Legislation and Policy Brief

Volume 5 | Issue 1 Article 1

2-17-2013

Shearson v. United States Department of Homeland Security: The Sixth Circuit Exempts National Security from the Privacy Act

Douglas A. Behrens
Villanova University School of Law

SHEARSON V. UNITED STATES DEPARTMENT OF HOMELAND SECURITY: THE SIXTH CIRCUIT EXEMPTS NATIONAL SECURITY FROM THE PRIVACY ACT

Douglas A. Behrens*

Flagged at the Border

"ARMED AND DANGEROUS."[1] Imagine those words flashing on a Customs and Border Protection ("CBP") agent's computer screen as you attempt to reenter your country of birth from a relaxing vacation.[2] Reacting to the computerized warning, the CBP agents detain and question you for several hours before you are released from custody—without an explanation—and allowed to continue on your trip home as if nothing had happened.[3]

* Villanova University School of Law, J.D. Candidate 2013; University of Delaware, B.S. 2010. Thanks are due to Professor Todd Aagaard for his helpful comments and editorial advice throughout the writing process. This Article would not have been possible without the love and unwavering support of the author's family.

[1] Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 499 (6th Cir. 2011) (flashing warning on screen of customs agent when Julia Shearson's passport was scanned).

[2] *See generally* Robert L. Smith, *Julia Shearson Tells How a Weekend Trip to Canada Became a 5-Year Fight for Rights*, The Plain Dealer (June 4, 2011, 5:10 PM), http://blog.cleveland.com/metro/2011/06/julia_shearson_tells_how_a_wee.html (providing details of Shearson's vacation).

[3] *See Shearson*, 638 F.3d at 499–500 (presenting similar scenario).

This hypothetical scenario became very real for Julia Shearson and her four-year old daughter in January 2006, and marked the beginning of her quest for answers.[4] Why was she flagged as "ARMED AND DANGEROUS?"[5] What actions had she taken that led the government to classify her in this way?[6] Could she obtain documents held by the Department of Homeland Security ("DHS") and CBP that might indicate why she was detained?[7] What recourse does she have to clear her name?[8]

In addition to Shearson's concern about being misclassified, her situation also raises several national policy questions.[9] What effect would mandatory disclosure requirements of an agency's inner operations have on its ability to protect the United States from threats to national security?[10] Under what circumstances should a federal agency that possesses sensitive information relating to national security be allowed to exempt itself from the disclosure requirements?[11]

These questions highlight the broader issue of establishing equilibrium between personal privacy and national security in the twenty-first century.[12] The notion that people needed to sacrifice some individual freedoms in return for the protection provided by organized society was developed early on in political philosophy.[13] But striking the appropriate societal balance between personal liberties and security has proven to be extremely difficult, and supporters for each have even

---

[4] *See id.* at 499–506 (describing factual background of Shearson's case).

[5] *See infra* note 52 and accompanying text (discussing CBP's claim that Shearson was flagged because of false alert, and her skepticism over this explanation).

[6] *See infra* notes 51–58 and accompanying text (offering potential reasons for Shearson's classification).

[7] *See infra* notes 53–57 and accompanying text (describing Shearson's attempts to obtain these documents under provisions of Privacy Act).

[8] *See* Privacy Act of 1974, 5 U.S.C. § 552a (1974) (providing certain remedies against agency for maintaining inaccurate information about individual).

[9] *See infra* notes 139–41 and accompanying text (discussing over-arching policy concerns involved with tension between individual privacy and national security).

[10] *See* Smith, *supra* note 2 (explaining apprehension on part of government attorneys regarding potential ramifications on national security of requiring agency to disclose information relating to border stops).

[11] *See infra* notes 134–38 and accompanying text (advocating in favor of permitting agencies to utilize general exemptions provision to prevent disclosure of information that could negatively impact national security).

[12] *See* Jennifer Chandler, *Privacy Versus National Security: Clarifying the Trade-off*, *in* Lessons From the Identity Trail: Anonymity, Privacy, and Identity in a Networked Society 121, 121 (Ian Kerr et al. eds., 2009) (acknowledging tension between protecting individual freedoms and maintaining national security in post-9/11 world).

[13] *See id.* at 126 (describing lack of protection in "state of nature" and emergence of social contract in which people voluntarily joined together to form societies and surrendered certain freedoms in exchange for security and protection provided by organized group).

taken to social media sites to advocate for their position.[14] Congress attempted to weigh these two competing considerations in its passage of the Privacy Act of 1974 ("Privacy Act"), which regulated the type of information a federal agency could maintain on an individual, but provided agencies with exemptions from the disclosure requirements for law enforcement activities.[15] The United States has changed dramatically since the Privacy Act's passage though, and several authors have noted that society now tends to give security more weight than personal liberties, especially after the events of September 11, 2001.[16]

This Article argues that the Sixth Circuit Court of Appeals improperly held that Shearson may compel DHS and CBP—a law enforcement branch of the DHS—to disclose documents relating to her detainment under the Privacy Act, and asserts that congressional action is required.[17] Part II provides a general overview of the Privacy Act and the factual background of Shearson's case.[18] Part III surveys other circuit court cases that have wrestled with interpreting the extent of the

---

[14] *See id.* at 127 (analyzing relationship between privacy and security). At one extreme, the survival of societal members is paramount and privacy considerations are secondary, but this could be taken so far that the secure life of those in the society is no longer worth living because they enjoy no liberties, privacy, or other fundamental rights. *See id.* (noting that at other extreme, if absolute privacy is viewed as most important factor, added privacy becomes useless if resulting security level is so minimal that no members of society survive to enjoy it); *see also Personal Privacy*, Facebook (Oct. 2, 2011, 11:36 AM), http://www.facebook.com/pages/Personal-privacy/108220189211921 (recognizing privacy as "right not to be subjected to unsanctioned invasion of privacy by the government, corporations or individuals"); *National Security*, Facebook (Oct. 2, 2011, 11:41 AM), http://www.facebook.com/pages/National-security/112812148732650 (listing use of "intelligence services to detect and defeat or avoid threats and espionage, and to protect classified information" as potential measure to increase national security).

[15] *See generally* Privacy Act of 1974, 5 U.S.C. § 552a (1974) (providing individual privacy protection and agency exemptions); *see also infra* notes 26–45 and accompanying text (discussing requirements of Privacy Act, its structure, and its purpose).

[16] *See* Conor Gearty, *Reflections on Civil Liberties in an Age of Counterterrorism*, 41 Osgoode Hall L.J. 185, 203 (2003) (describing security as "trump of trumps" when weighed against civil and political rights); Peter P. Swire, *Privacy and Information Sharing in the War on Terrorism*, 51 Vill. L. Rev. 951, 955 (2006) (advocating for greater information sharing, and thus less individual privacy, in order to prevent and preempt harm). Several potential reasons for the amount of weight society places on security are: 1) that security is a prerequisite for enjoying other values such as privacy, 2) human risk perception causes people to overestimate the risk of terrorism and underestimate the impact of reduced privacy, and 3) that the burden of reduced privacy is unlikely to affect every member of society equally, whereas the benefits of added security are enjoyed by society as a whole. *See* Chandler, *supra* note 12, at 125–26. Indeed, according to a recent Gallup poll, a clear majority of American citizens approve of sacrificing privacy for increased security. *See* Lymari Morales, *Most U.S. Air Travelers OK Sacrificing Privacy for Security*, Gallup (Nov. 23, 2010), http://www.gallup.com/poll/144920/air-travelers-sacrificing-privacy-security.aspx (reporting that seventy-one percent of people polled indicated that potential loss of privacy from full-body scanners or pat-downs was acceptable as method to prevent acts of terrorism).

[17] *See infra* notes 101–07 and accompanying text (discussing how Sixth Circuit overlooked plain language and structure of Privacy Act in favor of legislative history and purpose). Additionally, the considerable policy implications regarding the national security of the United States weigh against the Sixth Circuit's decision. *See infra* notes 139–46 and accompanying text.

[18] *See infra* notes 23–61 and accompanying text (providing discussion of purpose and structure of Privacy Act, as well as background of Shearson's case).

permissible exemptions under the Privacy Act's general exemptions provision.[19] Part IV of this Article details both parties' positions and summarizes why Shearson's argument persuaded the Sixth Circuit.[20] Part V critically analyzes the Sixth Circuit's reasoning and suggests that the court's holding was improper in light of the Privacy Act's plain language and the likely effects of its decision on national security.[21] Part VI explores the potential implications of the Sixth Circuit's ruling on the future of personal privacy and the national security of the United States.[22]

I. The Privacy Act to the Rescue

The Privacy Act guards against a federal agency's abuse of an individual's privacy by regulating the collection of documents that relate to that person's activities.[23] In order to protect against unlimited information gathering by federal agencies, the Privacy Act attempts to restrain federal agencies in their collection, maintenance, use, and dissemination of information about private individuals.[24] The various provisions and structure of the Privacy Act, however, evince Congress's intent to balance an individual's right to privacy with the need to ensure that federal agencies function effectively.[25]

A. Discerning the Privacy Act's Purpose

The United States Constitution does not provide a general right to privacy, and although Supreme Court precedent has established a privacy right in certain situations, legislative action remains the main avenue for protecting privacy.[26] Congress passed the Privacy Act in response to concerns about the amount of personal information that the government gathered on its citizens and the way in which that sensitive

---

[19] *See infra* notes 62–74 and accompanying text (detailing previous court decisions regarding breadth of general exemptions provision).

