NONJUDICIAL FANGS: DEFENDING THE PRIVACY ACT'S COMPLETE CIVIL REMEDIES EXEMPTION

JOSHUA A. RUBIN*

The Privacy Act of 1974 places limitations on what federal agencies may do with the personal information they collect from the public. As its name suggests, a primary purpose of the law is to protect the privacy of individuals by mandating that agencies' systems of records be maintained in particular ways. At the same time, the Act preserves the ability of agencies to pursue their statutory goals by permitting law enforcement agencies to exempt their systems of records from select provisions of the Act. This Note concerns the scope of one of those exemptions, referred to as the "general exemption." Specifically, it addresses a statutory ambiguity surrounding whether these agencies may completely exempt their records from the Act's civil remedies provision, thereby foreclosing civil liability for all violations of the Act. This Note answers that question in the affirmative, and it supports that answer through two independent modes of analysis. First, the Note argues that, using traditional tools of statutory interpretation, the best reading of the portions of the Privacy Act in question is one that recognizes the complete exemption. Second, the Note meets a particular objection to that reading: that permitting a complete civil remedies exemption would authorize and encourage widespread violations of the Privacy Act, thereby "defanging" the Act. The Note maintains that civil remedies are not theoretically necessary to protect substantive rights, and that the particular context of the Privacy Act is replete with examples of nonjudicial institutions serving as effective checks—or fangs—on agency compliance with the law.

* Copyright © 2015 by Joshua A. Rubin, J.D., 2015, New York University School of Law; B.A., 2013, Macalester College. I would like to thank Professor Sally Katzen for her advice and guidance on this topic. Much thanks also to the editors of the *New York University Law Review*, especially Ali Ziegler for her immense help. Finally, I am grateful to Ivy for her love and support.

INTRODUCTION

Passed in 1974 amidst fears of government overreach, the Privacy Act governs the way federal agencies must handle the personal information they collect from individuals.[1] The Act sought to strike an ideal balance between individual privacy on one hand, and the preservation of an effective executive on the other. The establishment of broad and constraining requirements on agencies, which were then somewhat moderated by the presence of exemptions and limits on liability, achieved this compromise.

Like much legislation, the Act's exemptions contain ambiguities that have produced litigation and academic notice. This Note addresses one of these ambiguities, which concerns the interplay between two of its parts: the Act's civil remedies provision and its general exemption provision. The interpretive question is whether the civil remedies are among those provisions which may be exempted. Courts that have directly addressed the issue have held that they are

[1] *See* Haeji Hong, *Dismantling the Private Enforcement of the Privacy Act of 1974:* Doe v. Chao, 38 AKRON L. REV. 71, 72 (2005) ("Congress enacted the Privacy Act to prevent the federal government from violating privacy rights of American citizens.").

not, warning quite ominously that permitting the civil remedies exemption would "defang completely" the Privacy Act.[2]

This Note demonstrates why these courts are incorrect. It provides a variety of reasons why the best reading of the Privacy Act would permit law enforcement agencies to completely exempt their records from civil judicial review. In doing so, this Note makes both traditional interpretive arguments—what one might call "legal" arguments—as well as more policy-minded analysis about different mechanisms for encouraging and enforcing agency compliance with the Privacy Act. These latter arguments are meant to ease the anxiety that a rejection of judicial remedies in certain contexts would be tantamount to an elimination of the Privacy Act itself. Ultimately, this Note concludes that while judicial review would indeed be one way to promote compliance with the law, it is by no means the only way, nor is it necessarily the best way. Other institutions play a vital role in legal enforcement—both generally and with respect to the particular provisions of the Privacy Act. In other words, even if courts and commentators are correct in their notions that the Privacy Act must possess "fangs" to guarantee administrative compliance, there exists an opportunity for nonjudicial fangs to play a meaningful role.

In Part I, this Note lays out in detail the statutory ambiguity around the so-called "complete" subsection (g) exemption,[3] and describes the manner in which both agencies and courts have responded. Part II critiques the interpretive method and conclusions of the courts to have ruled on the illegality of the exemption, and presents an alternative statutory interpretation of the provisions in tandem, ultimately concluding that the best interpretation is one which permits law enforcement agencies to exempt their records from judicial review. Part III turns from law to policy and discusses normative issues related to the question of the complete subsection (g) exemption. At its core, Part III represents a defense against a particular objection—that disallowing judicial review will authorize the executive to behave without any legal restrictions.

