though the notion of a complete exemption from subsection (g) was explicitly held only in *Alexander*, other district court cases have confirmed the acceptance of this construction.[106] In *Aquino v. Stone*, the plaintiff claimed that the Army wrongfully failed to amend a record stating that the plaintiff had been investigated for sexual abuse of a

States, 787 F.2d 1349 (9th Cir. 1986).

96. *Kimberlin*, 788 F.2d at 435–38.

97. *Id.* at 436 n.2.

98. *Compare Kimberlin*, 788 F.2d at 436, *with* Ryan v. Dep't of Justice, 595 F.2d 954, 958 (4th Cir. 1979).

99. *Alexander*, 787 F.2d at 1351–52.

100. *Id.* at 1350.

101. *Id.*

102. *Id.* at 1351.

103. *Id.* at 1351 n.2.

104. Alexander v. United States, 787 F.2d 1349, 1351 (9th Cir. 1986).

105. *See id.* at 1351–52.

106. *See, e.g.*, Aquino v. Stone, 768 F. Supp. 529 (E.D. Va. 1991), *aff'd*, 957 F.2d 139 (4th Cir. 1992).

child.[107] The court cited *Ryan* for the proposition that an agency may exempt law enforcement records from subsection (g) and never considered the merits of the plaintiff's claim.[108] Similarly, in *Witherspoon v. F.B.I.*, the District Court for the District of Columbia succinctly held that the plaintiff did not state a cause of action for the F.B.I.'s alleged failure to maintain accurate records of his "rap sheet."[109] As recently as March 2010, the District Court for the Northern District of Florida again confirmed the "total exemption" interpretation in *Study v. United States*.[110] In *Study*, the court dismissed the pro se plaintiff's wrongful dissemination claim against county officials and the F.B.I.[111]

B. The "Limited Exemption" Interpretation

Though the *Ryan* interpretation seemed to dominate the circuit courts, the D.C. Circuit reached a significantly narrower interpretation of the law enforcement exemption.[112] In *Tijerina v. Walters*, the D.C. Circuit broke from the earlier line of cases, holding that the government could not use subsection (j) to exempt itself entirely from subsection (g).[113] In *Tijerina*, the plaintiff alleged that the Veterans Administration (VA) failed to maintain records accurately and improperly disclosed the results of a home mortgage audit.[114] The VA had conducted a random audit of Tijerina's loan transaction and concluded Tijerina had lied on his verification of employment form.[115] Though the agency declined to prosecute Tijerina, one of the agency's inspectors learned that Tijerina had taken the District of Columbia bar exam and planned to take the Texas bar exam as well.[116] The inspector sent unsolicited letters to the bar admissions authorities in both jurisdictions, informing them that Tijerina had falsified a document during his mortgage application

107. *Id.* at 529–30.

108. *Id.* at 530.

109. Witherspoon v. F.B.I., No. CIV.A. 96-619 GK, 1997 WL 135718, at *1 (D.D.C. Mar. 17, 1997). This is a most perplexing result, since the Court of Appeals for the D.C. Circuit had previously rejected such a construction in *Tijerina v. Walters*, 821 F.2d 789, 799 (D.C. Cir. 1987); *see also* discussion *infra* Part III.B.

110. Study v. United States, No. 3:08-CV-493/MCR/EMT, 2010 WL 1257655, at *4 (N.D. Fla. Mar. 4, 2010), *report and recommendation adopted*, No. 3:08-CV-493/MCR/EMT, 2010 WL 1257654 (N.D. Fla. Mar. 25, 2010).

111. *Id.* at *1–4. Admittedly, this claim was poorly made at best. State and local officials are not subject to the Privacy Act.

112. *Tijerina*, 821 F.2d at 797.

113. *Id.*

114. *Id.* at 791–93.

115. *Id.* at 792.

116. *Id.*

process.[117]

The court engaged in a lengthy analysis of subsections (g) and (j), ultimately rejecting the government's complete exemption interpretation.[118] The court initially observed that subsection (j) permits an agency to exempt a system of records from provisions of the Act—not the agency itself.[119] The exemption, the court reasoned, applies only to substantive requirements of the Act that would interfere with the secrecy of law enforcement activities.[120] The court also cited a House Report that said law enforcement records would still be subject to the disclosure requirements.[121] The court expressly declined to follow the reasoning of *Ryan* and *Kimberlin*, finding that the issue had not been squarely presented in those cases and such a construction would "make[] the Act a foolishness."[122] The D.C. Circuit later clarified *Tijerina*'s holding in *Doe v. FBI*, declaring, "[A]n agency cannot escape liability for *non-exemptible* Privacy Act obligations simply by exempting itself from the Act's remedial provisions."[123]