[20] *See infra* notes 78–107 and accompanying text (summarizing arguments made by each party and stating Sixth Circuit's holding).

[21] *See infra* notes 108–30 and accompanying text (critiquing Sixth Circuit's analysis).

[22] *See infra* notes 131–46 and accompanying text (examining impact that Sixth Circuit's decision will likely have on national security).

[23] *See* Gregory R. Firehock, *The Increased Invulnerability of Incorrect Records Maintained by Law Enforcement Agencies:* Doe v. FBI, 60 Geo. Wash. L. Rev. 1509, 1510–11 (1991) (noting that Privacy Act protects against abuse of privacy rights by federal government).

[24] *See id.* at 1511 (discussing Privacy Act's methods of safeguarding informational privacy rights).

[25] *See id.* at 1512–13 (illustrating competing factors that Congress weighed in drafting Privacy Act).

[26] *See, e.g.*, Lawrence v. Texas, 539 U.S. 558 (2003) (recognizing right to intimate, consensual sexual conduct); Roe v. Wade, 410 U.S. 113 (1973) (stating that right to abortion is included within general right to privacy); Griswold v. Connecticut, 381 U.S. 479 (1965) (establishing right to sexual privacy within marital relationship); *see also* Firehock, *supra* note 23, at 1545 n.6 (explaining that statutes, not Constitution, regulate agency's system of records).

information was being handled.[27] In fact, many people believe that the well-publicized informational abuses that took place during the infamous Watergate scandal prompted Congress to act.[28]

In the Privacy Act's Congressional Findings and Statement of Purpose section, Congress explicitly acknowledged the perils that inappropriate use of personal information presents to individuals in an increasingly technological age.[29] The advent of computers and developments in technology made storing and organizing massive amounts of personal information in an agency's system of records easier than ever before.[30] In drafting the Privacy Act, however, Congress balanced the need to protect individual privacy with the concern that absolute informational rights may obstruct a federal agency's

---

[27] *See* Larie A. Doherty, *Privacy Act*, 56 Geo. Wash. L. Rev. 1028, 1028–29 (1987) (explaining that Privacy Act was intended to prevent invasions of privacy resulting from federal agency misusing personal information); Kirsten L. Peters, *Freedom of Information Act/Privacy Act*, 65 Geo. Wash. L. Rev. 792, 793–94 (1997) (commenting that goal of Privacy Act was to calm apprehension about extent of personal information kept by various federal agencies).

[28] *See* Privacy Act of 1974, Pub. L. No. 93-579 (1974), *reprinted in* Joint Comm. on Gov't Operations, 94th Cong., Legislative History of the Privacy Act of 1974, at 4 (1976), *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf [hereinafter Legislative History of the Privacy Act] (stating that Watergate scandal taught Americans that there must be limits on what government can know about each citizen). "Each time we give up a bit of information about ourselves to the Government, we give up some of our freedom. For the more the Government or any institution knows about us, the more power it has over us." *See id.* (explaining that when government knows all of our secrets, "we stand naked before official power" and lose our rights and privileges).

[29] The Congressional Findings and Statement of Purpose, enacted as a part of the Privacy Act but not codified, explain Congress' concerns that led to passage of the Privacy Act:

> (1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by federal agencies;
>
> (2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;
>
> (3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;
>
> (4) the right to privacy is a personal and fundamental right protected by the constitution of the United States; and
>
> (5) in order to protect the privacy of individuals identified in information systems maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

Privacy Act of 1974, Pub. L. No. 93-579 § 2(a), 88 Stat. 1896, 1896 (1974).

[30] *See id.* § 2(a)(2) (citing increased use of computers and sophisticated information technology as magnifying harm to individual privacy); *see also* 5 U.S.C. § 552a(5) (1974) (defining "system of records" as "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").

ability to perform certain functions relating to law enforcement and national security.[31]

B. The Privacy Act's Complicated Structure

The Privacy Act is comprised of multiple sections, including provisions that regulate the disclosure and access to a system of records, the civil and criminal remedies available to an aggrieved citizen, and the possible exemptions available to an agency.[32] Of particular importance to Shearson's case are subsections (b), (d), (e), (g), (i), and (j).[33] Subsection (b) regulates the conditions for disclosure of records by an agency, and limits an agency's ability to disseminate information to certain scenarios.[34] Agencies must account for these information disclosures under subsection (c), which requires the date, nature, and purpose of any disclosure, in addition to the name and address of the person receiving the disclosure.[35]

---

[31] *See* Privacy Act of 1974, Pub. L. No. 93-579 § 2(b)(5), 88 Stat. 1896 (1974) (stating that purpose of Privacy Act is to provide safeguards for individuals from abuse of information by federal agencies, but also recognizing need to permit agency exemptions from requirements in cases where important public policy need for such exemption exists); *see also* Legislative History of the Privacy Act, *supra* note 28, at 297 (noting need to balance fundamental and conflicting needs of "individual American for a maximum degree of privacy over personal information he furnishes his government, and on the other, that of the government for information about the individual which it finds necessary to carry out its legitimate functions"). It also recognized that the government has a right to collect certain information, and that exemptions need to be available for agencies to protect information that is highly confidential. *Id.* at 296 (explaining legitimate need of government to collect, store, use, and share certain types of personal data, in addition to realizing that "certain areas of Federal records are of such a highly sensitive nature that they must be exempted from some of its provisions").

[32] *See generally* § 552a (establishing certain controls on data use by federal agencies).

[33] *See id.* (listing various provisions relating to collection, use, access, and potential exemptions for data under Privacy Act).

[34] The Privacy Act states, in relevant part, that "no agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency" except pursuant to a written request by the individual to whom the record pertains, unless the disclosure would be:

> (1) to those officers and employees of the agency which maintains records who have a need for the record in the performance of their duties;
>
> (2) required under section 552 of this title; . . .
>
> (5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record . . . ;
>
> (7) to another agency . . . ;
>
> (9) to either house of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee; . . .
>
> (11) pursuant to the order of a court of competent jurisdiction.

Id. §§ 552a(b)(1)-(11).

[35] *See id.* § 552a(c) (illustrating accounting requirements for disclosures under subsection (b) with exception that no accounting is required for disclosures made under subsections (b)(1) and (b)(2)).

Subsection (d) grants an individual the right to access her records and to request an amendment of her records if she believes them to be inaccurate, but also clearly indicates that individuals will not be allowed to access information collected in reasonable anticipation of a civil action against that person.[36] The amount and type of information that an agency can maintain on an individual is regulated by subsection (e).[37] Subsection (e)(7)—which requires that no agency maintain a record pertaining to an individual's exercise of her First Amendment rights unless that record is pertinent to law enforcement activity—is particularly relevant to Shearson's case.[38]

The Privacy Act also has two enforcement provisions: the civil remedies provision, subsection (g), and the criminal penalties provision, subsection (i).[39] The civil remedies provision grants district courts jurisdiction to hear civil suits brought by any individual who is harmed by an agency that failed to allow access to her records or refused a request to amend her records—violations that are enumerated in other sections

---

[36] Subsection (d) provides individuals with both access and restrictions to records pertaining to themselves by stating, in relevant part, that each agency that maintains a system of records shall:

> (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence;
>
> (2) permit the individual to request amendment of a record pertaining to him and . . .
>
> (B) promptly, either--
>
> (i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or
>
> (ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official . . . ;
>
> (5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

Id. § 552a(d).

[37] *See id.* § 552a(e) (asserting that agency shall maintain in its records only information about individual that is relevant and necessary to accomplish agency's purpose as required by statute or executive order by President). Agencies are also required to publish the existence and character of any new or revised system of records in the Federal Register, and shall maintain those records with the accuracy, relevance, timeliness, and completeness reasonably necessary to assure fairness to an individual. *See id.* § 552a(e)(4), (5).

[38] *See id.* § 552a(e)(7) (stating that agencies shall not maintain any record describing any individual's exercise of rights guaranteed by First Amendment unless expressly authorized by statute, or unless pertinent to and within scope of authorized law enforcement activity); *see also infra* notes 105–07 (discussing Sixth Circuit's holding that subsection (e)(7) was one of two subsections pursuant to which Shearson was entitled to disclosure of documents held by DHS and CBP).

[39] *See* § 552a(g), (i) (listing two methods under Privacy Act through which individuals may enforce privacy rights against federal agency).

of the Privacy Act.[40] The criminal penalties provision allows criminal sanctions against agency employees who willfully disclose information in violation of the Privacy Act, against agency employees who willfully maintain records in violation of the Privacy Act, and against any person who willfully obtains a record concerning another individual under false pretenses.[41]

Finally, the general exemptions provision, subsection (j), permits the head of an agency to promulgate rules exempting a system of records from certain provisions of the Privacy Act as long as the system

---

[40] The civil remedies provision provides, in relevant part, that whenever an agency:

> (1)(a) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection; [or]
>
> (1)(b) refuses to comply with an individual request under subsection (d)(1) of this section . . . ;
>
> the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in matters under the provisions of this subsection.
>
> (2)(a) In any suit brought under the provision of subsection (g)(1)(a) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. . . .
>
> (3)(a) In any suit brought under the provision of subsection (g)(1)(b) of this section, the court may enjoin the agency from withholding the records and order the production to the complaintant of any agency records improperly withheld from him.

Id. § 552a(g).

[41] The criminal penalties provision provides that:

> (1) Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than $5,000.
>
> (2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than $5,000.

Id. § 552a(i).

of records meets one of the criteria set out in subsections (j)(2)(A)-(C).[42] The agency must also provide a reason in the promulgated rule explaining why the system of records is being exempted from any provision in the Privacy Act.[43] There are, however, several non-exemptible provisions from which an agency may not exempt its system of records.[44] The non-exemptible provisions include the criminal penalties provision, but significantly, the civil remedies provision is not included in that list.[45]

C. A Stressful Ending to the Family Vacation

Julia Shearson is a United States citizen, a Muslim, and an outspoken advocate for Muslim rights—as evidenced by her position as

---

[42] The general exemptions provision, in relevant part, provides that:

> 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 police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.
>
> At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this subsection.

Id. § 552a(j).

[43] *See id.* (noting steps agency must take in order to exempt system of records from provisions of Privacy Act).

[44] *See id.* (listing fourteen provisions for which agency may not use general exemptions provision to exempt its system of records from Privacy Act requirements); *see also supra* note 42 (providing text of subsection (j)).

[45] *See* § 552a(j) (stating that following subsections are non-exemptible: subsection (b) which prohibits disclosure of personal information except under certain conditions; subsections (c)(1) and (2) which regulate maintenance of records and their disclosures; subsections (e)(4)(A) through (F), which mandate that agencies publish in Federal Register certain characteristics of each system of records maintained by agency; subsection (e)(6) which requires agencies to use reasonable efforts to ensure accuracy and completeness of information prior to disclosure; subsection (e)(7) which prohibits agencies from maintaining any records relating to individual's exercise of First Amendment rights; subsection (e)(9) which mandates that agencies develop rules of conduct for personnel who maintain any system of records; subsection (e)(10) which requires agency implemented safeguards to protect integrity of any system of records; and subsection (i) which provides criminal liability for violation of certain sections of Privacy Act). The criminal penalties provision, but not the civil remedies provision, is listed as a non-exemptible under general exemptions provision. *See id.*

a Director of the Cleveland Council on American-Islamic Relations ("CAIR").[46] As she was driving home with her four-year old daughter from a weekend trip to Canada on January 2, 2006, they were stopped at the U.S. border for a routine border stop.[47] When their U.S. passports were scanned, the CBP computer flashed the words "ARMED AND DANGEROUS."[48] Shearson and her daughter were detained several hours for questioning and were later released without any explanation, despite Shearson's repeated requests for information about why she was held.[49] As Shearson was leaving, she inquired as to whether a search of her vehicle had been conducted, and she was assured by CBP agents that no search had occurred.[50]

Shearson then reached out to her congressional representatives for help, and after they also failed to gain traction with the CBP, she submitted information requests to DHS and CBP under several sections of the Privacy Act.[51] CBP searched the Treasury Enforcement Communications System ("TECS"), its system of records, and provided Shearson with nine pages of highly redacted documents, but several unredacted sentences indicated that Shearson had been included

[46] *See* Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 499 (6th Cir. 2011) (stating that Shearson was resident of Northern District of Ohio and worked as regional office director for Cleveland division of non-profit Muslim civil rights organization called CAIR).

[47] *See id.* (illustrating events leading up to Shearson's lawsuit).

[48] *See id.* (explaining why Shearson and her daughter were detained and questioned).

[49] *See id.* at 499–500 (describing facts of case).

[50] *See id.* at 499 (noting that Shearson later realized, based on documents describing her detainment, that her car had been searched by CBP agents while she was being questioned).

[51] *See* Smith, *supra* note 2 (explaining that day after she was stopped for questioning, Shearson wrote letters to two United States senators from Ohio and United States representative for her township asking them to assist her in obtaining information from CBP regarding her border encounter and they agreed). The CBP, however, responded to the Congressmen's queries with a memo refusing to divulge the requested documents and indicating that Shearson was stopped because of a "false alert" caused by a computer mistake. *See id.* Shearson issued information requests to the DHS and CBP under sections 552a(b), (d), (e)(1), (e)(4), (e)(5), and (e)(7) of the Privacy Act. *See Shearson*, 638 F.3d at 499–500 (describing Shearson's effort to uncover answers about her detainment).

on a terrorist watch list.[52] At some point after the initial search, CBP performed a second search of its system of records and uncovered three more documents.[53] CBP, however, withheld these new documents in their entirety.[54] Outraged that she had been deemed a terrorist threat, Shearson initiated an administrative appeal and requested that all information relating to the border stop be reissued in full.[55]

After several weeks without progress on her administrative appeal, Shearson became frustrated and sought relief through the legal system.[56] She filed a complaint pro se and an amended complaint pro se, on June 15, 2006 and August 23, 2006, respectively, seeking a declaration that DHS and CBP's refusal to provide unredacted records, access to documentation, and amendment of erroneous information violated the Privacy Act.[57] Her amended complaint alleged that the agency did not take reasonable efforts to ensure the accuracy of her records, illegally maintained records relating to her First Amendment activity, and did not properly account for certain disclosures of personal information.[58]

The district court granted the agency's summary judgment motion and dismissed Shearson's Privacy Act claims.[59] The court concluded that even though sections (b) and (e) were non-exemptible under subsection (j), the court lacked jurisdiction to hear Shearson's claims under those provisions because the agency stripped the court of jurisdiction to hear civil complaints by exempting its system of records from the

---

[52] *See Shearson*, 638 F.3d at 499 n.1 (describing TECS as computerized system containing information from variety of federal, state, and local sources); *see also* Smith, *supra* note 2 (discussing contents of redacted documents given to Shearson). Several words and phrases included in the documents that were not redacted were "pertaining to terrorism" and Shearson's "TSC" number, or Terrorist Screening Center ID number. *See id.* (indicating how Shearson realized that she had been included on terror watch list).

A retired FBI agent who specialized in terror financing indicated that combinations of several activities, whether it be travel, financial activity, or internet use, can cause suspicion and land a person on the terror watch list. *See id.* (explaining possible activities that may have caused DHS and CBP to flag Shearson as potential threat to national security). Interestingly, the FBI has no formal relationship with CAIR, which dates back to 2009 when FBI agents investigated CAIR's national leaders' links to Hamas, a group that has been designated by the United States as a terror organization. *See id.* (noting CAIR's checkered past, CAIR's insistence that it has no ties to terrorism, and Shearson's belief that her role in CAIR did not play any part in her being placed on terrorist watch list because other more prominent members of group have been able to travel freely). In addition to Shearson's leadership position in CAIR, the father of her daughter currently resides in Saudi Arabia. *See id.* (establishing another possible but, according to Shearson, unlikely reason for her inclusion on terror watch list).

[53] *See Shearson*, 638 F.3d at 500 (explaining factual background).

[54] *See id.* (describing facts leading up to Shearson's lawsuit against DHS and CBP).

[55] *See id.* (detailing administrative appeal filed by Shearson on April 21, 2006).

[56] *See id.*

[57] *See id.*

[58] *See Shearson*, 638 F.3d at 500 (stating alleged Privacy Act violations committed by defendants in plaintiff's legal complaint).

[59] *See id.*

civil remedies provision.[60] Shearson then appealed her case to the Sixth Circuit Court of Appeals.[61]

II. Navigating a Circuit Split: The Breadth of the Privacy Act's General Exemptions Provision Has Deeply Divided the Federal Courts

The circuit courts are split regarding whether the Privacy Act's general exemptions provision permits a federal agency to exempt its system of records from the civil remedies provision and thus avoid all civil liability, even for violations of non-exemptible provisions.[62] Two decisions from the United States Court of Appeals for the District of Columbia have held that a federal agency cannot evade liability for violations of non-exemptible provisions by using the general exemptions provision to exempt its system of records from the civil remedies provision.[63] In *Tijerina v. Walters*,[64] the D.C. Circuit reasoned that allowing the Administrator of Veteran's Affairs ("VA") to use the general exemptions provision to exempt itself from the civil remedies provision "would give agencies license to defang completely the strict limitations on disclosure that Congress intended to impose."[65]

---

[60] *See id.* (holding that defendant's exemption of its system of records from civil remedies provision barred plaintiff's claims); *see also* Shearson v. U.S. Dep't of Homeland Sec., No. 06-1478, 2007 U.S. Dist. LEXIS 16902, at *42 (N.D. Ohio Mar. 9, 2007) (stating that TECS system of records was properly exempted under subsection (j)), *vacated*, 638 F.3d 498 (6th Cir. 2011). According to the district court, the CBP is a law enforcement agency, and thus clearly fell within the exemption provided by subsection (j)(2) of the Privacy Act for law enforcement activities. *See id.*

[61] *See Shearson*, 638 F.3d at 499.

[62] *See id.* at 502–03 (noting circuit split on this issue).

[63] *See infra* notes 64–69 (describing narrow interpretation of general exemptions provision applied by several courts).

[64] 821 F.2d 789 (D.C. Cir. 1987).

[65] *Id.* at 797 (noting court's reasoning). In *Tijerina*, Mr. Tijerina sued the VA for disclosing personal information via an unsolicited letter to the Texas Board of Law Examiners without his consent and in violation of the Privacy Act. *See id.* at 791–93 (explaining that VA learned that Mr. Tijerina, current law student, had falsified document in connection with VA guaranteed home loan, realized that Mr. Tijerina intended to sit for Texas bar examination, and then sent unsolicited letter to Texas Board of Law Examiners detailing results of its investigation into Mr. Tijerina). The VA responded that it had used the general exemptions provision to exempt its system of records from the civil remedies provision, and therefore the plaintiff could not sue the agency in a civil action for its disclosure. *See id.* at 795 (describing court's rejection of VA's argument because "agency's efforts to elude civil liability for violations of statutory duties which cannot be shirked under the Act contravene the language of the Act and the purpose behind the general exemptions provision").