C. The District Court's Opinion in Shearson v. DHS

In *Shearson v. DHS*, the District Court for the Northern District of Ohio accepted the complete exemption interpretation and dismissed the plaintiff's Privacy Act claims against DHS.[124] In her complaint, Shearson alleged that DHS had improperly refused her access to records and had improperly disseminated her records.[125] She claimed that DHS had "failed to make reasonable efforts to ensure the accuracy of the records, improperly maintained records pertaining to her First Amendment activity, and failed to properly account for certain disclosures."[126]

Upon consideration of these claims, the district court concluded that, regardless of the merits of her allegations, Shearson had "no private

117. Tijerina v. Walters. 821 F.2d 789, 792 (D.C. Cir. 1987). This ultimately led to the Texas bar authority finding Mr. Tijerina "morally unfit to take the Texas bar examination." *Id*. at 791.

118. *Id.* at 795.

119. *Id.* at 795–96.

120. *Id.* at 796.

121. *Id.*

122. Tijerina v. Walters. 821 F.2d 789, 797 (D.C. Cir. 1987).

123. Doe v. F.B.I., 936 F.2d 1346, 1352 (D.C. Cir. 1991). The plaintiff in *Doe v. F.B.I.* attempted to strain the holding of *Tijerina* to render the agency liable under an *exemptible* part of the Act. *See id*.

124. Shearson v. U.S. Dept. of Homeland Sec., 106 CV 1478, 2007 WL 764026 at *12–13 (N.D. Ohio Mar. 9, 2007), *rev'd on reconsideration*, 1:06 CV 1478, 2008 WL 928487 (N.D. Ohio Apr. 4, 2008).

125. Complaint, *supra* note 9, at ¶¶ 44, 50.

126. *Shearson*, 2007 WL 764026 at *12 n.14.

right of action" to pursue them under the Privacy Act.[127] The court examined the reasoning of *Tijerina* closely, but ultimately rejected it for two reasons.[128] First, the court found that the plain language of subsection (j) permits an agency to exempt a system of records from any provision other than those specifically listed.[129] Second, the court compared the civil remedies provision with the criminal enforcement provision (subsection (i)) and determined that the inclusion of the latter on the non-exemptible list meant that Congress had deliberately excluded the civil remedies provision.[130]

D. The Sixth Circuit Court of Appeals Decision

On appeal, the Sixth Circuit reversed the district court's decision, concluding the limited exemption interpretation reached by the D.C. Circuit was the better approach.[131] The Sixth Circuit began its analysis with the plain language of the statute, but found that the language pointed in two different directions: subsection (j) omits subsection (g) from the list of non-exemptible provisions, but subsection (j) simultaneously precludes an agency from exempting a system of records from other provisions which would be vindicated through subsection (g)'s remedies.[132] Against this backdrop, the court considered the case law for both interpretations.[133] The court revisited the lower court's comparison of the civil remedies provision and the criminal penalties provision, but ultimately found such a comparison unhelpful.[134] The criminal penalties section makes certain conduct a crime while the civil remedies provision is "strictly an enforcement section" that relies on the rest of the Act's substantive obligations.[135] Thus, the court reasoned, the two sections are not parallel.[136]

Moreover, the court observed that including subsection (g) on the list of non-exemptible subsections "might have caused confusion with respect to exemptible obligations."[137] If, as the court in *Tijerina* reasoned, subsection (g) provides remedies to both exemptible and non-exemptible provisions then it would be confusing to include the whole

127. *Id.* at *12, *12 n.14.
128. *Id.* at *12.
129. *Id.*
130. *Id.*
131. Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 504 (6th Cir. 2011).
132. *Id.* at 502.
133. *Id.* at 502–03.
134. *Id.* at 503. The court noted that this problem gave them pause, however. *See id.*
135. *Id.*
136. *Id.*
137. *Id.*

of subsection (g) on the list.[138] The court also noted that subsection (j)'s non-exemptible provisions list omits a part of the Act that enables guardians to act on the behalf of minors, another provision devoid of substantive obligations which Congress probably did not intend to make exemptible.[139]

Additionally, the court scrutinized DHS's regulations and determined it was unclear whether they sufficiently exempted the system of records from subsection (g) in the first place.[140] According to regulations, the system of records was "exempted from [subsection (g)] to the extent that the civil remedies may relate to provisions of [the Privacy Act] from which these rules exempt the systems of records, since there should be no civil remedies for failure to comply with provisions from which the Department is exempted."[141] With the scope of this exemption somewhat unclear, the court found the regulation to be ambiguous.[142]

Since it had concluded that DHS's system of records was not exempt from the civil remedies provision, the court vacated the dismissal of Shearson's Privacy Act claims and remanded the case for proceedings in the district court.[143]

IV. DISCUSSION

The Sixth Circuit's interpretation of the law enforcement exemption closes a loophole for government agencies that departs from the original intent of the Privacy Act.[144] The court wisely considered the operation of other provisions to determine the proper function of the law enforcement exemption, rejecting earlier analyses that failed to do so.[145] The court's decision supports private enforcement that the legislature intended as a key component of the Privacy Act.[146] Though the vitality of the private enforcement scheme is in doubt, the court's holding in *Shearson* preserves the core principle that government agencies must answer for failures to maintain records in the manner Congress

138. *See id.*

139. *Id*. at 503–04.

140. *Id.* at 504. The regulations further justified the exemption as "protect[ing] the Department from baseless civil court actions that might hamper its ability to collate, analyze, and disseminate investigative, intelligence, and law enforcement data." *Id.* Presumably, however, not all civil lawsuits will be baseless. To the extent that they may hamper the collection and dissemination of intelligence information, meritorious private lawsuits are the means Congress chose to enforce the Privacy Act. *See* Hong, *supra* note 62, at 103–05.

141. *Id.* (quoting 31 C.F.R. § 1.36(d)(12)).

142. *Id*. at 504–05.

143. *Id*. at 506.

144. *See supra* notes 44, 53.

145. *Shearson*, 638 F.3d at 503–04.

146. *See* Hong, *supra* note 62, at 103.

prescribed.[147]

A. Textual Interpretation

Upon meaningful consideration, a construction of subsection (g) that prevents complete exemption follows well-established principles of textual interpretation. It is axiomatic that the starting point of any statutory interpretation must be the plain language.[148] Acknowledging this principle, the Sixth Circuit observed that subsection (g) is "conspicuously absent" from the list of non-exemptible provisions of the Act.[149] To other courts, this has ended the inquiry—subsection (g) is not on the list, so it must be exemptible.[150] However, an appropriate analysis of subsection (g) must consider its role in the context of the whole statute. Construing only one part of a complex statute could easily lead to illogical results, and such a construction should be avoided.[151] The court observed that subsection (g) is "strictly an enforcement section" that must be interpreted according to its interaction with the substantive duties set forth in the statute.[152] Congress did not include subsection (g) on the list of non-exemptible sections because it does not belong there. Rather, it is meant to enforce numerous substantive duties, some of them mandatory and others subject to the law enforcement exemption.[153]

The Sixth Circuit declined to mention the simplest and strongest rejection of the government's interpretation: the difference between an agency and a system of records.[154] As the D.C. Circuit observed in *Tijerina*, subsection (j) permits an agency to exempt a system of records from most of the Act's requirements, not the agency itself.[155] Subsection (g) provides a civil remedy when an agency fails to comply with certain parts of the Act.[156] This remedy is used to enforce substantive obligations placed upon the agency elsewhere in the Act. Thus, an agency may exempt law enforcement records from subsection

147. *See* S. REP. NO. 93-1183, at 16, *reprinted in* SOURCE BOOK, *supra* note 16, at 169.

148. *Shearson*, 638 F.3d at 500.

149. *Id.* at 502.

150. *See, e.g.*, Alexander v. United States, 787 F.2d 1349, 1351 (9th Cir. 1986).

151. *See* Griffin v. Oceanic Contractors, Inc., 458 U.S. 564, 571 (1982) ("[I]n rare cases the literal application of a statute will produce a result demonstrably at odds with the intentions of its drafters, and those intentions must be controlling.").

152. *Shearson*, 638 F.3d at 503.

153. *Id.*

154. *Compare* Tijerina v. Walters, 821 F.2d 789, 795–96 (D.C. Cir. 1987), *with Shearson*, 638 F.3d at 503–04.

155. *Tijerina*, 821 F.2d at 795–96; *see also* 5 U.S.C. § 552a(j) (2006).

156. 5 U.S.C. § 552a(g) ("Whenever any agency . . . fails to comply with any other provision of this section . . . ."); *see Tijerina*, 821 F.2d at 795–96.

(d)'s provision for individual access rather than attempting to exempt the agency itself from subsection (g)(1)(B)'s enforcement mechanism.[157] This difference reflects Congress's intention that exemptions should be determined by the nature of the database—presumably, a law enforcement agency may maintain systems of records about employment, financial data, or other non-sensitive subjects that are properly regulated by the Privacy Act.[158] Using the exemption procedures cannot provide a basis for an agency to escape all liability under the Privacy Act when the law enforcement exemption protects only certain systems of records.[159] The court should have included this significant textual argument in support of its interpretation.