In support of this conclusion, the court emphasized that the general exemptions provision permits an agency to exempt a "system of records" from the requirements of the Privacy Act, and that the civil remedies provision is directed towards courts and aggrieved individuals, not systems of records. *See id.* at 795–96 (reasoning that it "simply makes no sense for an agency to use subsection (j) to exempt a system of records from civil liability: records are not subject to civil liability under the Act; the United States is"). Additionally, the court observed that the general exemptions provision was intended to permit the government to withhold access to information, not to permit agencies to avoid liability for irresponsible disclosure. *See id.* at 796.

The court suggested, however, that the exemption of some systems of records under the Privacy Act was justified because they related to law enforcement activities that required a certain amount of secrecy.[66]

Four years later, the D.C. Circuit clarified *Tijerina* in the dicta of *Doe v. Federal Bureau of Investigation*, and stated that, "the touchstone for an agency's liability to suit under the Act is the substantive obligation underlying the plaintiff's claim."[67] Together, these two decisions stand for the proposition that an agency can exempt its system of records from the civil remedies provision only to the extent that the substantive provision that has been violated is also exemptible under the general exemptions provision.[68]

A divergent line of federal appellate and district court opinions has held that a federal agency can use the general exemptions provision to entirely exempt a system of records from the civil remedies provision.[69] In *Ryan v. U.S. Department of Justice*, the Fourth Circuit held that the general exemptions provision permits an agency to exempt its system of records from the civil remedies provision if the proper rules have been promulgated by the agency.[70] Similarly, the Seventh Circuit explained in *Kimberlin v. U.S. Department of Justice* that systems of records can be exempted from the civil remedies provision pursuant

---

[66] *Tijerina*, 821 F.2d at 796 (noting that broad language of general exemptions provision was acceptable because certain records contain particularly sensitive information that cannot be released).

[67] 936 F.2d 1346, 1352 (D.C. Cir. 1991) (holding that agency cannot escape liability for violating non-exemptible Privacy Act obligations by exempting its system of records from Privacy Act's civil remedies provision).

[68] *See supra* notes 64–67 (describing narrow interpretation of general exemptions provision taken by these two courts).

[69] *See infra* notes 70–74 (discussing broad interpretation of general exemptions provision that several courts have adopted).

[70] 595 F.2d 954, 958 (4th Cir. 1979) (explaining that agency may use general exemptions provision to exempt its system of records from civil remedies provision as long as agency follows proper steps). In *Ryan*, the plaintiff, a security officer for the FBI, requested a memorandum from the Justice Department that he alleged dealt with the removal, insulation, and reassignment of official actions he had taken with respect to an investigation of surreptitious entries by FBI agents. *See id.* at 955–56. After the plaintiff commenced his action, a Justice Department attorney told the Washington Post that the requested document said that the plaintiff was "getting in the way of investigations," and the plaintiff responded by amending his complaint to include a claim for wrongful disclosure under the Privacy Act. *See id.* (discussing events leading to plaintiff's wrongful disclosure claim under Privacy Act).

The Justice Department asserted that the plaintiff lacked a cause of action because the Justice Department had exempted its system of records from the civil remedies provision pursuant to the general exemptions provision. *See id.* The court agreed that agencies can avoid civil liability for violations of the Privacy Act by utilizing the general exemptions provision to exempt its system of records from the civil remedies provision, but that the Justice Department had failed to follow the correct procedures in this case. *See id.* at 956–58 (stating court's reasoning that Justice Department could have exempted its system of records from civil remedies provision had agency not failed to state its reasons for exemption).

to the general exemptions provision, but that the Department of Justice failed to abide by the necessary exemption procedures.[71]

Lastly, in *Alexander v. United States*, the Ninth Circuit held that the plaintiff's claims against the FBI for passing inaccurate information to a third party were barred.[72] In that case, the Department of Justice properly promulgated rules pursuant to the general exemptions provision and successfully exempted its system of records from the civil remedies provision.[73] These cases advance the notion that, if an agency follows the prescribed administrative procedures, it can utilize the general exemptions provision to exempt its system of records from any

[71] 788 F.2d 434, 436 (7th Cir. 1986) (noting court's holding that system of records can be exempted from civil remedies provision pursuant to general exemptions provision if required procedures are followed). The plaintiff in *Kimberlin* was convicted for detonating an explosive device, and Ms. DeLong subsequently won a civil judgment against the plaintiff for injuries to her husband that were caused by the explosion. *See id.* Thomas Gahl, the plaintiff's probation officer, sent a letter to the warden of plaintiff's jail to inform him of the civil judgment, and Patrick Leddy, the plaintiff's prison case manager, informed Gahl that the plaintiff regularly sent money from his prisoner commissary account to an individual outside the prison. *See id.* (providing background that led to DeLong obtaining writ of attachment against plaintiff's commissary account, and plaintiff's response that Leddy violated Privacy Act by disclosing his personal information). In the course of its analysis, the court noted that a system can be exempted from the civil remedies provision according to the general exemptions provision, but that the exemption did not apply in this case because the Justice Department neglected to provide a reason for the exemption. *See id.* at 436 n.2 (citing Kimberlin v. U.S. Dep't of Justice, 605 F. Supp. 79, 82 (N.D. Ill. 1985)) (stating that only reason given for exemption was that records are exempt from subsection (d), which only relates to record access, and not to disclosure of those records to third parties which is at issue here).

[72] 787 F.2d 1349, 1351–52 (9th Cir. 1986) (expressing court's holding that general exemptions provision of Privacy Act permitted agency to exempt its system of records from civil remedies provision).

[73] *See id.* (explaining reasoning for court's holding). In *Alexander*, the plaintiff was conditionally hired as a security officer pending a background check from the FBI. *See id.* at 1350. The FBI sent the plaintiff's employer his "rap sheet" which contained information that resulted in the termination of the plaintiff's employment. *See id.* (describing events leading to plaintiff filing suit against government for negligence in failing to remove information on two previous arrests from his record that he believed California court had expunged). The court held that the plaintiff had no cause of action because the Department of Justice had properly exempted its system of records from the civil remedies provision. *See id.* at 1351–52; *see also* Pagani-Gallego v. Sabol, No. 07-40016-PBS, 2008 WL 886032, at *6 (D. Mass. Mar. 27, 2008) (holding that plaintiff's cause of action was barred because Bureau of Prisons ("BOP") properly exempted its system of records from civil remedies provision of Privacy Act pursuant to general exemptions provision). In *Pagani-Gallego*, the plaintiff, a prisoner, was investigated for his possible participation in a suspected prison escape plot involving a helicopter. *See id.* at *1. Despite the fact that officials determined there was insufficient evidence to discipline the plaintiff, his security management variable was increased and this prevented him from being transferred to a lesser security facility. *See id.* (describing impetus for plaintiff's Privacy Act claim). The court held, however, that the plaintiff's claims for access to and amendment of his records were ineffective because of the BOP's use of the general exemptions provision to exempt its system of records from the civil remedies provision. *See id.* at *6; Robinson v. Vazquez, No. CV207-082, 2007 WL 4209370, at *1 (S.D. Ga. Nov. 26, 2007) (noting that, despite availability of relief under civil remedies provision, general exemptions provision permits agency to establish regulations to exempt system of records from requirements of Privacy Act).

subsection of the Privacy Act that is not explicitly listed as non-exemptible in subsection (j).[74]

III. The Sixth Circuit Untangles Each Party's Arguments

The parties articulated statutory interpretations of the Privacy Act that were diametrically opposed.[75] Both parties relied on the Privacy Act's legislative history and purpose to bolster their statutory interpretations.[76] After weighing all of the evidence, the Sixth Circuit sided with Shearson and held that the statutory language and purpose of the Privacy Act would be contravened if DHS and CBP were permitted to entirely exempt their systems of records from the civil remedies provision.[77]

A. A Federal Agency May Not Exempt Its System of Records from the Civil Remedies Provision

Shearson cited the purpose and legislative history of the Privacy Act to support her position that a federal agency cannot exempt its system of records from the civil remedies provision through the general exemptions provision.[78] Shearson argued that the Privacy Act's creation was prompted by the privacy abuses that took place during the Watergate scandal and the government's desire to mend the public's general perception that federal officials were disregarding fundamental privacy rights.[79] With this as a backdrop for the legislation, Shearson contended it logically followed that Congress entrusted plaintiffs who were seeking civil remedies in court, and not the government itself,

---

[74] *See supra* notes 70–73 (discussing broad interpretation of general exemptions provision).

[75] *See* Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 502 (6th Cir. 2011) (laying out Shearson's position that agency cannot exempt its system of records from subsection (g) pursuant to subsection (j), and defendants' argument that all of Shearson's claims are barred because its system of records was properly exempted from subsection (g)); *see also infra* notes 78–100 (discussing statutory arguments made by parties in detail).

[76] *See Shearson*, 638 F.3d at 502–05 (recognizing arguments made by parties in support of statutory interpretation).

[77] *See id.* at 502–04 (detailing court's analysis of case and reasons for decision in favor of Shearson).

[78] *See infra* notes 82–96 (laying out framework for plaintiff's argument).