On the other hand, the court provided two additional arguments based on analogies to other parts of the statute.[160] First, the court rejected the government's argument by analogy that Congress's inclusion of the criminal penalties provision in subsection (j) indicates Congress meant to make subsection (g) exemptible.[161] This argument invokes a traditional canon of statutory construction,[162] suggesting that the inclusion of the criminal penalties provision is instructive to Congress' intent to exclude others. However, as the court wisely observed, Congress needed to include the criminal penalties provision because "there is no other place in [the Act] where conduct is made criminal and subject to penalty."[163] Since subsection (g) enforces the duties that other sections of the Act impose, it would be confusing to place subsection (g) among the non-exemptible provisions.[164] Doing so would circularly create a non-exemptible cause of action against the violation of exemptible duties.[165]

Second, the court made another analogy between the omission of subsection (g) and the omission of subsection (h).[166] Subsection (h)

157. 5 U.S.C. § 552a(d), (g)(1)(B); *see also* Doe v. F.B.I., 936 F.2d at 1351–52.

158. *See* H.R. REP. NO. 93-1416, at 18–19 (1974), *reprinted in* SOURCE BOOK, *supra* note 16, at 311–12.

159. 5 U.S.C. § 552a(j) ("The head of any agency may promulgate rules . . . to exempt any *system of records* within the agency . . . .") (emphasis added).

160. Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 503–04 (6th Cir. 2011).

161. *Id.*

162. The canon *expressio unius est exclusio alterius* holds "that to express or include one thing implies the exclusion of the other, or of the alternative." BLACK'S LAW DICTIONARY (9th ed. 2009); *see also Shearson*, 638 F.3d at 503.

163. *Shearson*, 638 F.3d at 503.

164. *See id.*

165. *See id*. Consider subsection (g)(1)(B), which refers explicitly to an exemptible provision: "Whenever any agency refuses to comply with an individual request under subsection(d)(1) of this section . . . the individual may bring a civil action against the agency . . . ." 5 U.S.C. § 552a(g)(1)(B) (2006).

166. *Shearson*, 638 F.3d at 503–04.

provides "that a guardian may act on behalf of a minor or incapacitated person" in pursuing a Privacy Act claim.[167] It seems unlikely that Congress meant for agencies to exempt their databases from being accessed by legal guardians.[168]

B. Lack of Analysis in Early Cases Interpreting Subsection (g)

The Sixth Circuit appropriately rejected early cases dealing with the law enforcement exemption, since these cases reached a poor conclusion about the meaning of subsection (g) by extending *Ryan*'s initial interpretation without meaningful analysis.[169] To begin with, the Fourth Circuit in *Ryan* mentioned the possibility of total exemption only in *dicta*.[170] The court ultimately found that the government had not followed the procedure to exempt its system of records, making its interpretation of the breadth of such an exemption irrelevant to the holding.[171] In *Alexander*, the Ninth Circuit went further afield by holding that the exemption "expressly prohibits suits against an agency" based on third party disclosure. This was certainly a stretch, considering the Act makes no mention of "prohibiting suits," and the "conditions of disclosure" section of the Act is non-exemptible under subsection (j).[172] Indeed, it is clear from the legislative history that Congress reached a compromise that avoided this type of "blanket exemption."[173] Courts, nonetheless, seem to have accepted this analysis over the years.

To what may continued reliance on these cases be attributed? Perhaps this trend has emerged because plaintiffs have failed to present, effectively, the argument that *Tijerina* and *Shearson* support. Several of the law enforcement exemption cases involve inmates who filed complaints pro se and seemed to find little sympathy with the courts.[174]

---

167. *Id.*

168. *Id.*

169. *See, e.g.*, Alexander v. United States, 787 F.2d 1349, 1351–52 (9th Cir. 1986).

170. Ryan v. Dep't of Justice, 595 F.2d 954, 958 (4th Cir. 1979) ("[T]he Justice Department could have exempted [its system of records] from the application of the 552a(g) civil remedies provisions . . . ."); *see also* Tijerina v. Walters, 821 F.2d 789, 797 (D.C. Cir. 1987) (discussing *Ryan*, 595 F.2d 954).

171. *Ryan*, 595 F.2d at 958.

172. 5 U.S.C. § 552a(j) (2006); *see also* statutory text *supra* note 74.

173. S. REP. NO. 93-1183, at 74, *reprinted in* SOURCE BOOK, *supra* note 16, at 227; H.R. REP. NO. 93-1416, at 18–19, *reprinted in* SOURCE BOOK, *supra* note 16, at 311–12.

174. *See, e.g.*, Kimberlin v. U.S. Dep't of Justice, 788 F.2d 434, 435–36 (7th Cir. 1986) (involving a plaintiff who sued for Privacy Act claims, *Bivens* claims for due process, and a conspiracy claim); Study v. United States, No. 3:08-CV-493/MCR/EMT, 2010 WL 1257655, at *2–3 (N.D. Fla. Mar. 4, 2010), *report and recommendation adopted*, No. 3:08-CV-493/MCR/EMT, 2010 WL 1257654 (N.D. Fla. Mar. 25, 2010) (involving a case in which the plaintiff named more than seventeen defendants and brought several claims including wrongful dissemination, reputational harm, and "pain and humiliation").

Courts in some cases struggled to articulate the causes of action that these plaintiffs presented, sorting meritorious claims out of a heap of allegations against the government.[175] It is easy to imagine that such a claim would not guide the court through the nuances of statutory construction.

Conversely, the plaintiff in *Tijerina*, though also a pro se litigant, was a law student who made very specific and credible allegations of improper disclosure.[176] This type of improper disclosure is one of the quintessential harms that the Privacy Act was aimed at preventing.[177] Indeed, many of the non-exemptible provisions specifically relate to the restrictions on disclosure.[178] Whatever the reason for this inadequacy, courts have spoken of the law enforcement exemption in absolute terms only when they also declined to consider the results of such a construction.[179]

C. Agencies' Recognition of Limits on the Exemption

Agencies themselves support the limited exemption interpretation, as evident from regulations promulgated by DHS and others.[180] While the *Shearson* court acknowledged that DHS's regulations were "ambiguous," the court could have simply interpreted the regulations to mean that the system was only partially exempt.[181] The regulations stated that the TECS database "should be exempt from [subsection (g)] to the extent that the civil remedies may relate to provisions of [the statute] from which these rules exempt the system of records."[182] Though the court found the rule to be unclear, a better reading seems to be that these regulations explicitly limit the exemption to the otherwise exemptible parts of the statute. Indeed, why would such language be included if it were the agencies intention to exempt a system of records from all civil liability?

Unfortunately, courts have similarly failed to hold an agency accountable for its own recognition of limits to the exemption in other cases. In *Ryan*, the court acknowledged that the FBI had justified its

175. *See* cases cited *supra* note 174.

176. Tijerina v. Walters, 821 F.2d 789, 791–93 (D.C. Cir. 1987).

177. *See* S. REP. NO. 93-1183, at 1, *reprinted in* SOURCE BOOK, *supra* note 16, at 154.

178. *See Tijerina*, 821 F.2d at 796.

179. *E.g.*, Kimberlin v. U.S. Dep't of Justice, 788 F.2d 434, 438 n.2 (7th Cir. 1986); Ryan v. Dep't of Justice, 595 F.2d 954, 957–58 (4th Cir. 1979).

180. *See, e.g.*, *Tijerina*, 821 F.2d at 796. Examining the Veterans Administration's regulations, the court concluded, "None of the purposes the VA cited is remotely served by allowing the agency to escape civil liability for violations of the disclosure or accuracy requirements of the Act." *Id.*

181. *See* Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 504–05 (6th Cir. 2011).

182. *See id.* at 504 (quoting 31 C.F.R. § 1.36(d)(12)).

law enforcement exemption with respect to only one provision of the Act (the access provision).[183] Rather than drawing an inference that the agency recognized limits to its own exemption authority, the court instead stated that the FBI could "completely exempt" its system of records.[184] Similarly in *Alexander*, the Ninth Circuit offered no analysis of the regulations exempting another FBI database.[185] Those regulations exempted the database because subsection (g) "concern[ed] an individual's right to access records which concern him [and correct inaccuracies]."[186] While this rationale plainly does not cover all parts of subsection (g), the court nonetheless considered this sufficient to bar all civil claims under the Act.[187] Interpreting the agency regulations so broadly swept away many of the duties deliberately that Congress imposed on agencies[188]

Admittedly, the Sixth Circuit did not have to rely on an interpretation of DHS's regulation to reach its holding.[189] Still, courts need not give agencies the benefit of the doubt concerning their own regulations. Since two viable interpretations of the law enforcement exemption exist, agencies should be on notice that their regulations will be scrutinized. This is particularly true, since there is essentially no incentive for agencies to police themselves.[190]

D. The Need for Private Enforcement

The *Shearson* court, like numerous others, largely avoided a discussion of the policies underlying the Privacy Act by reaching a conclusive holding based on the language of the Act.[191] While this shows a measure of judicial restraint, it does not address the weighty policies underlying Congress's enactment of the Privacy Act or the scheme of enforcement Congress designed.

While the legislative history of the Act is somewhat limited, debate and compromise over the extent of the law enforcement exemption

183. *Ryan*, 595 F.2d at 958.