[79] *See* Nakash v. U.S. Dep't of Justice, 708 F. Supp. 1354, 1359–60 (S.D.N.Y. 1988) ("Privacy Act was a product of the post-Watergate reform era and represented an effort by the Congress to begin to control the collection and dissemination of information about individuals by the federal government."). The court also noted that Representative Moorhead, who presented the House Bill, explained that Americans wanted more government credibility and the removal of any undue governmental power that could be used to invade an individual's personal privacy. *See id.* at 1359; *see also* Privacy Act of 1974, Pub. L. No. 93-579 § 2(a), 88 Stat. 1896, 1896 (1974) (mentioning growing concern over government's accumulation, use, and dissemination of personal information as impetus for Privacy Act).

to ensure accountability for Privacy Act violations.[80] Consistent with this interpretation, Shearson insisted that the inclusion of the criminal penalties provision—and not the civil remedies provision—among the list of non-exemptible provisions was insignificant and misleading because the criminal penalties provision was added amidst confusion at the last minute as a technical amendment.[81]

According to Shearson, the list of non-exemptible provisions proved Congress's intent that federal agencies be subject to the liability created by these subsections, and that the civil remedies provision be used to enforce them.[82] Additionally, Shearson asserted that the agency's interpretation that it can exempt its system of records from any provision except those specifically listed as non-exemptible is untenable because it would flout the Privacy Act's purpose and could lead to absurd results.[83]

Shearson then turned to the legislative history to support her interpretation of the Privacy Act.[84] Shearson alleged that nothing in the legislative history of the Privacy Act indicated that Congress intended to allow agencies to exempt themselves from the civil remedies provision.[85] Shearson also relied on comments in the legislative history that exhibited a congressional desire to provide citizens with recourse to

---

[80] *See* Petitioner's Brief Submitted Pro Se at 17, Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498 (6th Cir. 2011) (No. 08-4582) (arguing that lack of ability by government to regulate itself in past spurred creation of Privacy Act, and that civil remedies provision was included to ensure government credibility with respect to personal information stored by agencies).

[81] *See Nakash*, 708 F. Supp. at 1363–64 (suggesting that criminal penalties provision was added to close "perceived but nonexistent loophole"). The court goes on to note that a significant amount of the Privacy Act's drafting occurred in the commotion of the closing days of the congressional session, and that one of the Privacy Act's sponsors admitted that the legislation was "far from perfect." *See id.* at 1364 (declaring that "relatively little weight can be given to the last-minute and largely inexplicable addition of subsection (i) to the list of exclusions in the general exemption provision"); *see also* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 22–26 (stating that general exemptions provision was poorly drafted and that court must look to Privacy Act's purpose and legislative history to address this deficiency).

[82] *See* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 2 (stating that without civil remedies, agencies are not liable for violations of any subsection of Privacy Act, even those that Congress explicitly listed as non-exemptible); *see also* Tijerina v. Walters, 821 F.2d 789, 793–94 (D.C. Cir. 1987) (explaining that "[t]he principal enforcement mechanism for individuals whose rights under the Privacy Act have been violated is the provision for civil remedies contained in subsection (g)").

[83] *See* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 21–22 (noting that allowing federal agency to exempt its system of records from any subsection not listed as non-exemptible defeats Privacy Act's purpose of ensuring government accountability). The plaintiff also pointed out that the definitions section, subsection (a), is not listed as a non-exemptible provision, and that a federal agency could theoretically exempt its system of records from that provision as well. *See id.*

[84] *See infra* notes 85–86.

[85] *See Nakash*, 708 F. Supp. at 1360 (noting lack of indication that either House or Senate even considered allowing agencies to exempt their system of records from civil remedies provision as compelling reason not to construe Privacy Act in manner that permits it to occur); *see also Tijerina*, 821 F.2d at 797 (explaining court's discomfort with notion that Congress forbade agencies to violate Privacy Act provisions, but yet intended for agencies to be able to evade civil liability for those violations).

defend against Privacy Act violations.[86] Furthermore, Shearson claimed that even if the Privacy Act's purpose and legislative history supported the government's argument, it would be a moot point because the DHS failed to properly exempt its system of records from the Privacy Act's requirements.[87] Shearson argued that the DHS's attempt to exempt its system of records under the general exemptions provision of the Privacy Act failed because its rule promulgation was limited to a notice of proposed rule-making, and a final rule was never promulgated.[88]

Moreover, even if the rule promulgation did satisfy the Privacy Act's requirements, Shearson contended that the DHS's exemption did not bar her claims.[89] The rules promulgated by the DHS and CBP only exempted the system of records from the civil remedies provision to the extent that the system of records was exempt from other provisions of the Privacy Act.[90] The system of records was not exempt from the fourteen non-exemptible provisions listed under subsection (j), including subsections (b) and (e) under which Shearson sued the agencies, and therefore she alleged that she could still receive a remedy for the violation.[91] Finally, Shearson asserted that the Automated Targeting System ("ATS"), a subsystem of the TECS system of records, did not meet any of the law enforcement exemption criteria set out in section 552a(j)(2)(A)–(C).[92]

---

[86] *See* Legislative History of the Privacy Act, *supra* note 28, at 235 (mentioning grant of authority to citizens to protect against Privacy Act violations through civil suits).

[87] *See infra* notes 88–92 (discussing exemption procedures under subsection (j) for system of records).

[88] *See* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 26–28 (asserting that notice is legally insufficient to satisfy general exemptions clause's requirement that agencies "promulgate rules" to avail itself of any exemptions); *see also* Privacy Act of 1974, 5 U.S.C. § 552a(j) (1974) (stating requirements agency must follow in order to exempt system of records).

[89] *See* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 28–29 (arguing that exempting language used by agency was insufficient to exempt its system of records from subsection (g)); *see also infra* notes 90–92 (fleshing out Shearson's position).

[90] *See* Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System, 72 Fed. Reg. 43,567, 43,569 (Aug. 6, 2007) (to be codified at 6 C.F.R. pt. 5) (exempting system of records "[f] rom subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act").

[91] *See* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 28–29 (alleging that, because subsections (b) and (e)(7) were listed as non-exemptible provisions, exempting subsection (g) "to the extent that the system is exempt from other specific subsections" meant that civil liability was still available for violation of subsections (b) and (e)(7)).

[92] *See id.* at 29–34 (asserting that exemptions criteria were not satisfied because amount and type of information collected by DHS proved that information was not being used to identify "individual criminal offenders" under subsection (j)(2)(A), nor was it used "for the purpose of a criminal investigation" under subsection (j)(2)(B), or for "the process of enforcement of criminal laws" under subsection (j)(2)(C)); *see also* § 552a(j) (laying out requirements to exempt system of records under subsections 552a(j)(2)(A)–(C)).

B. "No" Means "No" and If a Provision Is Not Listed as Non-Exemptible, It Is Exemptible

The DHS utilized the text, structure, and legislative history of the Privacy Act, as well as the Office of Management and Budget's ("OMB's") statutory interpretation and prior case law, to support its position that all of the plaintiff's Privacy Act claims were barred.[93] The DHS argued that its exemption was proper because the plain language of the general exemptions provision, subsection (j), states that a federal agency can exempt its system of records from any provision of the Privacy Act except those explicitly listed as non-exemptible under subsection (j).[94] As the DHS points out, the civil remedies provision is absent from that list.[95] The structure of the Privacy Act, with multiple enforcement mechanisms, confirmed Congress's intent that alternative methods be utilized in place of the civil remedies provision in private civil suits to ensure that federal agencies complied with their Privacy Act obligations.[96] The legislative history highlighted the amendments to the Privacy Act's wording and furthered the conclusion, supported by the text and structure of the Privacy Act, that Congress did not intend for private civil enforcement of the Privacy Act for systems of records that had been exempted from the civil remedies provision.[97]

In addition to the clear language and legislative intent behind the Privacy Act, agencies and courts have interpreted the general exemptions provision to allow agencies to exempt their systems of records

---

[93] *See infra* notes 94–100 (detailing defendant's position).

[94] *See* § 552a(j) (stating that "head of any agency may promulgate rules, in accordance with the requirements . . . of this title, 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)"); *see also* Shearson v. U.S. Dep't of Homeland Sec., No. 06-1478, 2007 U.S. Dist. LEXIS 16902, at *42 (N.D. Ohio Mar. 9, 2007) (stating that "Congress clearly contemplated which types of enforcement remedies would be available against individuals and/or agencies" and concluded civil enforcement would not be available remedy for system of records exempted under subsection (j)), *vacated*, 638 F.3d 498 (6th Cir. 2011).

[95] *See* § 552a(j) (containing list of non-exemptible provisions, but subsection (g) is not included).

[96] *See* Privacy Act of 1974, Pub. L. No. 93-579 § 3, 88 Stat. 1896, 1902 (1974) (detailing supplemental enforcement mechanisms including criminal penalties provision and requirement that President provide annual report to Congress listing any system of records that had been exempted within prior year and reasons for agency's exemption).