184. *Ryan*, 595 F.2d at 957–58. The regulations read: "This subsection is inapplicable to *the extent that the system is exempt from other specific sub-sections* of the Privacy Act." *Id*. (emphasis added).

185. Alexander v. United States, 787 F.2d 1349, 1351–52 (9th Cir. 1986).

186. *Id.* at 1351 n.2.

187. *Id.* at 1351–52.

188. *See* discussion *supra* Part II(A).

189. Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 504 (6th Cir. 2011) (finding that the terms of Act itself permitted no such exemption).

190. *See* Hong, *supra* note 62, at 105.

191. *Shearson*, 638 F.3d at 503–04.

shows the balance that Congress sought to strike.[192] The Senate wanted to pass a bill that placed strict limits on agencies and gave strong enforcement powers to citizens and to an independent commission.[193] On the other hand, the House bill nearly cut law enforcement and national security agencies out of the bill entirely.[194] Exemptions in the House bill would have placed vast areas of government data collection out of the reach of individuals.[195] In light of differences between the bills, it is reasonable to conclude that subsection (j) contains a list of substantive duties that both Houses of Congress agreed to impose upon law enforcement agencies.[196]

Moreover, the legislative history shows that Congress intended many of the included provisions to be vindicated through private enforcement.[197] The Act provides a right to access and amend records that Congress designed with a private enforcement scheme in mind.[198] It follows that violations of the duty to maintain accurate and complete records would be enforced similarly. Individuals have the strongest interest to protect their own rights, and compromise on the extent of the privacy rights secured by the Act shows that Congress never agreed to place agencies beyond the reach of private enforcement.[199]

When considering the effectiveness of private enforcement, it is significant that the Supreme Court has placed strict limits on recovery under the Privacy Act.[200] In *Doe v. Chao*, the court narrowed entitlement to the statutory minimum of $1,000 by requiring the plaintiff to prove actual damages.[201] The Act itself imposes an initial limit on damages, which a plaintiff may recover only as the result of a government official's "intentional or willful" conduct.[202] The court found that the legislative history did not support "presumed damages"

192. *Compare* S. REP. NO. 93-1183, at 3, *reprinted in* SOURCE BOOK, *supra* note 16, at 156, *with* H.R. 16373 § 2(i) *reprinted in* SOURCE BOOK, *supra* note 16, at 252–53.

193. *See* S. REP. NO. 93-1183, at 3, *reprinted in* SOURCE BOOK, *supra* note 16, at 156.

194. H.R. 16373 § 2(i), 93rd Cong. (1974) (as introduced), *reprinted in* SOURCE BOOK, *supra* note 16, at 252–53.

195. *See id.*

196. *See* Tijerina v. Walters, 821 F.2d 789, 796 (D.C. Cir. 1987).

197. H.R. REP. 93-1416, at 4, *reprinted in* SOURCE BOOK, *supra* note 16, at 297; S. REP. NO. 93-1183, at 82–83, *reprinted in* SOURCE BOOK, *supra* note 16, at 235–36. The Senate report noted that enforcement by private citizens was "doubly important," since the revised bill no longer included enforcement through a Privacy Commission. *Id.*

198. *See* H.R. REP. 93-1416, at 4, *reprinted in* SOURCE BOOK, *supra* note 16, at 297; S. REP. NO. 93-1183, at 82–83, *reprinted in* SOURCE BOOK, *supra* note 16, at 235–36.

199. *See* Hong, *supra* note 62, at 103–06.

200. *See* Doe v. Chao, 540 U.S. 614, 627 (2004); Kardon, *supra* note 69, at 758–59.

201. *Chao*, 540 U.S at 627.

202. 5 U.S.C. § 552a(g)(4) (2006); *see Chao*, 540 U.S at 620.

for any such intentional or willful violations of the Act.[203] By requiring plaintiffs to prove actual damages, the court further raised what was already a high barrier to private enforcement of the Act.[204]

The high court may be poised to raise the barrier yet again, as it considers the Ninth Circuit's recent decision in *FAA v. Cooper*.[205] In *Cooper*, the Ninth circuit construed the recovery of damages under the Act to include pecuniary and non-pecuniary harms.[206] Other courts have reached the opposite conclusion, finding that damages may be awarded only for pecuniary harms.[207] As the Supreme Court has taken up the question, it may further limit recovery in a way that utterly disables the effectiveness of private enforcement.[208]

E. Other Means of Vindicating Privacy Rights

With the effectiveness of the Privacy Act's civil remedies in serious doubt, it is useful to consider other ways a plaintiff might seek to vindicate privacy rights. In *Shearson*, the plaintiff sought, essentially, declaratory and injunctive relief only.[209] Her objective was to learn the contents of the government databases that led to a "false report" and compel the government to amend them for accuracy and adherence to the terms of the Privacy Act.[210] However, there are numerous other situations where the plaintiff seeks monetary redress as well.[211]