[97] *See* Legislative History of the Privacy Act, *supra* note 28, at 249 (showing that original versions of Privacy Act introduced in House and Senate would have allowed any individual injured by violation of Privacy Act to sue). The legislation was amended, however, to allow the head of an agency to exempt a system of records from the majority of the requirements pursuant to subsection (j), thus suggesting that Congress did not intend for civil suits to be the primary enforcement mechanism. *See generally* Brief for Defendants-Appellees at 10–11 Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498 (6th Cir. 2011) (No. 08-4582) (stating defendant's argument); *see generally* § 552a(j) (allowing agency heads to exempt system of records from certain requirements of Privacy Act).

from the civil remedies provision.[98] OMB—the federal agency in charge of prescribing guidelines for the Privacy Act and overseeing its implementation—construed the general exemptions provision to allow an agency to exempt a system of records from the civil remedies provision.[99] Furthermore, several federal appellate courts have held that the general exemptions provision allowed a federal agency to exempt its system of records from the civil remedies provision of the Privacy Act.[100]

C. On the Straight and Narrow: The Sixth Circuit Narrowly Interprets the Breadth of the General Exemptions Provision

In analyzing the Privacy Act, the court began with the plain language of the statute.[101] The court noted that the general exemptions provision's list of non-exemptible provisions did not contain the civil remedies provision, and therefore the natural reading of the statute supported the view that an agency can exempt a system of records from the requirements of the civil remedies provision.[102] Upon closer inspection, however, the court pointed out that the general exemptions provision lists non-exemptible provisions whose violation must be resolved through the civil remedies provision, thus implying that an agency cannot avoid civil liability for the violation of those non-exemptible provisions.[103] After acknowledging the two potential statutory interpretations, the court examined the prior case law and recognized that the issue implicated a circuit split in authority.[104]

Given the uncertainty over the Privacy Act's text and the circuit split on the issue, the court turned to the congressional intent behind its inclusion of the criminal penalties provision, subsection (i), but not the civil remedies provision, subsection (g), among the non-exemptible

---

[98] *See infra* notes 99–100 (discussing how agencies and courts have interpreted language of general exemptions provision).

[99] *See* § 552a(v) (stating that Director of OMB shall: "(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and (2) provide continuing assistance to and oversight of the implementation of this section by agencies"); *see also* OMB, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,947, 28,971 (July 9, 1975) (noting that OMB guidelines state that "[e]xemptions under subsection (j) may be exempted from the civil remedies provision").

[100] For a discussion of federal court decisions holding that an agency may exempt its system of records from the civil remedies provision pursuant to the general exemptions provision, see *supra* notes 70–74 and accompanying text.

[101] *See infra* notes 102–03 and accompanying text (describing court's analysis of Privacy Act's plain language).

[102] *See* Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 502 (6th Cir. 2011).

[103] *See id.* (examining possible interpretations of Privacy Act's text).

[104] For a discussion of the circuit split, as well as the factual background and judicial analysis for each case, see *supra* notes 64–74 and accompanying text.

provisions.[105] Ultimately, the court determined that subsection (i) and subsection (g) were not parallel provisions, and therefore the inclusion of one and the omission of the other was not instructive.[106] After distinguishing the two subsections based on their structure, the court decided that *Doe v. Federal Bureau of Investigation* expressed the better interpretation, concluded that Congress intended for the remedy to follow the violation, and endorsed the minority view in the circuit split.[107]

IV. Security Breach! A Critical Analysis of the Sixth Circuit's Opinion

The Sixth Circuit found support for its holding in the legislative intent, but the Privacy Act's plain language and legislative history point to a different result that is more consistent with the canons of statutory interpretation and national security policy.[108] When determining the meaning of a statute, the starting point is the statutory language itself.[109] Here, the statutory language seems clear: Congress provided a general exemptions provision and listed in that provision several subsections of the Privacy Act that could not be exempted.[110] Although significant debate exists over the court's role in interpreting statutes, canons of statutory interpretation dictate that when the statutory language is plain and unambiguous, the court's sole responsibility is to apply that language.[111] Therefore, the court should have adhered to the plain language of the Privacy Act in its analysis and permitted the DHS

[105] *See infra* notes 106–07 and accompanying text (providing discussion of congressional intent behind composition of general exemptions provision's list of non-exemptible provisions).

[106] *See Shearson*, 638 F.3d at 503–04 (remarking that subsection (i) is only section that makes certain conduct criminal and therefore must be non-exemptible, whereas subsection (g) is strictly enforcement provision that refers to duties set forth in other subsections). The court bolstered this argument by noting that Congress omitted subsection (h), which states that a guardian may act on behalf of a minor or incapacitated person, from the list of non-exemptible provisions. *See id.* at 504 (explaining that subsection (h), like subsection (g), does not impose substantive duties, but that it is unlikely Congress intended to permit agency to exempt its system of records from subsection (h)). For text of the civil remedies and criminal penalties provisions, see *supra* notes 40–41.

[107] *See Shearson*, 638 F.3d at 504 (holding that agency may exempt system of records from civil remedies provision only if underlying substantive duty is exemptible under general exemptions provision).

[108] *See infra* notes 109–22 (discussing alternative analysis to that used by court).

[109] *See* Caminetti v. United States, 242 U.S. 470, 485 (1917) ("It is elementary that the meaning of a statute must, in the first instance, be sought in the language in which the act is framed, and if that is plain . . . the sole function of the courts is to enforce it according to its terms.").

[110] *See* Privacy Act of 1974, 5 U.S.C. § 552a(j) (1974) (listing specific provisions as non-exemptible in text of general exemptions provision).

[111] *See Caminetti*, 242 U.S. at 485 ("Where the language is plain and admits of no more than one meaning, the duty of interpretation does not arise, and the rules which are to aid doubtful meanings need no discussion."); Tenn. Valley Auth. v. Hill, 437 U.S. 153, 185 n.29 (1978) ("When confronted with a statute which is plain and unambiguous on its face, we ordinarily do not look to legislative history as a guide to its meaning."). *But see* Green v. Bock Laundry Mach. Co., 490 U.S. 504, 511 (1989) (explaining that plain text did not resolve textual ambiguities, and that history leading up to enactment of statute must be examined for guidance).

and CBP to exempt its system of records from the civil remedies provision because it was not listed among the non-exemptible provisions.[112]

Even assuming that the Sixth Circuit was correct in concluding that the statutory language was unclear, the relevant precedent also supports a finding that the DHS and CBP were permitted to exempt their system of records from the civil remedies provision.[113] In siding with the minority view, the court found that the decisions in *Tijerina* and *Doe* expressed "the better view."[114] The facts of *Tijerina*, however, are distinguishable because *Tijerina* dealt with the VA sending an unsolicited letter containing personal information to another agency in violation of the Privacy Act, whereas the current case involves Shearson's attempt to access and revise her own personal files.[115] Similarly, the decision in *Doe* can be distinguished because the relevant discussion in *Doe* was contained in dicta and only clarified the court's previous holding in *Tijerina*.[116]

---

[112] *See supra* note 111 (providing support for applying plain language of statute). Indeed, some scholars would argue that the plain language should always control, and that the legislative history and legislative intent of a statute should rarely, if ever, be consulted. *See* Antonin Scalia, A Matter of Interpretation 33–35 (1997) (noting that legislative history used to constitute development of statute and attempts by Congressmen to persuade those voting on piece of legislation). Now that it is universally expected for courts to look to legislative history, however, its primary purpose has become to affect judicial decisions rather than to inform members of Congress about a particular statute. *See id.* at 33–36 (explaining unreliable nature of legislative history and that legislative history of any major piece of legislation offers support for both sides). According to some scholars, the legislative intent is equally unhelpful. *See* Max Radin, *Statutory Interpretation*, 43 Harv. L. Rev. 863, 870–71 (1930) (disparaging legislative intent as means for statutory interpretation). According to Radin, the legislative intent is undiscoverable in any real sense, and any external signs of agreement with a piece of legislation could be motivated by many different forces. *See id.* at 870 (explaining that chances of several hundred Congressmen having same statutory meanings in mind is infinitesimally small). Moreover, even if the legislative intent were discoverable, it would have no binding legal force. *See id.* at 871 (emphasizing that function of Congressmen is not to impose their will on citizens, but instead to draft and enact statutes). Justice Scalia concurred with this reasoning. *See* Scalia, *supra* at 22 ("The text is the law, and it is the text which must be observed.").

[113] *See infra* notes 114–16 (discussing support for agency's ability to exempt system of records from civil remedies provision); *see also* Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 502–03 (6th Cir. 2011) (noting that case presented issue of first impression and analyzing circuit split for insight).

[114] *See Shearson*, 638 F.3d at 503–04 (explaining why court sided with minority view).

[115] *See* Tijerina v. Walters, 821 F.2d 789, 795–97 (D.C. Cir. 1987) (explaining that purpose of subsection (j) was to permit agencies to withhold access to sensitive information in attempt to avoid hampering law enforcement efforts). Because subsection (j) was not intended to permit agencies to avoid liability for disclosure, the provision did not protect the VA from liability for the disclosure of personal information. *See id.* at 796 (explaining distinction between access to and disclosure of information kept in system of records). But in Shearson's case, protecting law enforcement efforts were among the listed reasons why the DHS exempted its system of records. *See* Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System, 72 Fed. Reg. 43,567, 43,569 (Aug. 6, 2007) (to be codified at 6 C.F.R. pt. 5) (listing need to "avoid disclosure of investigative techniques" and to "safeguard sensitive information" as reasons why DHS exempted its system of records).

[116] *See* Doe v. Fed. Bureau of Investigation, 936 F.2d 1346, 1352 (D.C. Cir. 1991) (explaining holding in *Tijerina* and stating that agency cannot avoid liability for violating non-exemptible provisions by exempting its system of records from civil remedies provision).

After adopting the minority view in the circuit split, the court turned to the congressional intent to justify its holding.[117] The court concluded that Congress's inclusion of the criminal penalties provision, subsection (i), but not the civil remedies provision, subsection (g), among the general exemptions provision's list of non-exemptible provisions was "not instructive" because subsections (g) and (i) were not parallel provisions.[118] The court suggested that subsection (i) had to be listed as non-exemptible because it was a stand-alone provision, but subsection (g) did not because it provided remedies for violations listed in other sections of the Privacy Act, some of which were non-exemptible.[119]

Subsection (i), however, also refers to duties listed in other non-exemptible subsections and provides recourse for their violation, indicating that subsections (g) and (i) are more similar than the court thought.[120] In addition, the legislative history shows that earlier versions of the Privacy Act allowed individuals to bring civil actions against an agency whenever it violated a provision of the Privacy Act, whereas the current version of the statute allows an agency head to exempt its system of records from many of the Privacy Act requirements.[121] Therefore, a more plausible explanation of the congressional intent is that Congress envisioned criminal penalties to be available at all times, but gave agencies flexibility to exempt themselves from certain civil remedies in an effort to avoid hampering law enforcement activity.[122]

Several other arguments advanced by Shearson, but not considered by the court, were equally unconvincing.[123] In her brief, Shearson argued that the general exemptions provision does not apply to the civil remedies provision because the general exemptions provision permits an agency to exempt a "system of records," and the

---

[117] *See Shearson*, 638 F.3d at 503–04 (analyzing congressional intent behind drafting of Privacy Act).

[118] *See id.* (discussing different functions of subsections (g) and (i) as justification for Congress's decision not to list subsection (g) as non-exemptible).

[119] *See id.* (explaining subsection (g)'s nature as strictly enforcement provision because it provided recourse for duties set forth in other sections, whereas subsection (i) had to be listed as non-exemptible because there was no other section that criminalized and imposed penalties for certain conduct).

[120] *See* Privacy Act of 1974, 5 U.S.C. § 552a(i)(2) (1974) (providing criminal sanctions against any agency employee "who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section").

[121] *See* Legislative History of the Privacy Act of 1974, *supra* note 28, at 249 (noting that original version of Privacy Act provided citizens with right to enforce Privacy Act violations against agency via civil suits). The current version of the Privacy Act, however, allows the head of an agency to promulgate rules exempting its system of records from many of the Privacy Act's provisions. *See also* § 552a(j) (stating requirements for exemptions).

[122] *See* Brief for Defendants-Appellees, *supra* note 97, at 13 (discussing significance that must be given to Congress's decision to leave subsection (g) out of list of non-exemptible provisions).

[123] *See infra* notes 124–30 and accompanying text (providing rebuttal of additional arguments advanced by Shearson but not taken under review by court).

civil remedies provision does not explicitly refer to any "system of records."[124] This argument fails because the criminal penalties provision, which is listed under the general exemptions provision as non-exemptible, also does not specifically refer to a system of records.[125] Indeed the court in *Nakash v. U.S. Department of Justice*, a case heavily relied on by Shearson in her brief, noted that the reasoning in *Tijerina* was undermined because subsection (i)'s inclusion as a non-exemptible provision clearly indicated that subsection (j) applied to subsections that did not explicitly refer to a "system of records."[126]

Similarly, Shearson argued at length that the DHS did not properly exempt its system of records, either because the DHS did not promulgate a proper rule, because the language of the exemption was insufficient, or because the system of records did not meet the exemption requirements of subsection (j).[127] Not only would these claims be procedurally barred because Shearson failed to raise them in the district court, but they also lack merit.[128] While Shearson correctly pointed out that the

[124] *See* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 24–25 (arguing that civil remedies provision does not refer to system of records and that it is directed towards courts and aggrieved citizens, not agencies).

[125] *See* § 552a(i) (providing text of criminal penalties provision); *see also* Brief for Defendants-Appellees, *supra* note 97, at 10 (explaining that Congress did not limit scope of subsection (j)'s exemptions to subsections that specifically refer to "system of records" as evidenced by subsection (i)'s inclusion in text of subsection (j)). Defendant argued further that it would not make any sense for Congress to explicitly reference a subsection of the Privacy Act in the general exemptions provision—subsection (i)—if that subsection could not be exempted because it did not specifically refer to a system of records. *See id.*

[126] *See* Nakash v. U.S. Dep't of Justice, 708 F. Supp. 1354, 1362–63 (S.D.N.Y. 1988) (explaining weakness in *Tijerina* court's logic). According to the court in *Nakash*, the criminal penalties provision is similar to the civil remedies provision because neither subsection specifically references a "system of records." *See id.* at 1363 (recognizing that *Tijerina* court's premise that civil remedies provision cannot be subject to terms of general exemptions provision because it did not refer to system of records was undermined by subsection (i)'s status as non-exemptible provision under subsection (j)).

[127] *See* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 26–34 (alleging failure of DHS to properly exempt its system of records from Privacy Act requirements under general exemptions provision). First, Shearson argued that the DHS never promulgated a proper rule because the rule promulgation was limited to a notice of proposed rule-making. *See id.* at 27 (describing claimed lack of finality, and thus effectiveness, of promulgated rule). Second, Shearson alleged that the language of the exemption was insufficient to exempt the civil remedies provision from the general exemptions provision because that exemption was limited to the extent that it was exempt from other subsections of the Privacy Act. *See* Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System, 72 Fed. Reg. 43,567, 43,569 (Aug. 6, 2007) (to be codified at 6 C.F.R. pt. 5) (describing extent of exemption); *see also* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 26–34 (claiming that this action was not sufficient to permit DHS to exempt civil remedies provision from Privacy Act). Finally, Shearson contended that the DHS's system of records did not fall within the law enforcement exemption requirements of subsection (j). *See* § 552a(j)(2)(A)–(C) (providing requirements for exemption under general exemptions provision); *see also* Petitioner's Brief Submitted Pro Se, *supra* note 80, at 26–34 (alleging that none of law enforcement criteria set out in subsections (j)(2)(A)–(C) are met).

[128] *See* Brief for Defendants-Appellees, *supra* note 97, at 13 (advocating for rejection of Shearson's claims regarding allegedly inadequate exemption procedures used by DHS); *see also infra* notes 129–30 (analyzing merit of Shearson's claims).

DHS issued a proposed rule-making to exempt the ATS—one of the agency's systems of records—from certain provisions of the Privacy Act, the ATS was still covered by the exemption for the TECS system of records.[129] Moreover, while it is likely that the ATS also qualifies under the criteria laid out in subsections 552a(j)(2)(A) and 552a(j)(2)(C), the ATS clearly falls within the scope of 552a(j)(2)(B) which requires that the exempted system of records consist of "information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual."[130]

The Potential Impact: A Narrowing of National Security?

Shearson's case has garnered significant media attention, and the implications could be far-reaching.[131] The public remains heavily divided over whether individual privacy should be sacrificed to increase security, and if so, what forms of privacy invasion were acceptable.[132] Although polls will always differ, there seems to be a general consen-

---

[129] *See* Privacy Act of 1974: Implementation of Exemptions; Automated Targeting System, 72 Fed. Reg. at 43,569 (proposing new exemption rule). Shearson saw this notice but failed to realize the fact that the ATS, which is a part of the TECS, was still covered by an exemption under the Privacy Act for the TECS system of records. *See, e.g.*, 31 C.F.R. § 1.36 (2000) (exempting ATS and TECS from several Privacy Act provisions, including civil remedies provision).

[130] § 552a(j)(2)(B) (listing one criteria for exempting system of records under general exemptions provision); *see also* Brief for Defendants-Appellees, *supra* note 97, at 29 (explaining that TECS system of records collects information about people entering and exiting United States in order to identify potential law breakers and, specifically in case of ATS, to identify potential terrorists). Significantly, nothing in subsection (j)(2)(B) prevents the exemption of a system of records that is compiled for investigations whose scope is broader than a single individual or offense. *See id.* (asserting compliance of ATS and TECS with exemption criteria set out in general exemptions provision).

[131] *See Appeals Court Rules Ohio Activist's Privacy Case May Proceed*, Charity & Sec. Network (May 1, 2011), http://www.charityandsecurity.org/news/Appeals_Court_Rules_Ohio_Activist_Privacy_Case_Proceed (discussing Sixth Circuit's holding in Shearson's case); *DHS Can't "Opt Out" of Liability for Violating the Privacy Act*, Papers, Please!: The Identity Project (Apr. 21, 2011), http://www.papersplease.org/wp/2011/04/21/ (theorizing on national implications of Sixth Circuit's holding); *Federal Appeals Court Affirms Civil Penalties in Privacy Act Case*, Electronic Privacy Info. Ctr. (Apr. 25, 2011), http://epic.org/2011/04/federal-appeals-court-affirms-1.html (discussing holding of case); Ben Kerschberg, *Should Government Agencies Be Able to Exempt Themselves From the Privacy Act?*, Forbes (Apr. 26, 2011, 11:57 AM), http://www.forbes.com/sites/benkerschberg/2011/04/26/should-government-agencies-be-able-to-exempt-themselves-from-the-privacy-act/ (recognizing potential for Shearson's case to prompt Supreme Court to grant certiorari and settle circuit split, or for Congress to pass legislative amendments to Privacy Act); Smith, *supra* note 2 (describing details of Shearson's legal battle).