One possibility might lie in state tort law, pursuant to which a plaintiff could seek redress for harms caused by improper record keeping.[212] However, holding the government liable on pure tort theories, such as defamation, is difficult to accomplish.[213] Often in such cases, "the primary damage . . . is mental distress,"[214] which may be difficult to prove. Another possibility might be a Constitutional claim—the drafters of the Privacy Act based their grant of statutory rights on those found in the Constitution.[215] As Senator Ervin noted, the Supreme

203. *Chao*, 540 U.S at 622–23.

204. *See* Kardon, *supra* note 69, at 759; *see also* Hong, *supra* note 62, at 102–03.

205. F.A.A. v. Cooper, 622 F.3d 1016 (9th Cir. 2010), *cert. granted*, 131 S. Ct. 3025 (2011); *see also* Kardon, *supra* note 69, at 766.

206. *Cooper*, 622 F.3d at 1035.

207. *E.g.*, Cooper v. F.A.A., No. C 07-1383 VRW, 2008 WL 8648952, at *12–13 (N.D. Cal. Aug. 22, 2008), *rev'd*, 622 F.3d 1016 (9th Cir. 2010).

208. F.A.A. v. Cooper, 131 S. Ct. 3025 (2011); *see* Kardon, *supra* note 69, at 766–67.

209. Complaint, *supra* note 9.

210. *Id.*

211. *See, e.g.*, Doe v. F.B.I., 936 F.2d 1346, 1348 (D.C. Cir. 1991).

212. *See* Kardon, *supra* note 69, at 741–43.

213. *See id.*

214. *Id.* (quoting Time, Inc. v. Hill, 385 U.S. 374, 385 n.9 (1966)).

215. *See* 120 CONG. REC. 12646 (May 1, 1974) (remarks of Sen. Ervin), *reprinted in* SOURCE

Court has recognized fundamental rights to privacy in numerous circumstances.[216] In *Shearson*, the plaintiff specifically alleged interference with her right to travel,[217] a right that finds support in numerous Supreme Court decisions.[218]

Ultimately, as Congress recognized in 1974, a specific legislative remedy is far superior to these mechanisms.[219] Congress has the ability to consider diverse national interests in determining what privacy restrictions to place upon federal agencies.[220] Leaving the remedies up to state tort regimes could lead to great inconsistency. Because the right to privacy is implied only through certain parts of the Constitution, relying on the Constitution to protect individual privacy of its own force is also problematic.[221]

F. The Balance Between Government Power and Individual Rights

The history of the Privacy Act shows that legislators intended to limit the power of government in specific ways in order to secure important individual rights.[222] By limiting the ways that the government can collect, maintain, and use personal information, the Privacy Act creates a tension between an individual's right to privacy and the government's interests in national security and law enforcement.[223] Congress did not impose these limits lightly; the Act's drafters considered privacy rights to be fundamental and rooted in the Constitution.[224] The Supreme Court has also endorsed the concept of privacy rights arising out of Constitutional principles, whether through the Fourteenth Amendment's protection of liberty,[225] through the First Amendment's broad protection of speech and assembly,[226] or through the history and tradition of our country.[227] Given the importance of such rights, courts have every reason to examine closely any government agency's attempt to escape

BOOK, *supra* note 16, at 3–5; H.R. Rep. 93-1416, at 9, *reprinted in* SOURCE BOOK, *supra* note 16, at 302.

216. *See* 120 CONG. REC. 12646 (May 1, 1974) (remarks of Sen. Ervin), *reprinted in* SOURCE BOOK, *supra* note 16, at 4.

217. Complaint, *supra* note 9, at ¶ 21.

218. *See* Mem'l Hosp. v. Maricopa Cnty., 415 U.S. 250, 282 n.7 (1974).

219. *See* H.R. REP. NO. 93-1416, at 4–10, *reprinted in* SOURCE BOOK, *supra* note 16, at 297–303.

220. *See id.*

221. *See id.* at 10, *reprinted in* SOURCE BOOK, *supra* note 16, at 303.

222. S. REP. NO. 93-1183, at 1, *reprinted in* SOURCE BOOK, *supra* note 16, at 154.

223. Hong, *supra* note 62, at 83–84.

224. H.R. REP. NO. 93-1416, at 9–10, *reprinted in* SOURCE BOOK, *supra* note 16, at 302–03.

225. Roe v. Wade, 410 U.S. 113, 152–53 (1973), *modified on other grounds by* Planned Parenthood v. Casey, 505 U.S. 833 (1992).