[132] *See* Kristin Fisher, *Privacy vs. Security: New AP Poll Ten Years After 9/11*, WUSA (Sept. 6, 2011 6:00 PM), http://www.wusa9.com/news/article/165944/373/Privacy-vs-Security-New-Poll-10-Years-After-911 (reporting that sixty-four percent of Americans admit that sometimes it is necessary to forego individual privacy to fight terrorism); Morales, *supra* note 16 (commenting that large majority of frequent travelers view preventing acts of terrorism as outweighing any potential loss of privacy). *But see* Jennifer Agiesta & Nancy Benac, *Poll: OK to Trade Some Freedoms to Fight Terrorism*, The Associated Press (Sept. 6, 2011, 12:43 PM), http://www.apnorc.org/news-media/Pages/News+Media/poll-ok-to-trade-some-freedoms-to-fight-terrorism.aspx (finding that fifty-four percent of American would choose preserving rights and freedoms over protecting people from terrorists).

sus that additional security is desired, so long as the privacy invasions are not extensive.[133]

Given the contentious nature of the issue, the district court acted properly by relying heavily on the plain language of the statute, and the weight of prior precedent, in making its decision.[134] The district court noted that it had concerns regarding whether its decision produced a just result, but correctly pointed out that Congress possesses the power to rectify the statutory language if it so chooses.[135] Instead of heeding the district court's warning, the Sixth Circuit relied on the legislative history and legislative intent in thrusting itself into the middle of a policy debate that is the province of the political branches.[136] The Sixth Circuit's interpretation effectively amended the statutory language of the Privacy Act by adding the civil remedies provision to the list of non-exemptible provisions, presumably because it did not agree with the outcome that would have resulted from the application of the plain statutory language.[137] Yet, in a situation where a plain reading of the statute would result in a similarly questionable outcome, the Supreme Court held that the plain language of the Endangered Species Act must be followed—the Court ordered the Tennessee Valley Authority to enjoin construction of a dam that would have provided electricity to 20,000 households because its operation would destroy the habitat of the snail darter, an endangered

[133] *See* Agiesta & Benac, *supra* note 132 (noting that even poll which reported Americans chose liberties over security found that majority of people surveyed also supported surveillance in public areas, random searches, full-body scans and pat-downs of airline passengers, and warrantless government analysis of financial transactions processed by United States banks).

[134] *See* Shearson v. U.S. Dep't of Homeland Sec., No. 06-1478, 2007 U.S. Dist. LEXIS 16902, at *41–42 (N.D. Ohio Mar. 9, 2007), *vacated*, 638 F.3d 498 (6th Cir. 2011).

[135] *See id.* at *38 (explaining that district court "recognizes the hardship that may befall law abiding citizens who lack a mechanism to correct erroneous information. This Court, however, is charged only with applying the laws Congress passes and lacks the authority to rewrite those laws.").

[136] *See* Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 502–05 (6th Cir. 2011) (describing court's focus on legislative intent); *see also supra* notes 111–12 (providing general discussion of problems incumbent upon court's consideration of legislative history and legislative intent when statutory language is clear).

[137] *See* Privacy Act of 1974, 5 U.S.C. § 552a(j) (1974) (listing subsections that are non-exemptible under general exemptions provision); *see also supra* notes 108–22 and accompanying text (discussing how Sixth Circuit overlooked seemingly plain and unambiguous exclusion of civil remedies provision from list of non-exemptible provisions in order to hold that Shearson's claims were not barred).

species of fish.[138] Therefore, although denying Shearson's information request may not be a desirable result from a policy standpoint, the purview of the judicial system is to apply the law, not to re-write it.

While the full and exact ramifications of the Sixth Circuit's decision have yet to be felt, its impact on national security is inevitable.[139] Government attorneys have resisted the release of information detailing methods by which citizens are identified, traced, and investigated at border stops because certain agencies feel that terrorists could use that information to discover how to circumvent attempts by the government and law enforcement agencies to target them in the future.[140] In recognition of this concern, several federal courts have deemed the exemptions under the Privacy Act as essential for national security so long as the records are relevant and necessary to accomplish a legally permissible purpose.[141]

The Sixth Circuit's decision has prompted commentators to call for congressional action to modernize the statute, or, alternatively, for guidance from the Supreme Court to settle the circuit split.[142] It is unlikely that Congress ever envisioned terrorist watch lists, the expansive reach of the internet, or other major technological developments

---

[138] The Endangered Species Act provides, in relevant part, that:

> Federal departments and agencies shall . . . utilize their authorities in furtherance of the purposes of this chapter by carrying out programs for the conservation of endangered species . . . by taking such action necessary to insure that actions authorized, funded, or carried out by them do not jeopardize the continued existence of such endangered species . . . or result in the destruction or modification of habitat of such species which is determined by the Secretary . . . to be critical.

Endangered Species Act, 16 U.S.C. § 1536 (1976); *see also* Tenn. Valley Auth. v. Hill, 437 U.S. 153, 173–74 (1978) (finding statutory provision and its requirements to be crystal clear, despite seemingly ridiculous outcome of applying statutory language). The Tennessee Valley Authority ("TVA") argued that the Endangered Species Act ("ESA") cannot be reasonably interpreted to require shutting down a federally funded project that had been well under way before the ESA was even enacted. *See id.* (noting that TVA's argument must fail because its interpretation would force Court to ignore ordinary meaning of plain language).

[139] *See infra* notes 140–41 (discussing potential repercussions of Sixth Circuit's ruling).

[140] *See* Smith, *supra* note 2 (explaining government and agency fears that disclosure of this sensitive information might compromise national security).

[141] *See* Kerschberg, *supra* note 131 (discussing importance some federal courts placed on protecting sensitive information with relevance to national security).

[142] *See id.* (calling for guidance from Supreme Court or legislative amendments to Privacy Act).

when it drafted the Privacy Act.[143] The outdated language of the Privacy Act, and the results that could arise from strict adherence to the statutory text, might explain why several courts have found the Privacy Act's language to be ambiguous and have instead focused on the Privacy Act's legislative history to reach what the court perceives to be a just outcome.[144] Congress must lend finality through legislative action updating the Privacy Act's language and purpose to reflect current federal policies.[145] Because Congress has the knowledge, resources, and expertise to properly weigh the competing interests in an ever-changing world, it remains the best vehicle for modernizing of the Privacy Act.[146]

---

[143] *See* Privacy Act of 1974, 5 U.S.C. § 552a (1974) (establishing 1974 as year in which Privacy Act was drafted). Many Americans viewed the collapse of the World Trade Towers on September 11, 2001 as the first real notice of the threat terrorism poses to the United States. *See* Nick J. Sciullo, *The Ghost in the Global War on Terror: Critical Perspectives and Dangerous Implications for National Security and the Law*, 3 Drexel L. Rev. 561, 562 (2011) (describing terrorism as relatively new threat to America); *see also* Daniel J. Mitchell, *Fighting Terror and Defending Freedom: The Role of Cost-Benefit Analysis*, 25 Pace L. Rev. 219, 219 (2005) (observing policy maker's recognition after 9/11 that federal government needed better tools to deter terrorist attacks in future); Igor Primoratz, *A Philosopher Looks at Contemporary Terrorism*, 29 Cardozo L. Rev. 33, 33 (2007) (noting that scale of attacks on 9/11 and large number of victims created new public awareness for terrorism that had not existed prior to attacks); *Updating the Privacy Act of 1974*, Ctr. for Democracy and Tech. (June 5, 2009), http://www.cdt.org/policy/updating-privacy-act-1974#4 (asserting that wording of Privacy Act from over thirty years ago "renders it ill-equipped to meet many of the privacy challenges posed by modern information technology"). In fact, loopholes were reported as early as 1977, and a report by the Privacy Protection Study Commission warned that technological advancements threatened to outpace the Privacy Act. *See id.* (explaining that Privacy Act was "designed to accommodate agency-held flat files, but computing has moved towards forms of networked centralization and relational databases beyond the Privacy Act's reach").

[144] *Compare* Shearson v. U.S. Dep't of Homeland Sec., No. 06-1478, 2007 U.S. Dist. LEXIS 16902, at *38 (N.D. Ohio Mar. 9, 2007) (realizing that outcome of Shearson's case may not be just, but adhering to statutory language as drafted by Congress), *vacated*, 638 F.3d 498 (6th Cir. 2011), *with* Shearson v. U.S. Dep't of Homeland Sec., 638 F.3d 498, 503–04 (6th Cir. 2011) (looking past plain language of Privacy Act to interpret its legislative intent).

An analogy may be drawn between the effect that the emergence of terrorism has had on the Privacy Act with the effect that continual technological advancements have had on the Copyright Act. Section 106 of the Copyright Act gives the author of a copyrighted work the exclusive right to, among other things, copy and distribute her work and to prepare derivative works. *See* Copyright Act, 17 U.S.C. § 106 (2002) (listing rights granted to authors of copyrighted work). The Copyright Act, however, has largely been driven by changing technologies. Sony Corp. of Am. v. Universal City Studios, Inc., 464 U.S. 417, 430 (1984) ("[L]aw of copyright has developed in response to significant changes in technology."). In *Sony*, the court was asked to decide whether Sony was liable as a contributory infringer for selling VCRs that allowed users to record copyrighted broadcasts for viewing at a later time. *See id.* at 420. The Supreme Court explained that, as new developments have occurred, Congress has been the governmental entity that has fashioned the new rules necessitated by the evolving technology. *See id.* at 430–31 ("[I]n a case like this, in which Congress has not plainly marked the course to be followed by the judiciary, this Court must be circumspect in construing the scope of rights created by a statute that never contemplated such a calculus of interests."). According to the Court, Congress possesses the constitutional authority and institutional ability to fully address competing interests implicated by new technologies. *See id.* at 431 (recognizing Court's reluctance to act without guidance from Congress in applying outdated statutory language to unforeseen technologies).

[145] *See* Kerschberg, *supra* note 131 (acknowledging Congress's ability to settle debate and promote uniformity on issue that has fractured circuit courts).

[146] *See* Firehock, *supra* note 23, at 1545 n.6 (discussing privacy regulation in United States as area left to Congress).