226. Griswold v. Connecticut, 381 U.S. 479, 483–84 (1965).

227. Moore v. East Cleveland, 431 U.S. 494, 503–04 (1977).

liability for its misuse of private information.

The increased consolidation of government information gathering indicates that the Privacy Act, in its current form, will not suffice to protect individual rights as Congress originally intended.[228] As a part of ensuring national security after the attacks on 9/11, Congress created DHS and provided for a series of "fusion centers" that consolidate intelligence and law enforcement data.[229] These fusion centers allow for cooperation among national intelligence agencies and local law enforcement.[230] As a side effect, however, these agencies have applied anti-terrorism techniques to domestic law enforcement and created massive databases of shared information, which may often include incorrect or investigative information.[231] Maintaining these centralized databases without mechanisms to ensure the accuracy of records will lead to the deprivations of due process that Congress sought to avoid when it enacted the Privacy Act.[232] These may be the "blacklists" that Congress once feared, which can label a citizen a threat without bringing criminal charges or providing him an opportunity to prove innocence.[233]

V. CONCLUSION

In today's era of staggering technological development, Congress and the courts must each play a role in protecting citizens from the harms our nation feared during the passage of the Privacy Act. Courts should safeguard the Privacy Act's enforcement scheme by refusing to recognize a total exemption for law enforcement agencies. Providing for private enforcement of the Act's substantive obligations is an important part of the statutory scheme Congress designed. Individuals have the strongest incentive to ensure the accuracy and confidentiality of their own records, so allowing private judicial enforcement is an effective way to ensure government compliance.[234] Since limits on damages have already reduced the effectiveness of private enforcement, maintaining at least basic liability for injunctive relief is essential to the continued utility of the Privacy Act.

Ultimately, however, the legislature must act to provide broader protection of privacy rights. Under the current systems, there are too

228. *See* Danielle Keats Citron & Frank Pasquale, *Network Accountability for the Domestic Intelligence Apparatus*, 62 HASTINGS L.J. 1441, 1442–43 (2011).

229. *Id.* at 1442–45.

230. *Id.* at 1448–54.

231. *Id.* at 1460–61.

232. *See* S. REP. NO. 93-1183, at 16, *reprinted in* SOURCE BOOK, *supra* note 16, at 169. For a discussion including recent examples, see Crary, supra note 1.

233. *See* Ervin, *supra* note 20, at 19.

234. *See* Hong, *supra* note 62, at 109–11.

many obstacles preventing a plaintiff from obtaining relief—not only in damages, but also in injunctive relief to correct noncompliance. After Julia Shearson was detained at the U.S. border without any explanation, she only wanted to understand what happened and to correct the government's records about her. As it stands today, the Act seems to appeal only to those who, like Ms. Shearson, are willing to fight a lengthy legal battle simply to access or amend a government record. In some ways, the creation of the centralized DHS has realized the fears that Congress had in 1974, and cases like *Shearson* confirm the risk that inaccurate records may deprive someone of basic guarantees of due process.

There are a number of possible solutions. Congress could expand the damages available and narrow the scope of the law enforcement exemption.[235] This would allow plaintiffs to enforce certain rights effectively, though it would still leave many records inaccessible. Alternatively, plaintiffs might seek other routes to vindicate privacy rights under state law or perhaps under Constitutional theories, though there are a number of problems with these approaches.[236]

The best strategy may be for Congress to create a stronger, centralized administrative system, like the Privacy Protection Commission that the original Senate proposal contemplated.[237] The report from the Committee on Government Operations called for "an independent body of experts charged with protecting individual privacy as a value in government and society."[238] This administrative system would have several advantages, including: (1) complaints could be handled rapidly, (2) the amount of legal fees from litigation could be greatly reduced, (3) plaintiffs would have greater access to equitable relief, (4) the availability of damages could be kept to a minimum, (5) access to sensitive records would be limited to commissioners. An organization like the Privacy Commission would give Congress greater oversight of government agencies and reveal areas of concern. It would allow Congress to restore the original vision of the Privacy Act and renew its vitality in protecting citizens from the perils of unchecked government data collection.

235. *See id.*

236. *See* Kardon, *supra* note 69, at 741–45.

237. S. REP. NO. 93-1183, at 23–27, *reprinted in* SOURCE BOOK, *supra* note 16, at 176–80.

238. *Id.* at 23, *reprinted in* SOURCE BOOK, *supra* note 16, at 176. The Privacy Commission would have been empowered to monitor federal databases, investigate violations of the Act, and develop recommendations for improvements. *Id.* at 23–24, *reprinted in* SOURCE BOOK, *supra* note 16, at 176–77.