---

[2] *See, e.g.*, Tijerina v. Walters, 821 F.2d 789, 797 (D.C. Cir. 1987) ("Agency exemption from civil liability is not in keeping with the language of the Act, and it serves none of the purposes behind the exemptions provision or the Act as a whole.").

[3] *See, e.g.*, Maxim Brumbach, Note, *Are You on the List? Dispelling the Myth of a Total Exemption from the Privacy Act's Civil Remedies in* Shearson v. DHS, 81 U. CIN. L. REV. 1027, 1037–40 (2013) (describing both the "complete" and the "limited" theories of the exemption).

I
THE QUESTION OF THE COMPLETE EXEMPTION AND ITS CURRENT ANSWERS

Part I of this Note identifies the ambiguity that arises with regard to the interaction between subsections (g) and (j). It first provides an overview of the Privacy Act—with special emphasis placed on these relevant subsections—and then flags the particular interpretive issue that arises regarding the interaction. Next, it discusses the response to this ambiguity by both agencies and courts, the latter of which have been hostile to the complete subsection (g) exemption.

A. The Textual Problem: The Collision of Two Subsections

Passed in the wake of the Watergate scandal during a time of heightened suspicion of government,[4] the Privacy Act of 1974 ("the Privacy Act" or "the Act") seeks "to protect the integrity and security of an individual's records by regulating how the agencies maintain and disseminate these records."[5] The Privacy Act supplies explicit restrictions on the actions of federal agencies "at all three stages of the information systems process: collection, maintenance, and dissemination of information."[6]

1. Substantive Requirements of the Privacy Act

The Privacy Act restricts the manner in which federal agencies handle the personal information they collect from individuals. The affirmative rules that agencies must comply with under the Privacy Act can be conceptually divided into five functions: (1) limiting agencies' ability to disclose individuals' information to third parties;[7] (2) allowing individuals to gain access to their records and to request amendments to their records, and requiring agencies to grant those amendments if appropriate;[8] (3) requiring agencies to keep an account of disclosures of personal information;[9] (4) requiring agencies to establish and publish procedures for carrying out other provisions of

---

[4] *See* DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974, at 4 [hereinafter DOJ PRIVACY ACT OVERVIEW], http://www.justice.gov/sites/default/files/opcl/docs/1974privacyact-2012.pdf ("Congress was concerned with curbing the illegal surveillance and investigation of individuals by federal agencies that had been exposed during the Watergate scandal.").

[5] Laurie A. Doherty, *Privacy Act*, 56 GEO. WASH. L. REV. 1028, 1028 (1988).

[6] Introductory Remarks of Sen. Sam J. Ervin, Jr., on S. 3418, at 2, *reprinted in* LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, at 7, *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

[7] These limits are set forth in 5 U.S.C. § 552a(b) (2012).

[8] These limits are set forth in § 552a(d).

[9] These limits are set forth in § 552a(c).

the Act;[10] and (5) prohibiting the maintenance of any information not "relevant and necessary to accomplish a purpose of the agency required to be accomplished."[11]

Certain law enforcement agencies have the authority to exempt themselves from certain parts of the Act.[12] The main substantive provisions falling within this exemptible category include all of the access and amendment rules and the procedural rules.[13] Because law enforcement agencies can choose to exempt their records from these substantive provisions, these provisions are not of direct interest in this Note. Rather, this Note focuses on those provisions that qualifying law enforcement agencies are substantively required to follow.[14] Throughout this Note, these provisions will be referred to as "nonexemptible provisions." The most important of these provisions are the disclosure rules to third parties (subsection (b)) and the requirement that, before such disclosure is made, the agency "make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes."[15] These provisions are mandatory for all agencies, with no exceptions.

2. Civil Judicial Enforcement

The above discussion outlines the substantive requirements that the Privacy Act imposes upon federal agencies. A distinct issue is enforcement. The Act provides for civil remedies in subsection (g), where four separate types of lawsuits are described and authorized.[16] Of particular interest to this Note is subsection (g)(1)(D), which permits a suit whenever an agency "fails to comply with any other provision of [the Act] . . . in such a way as to have an adverse effect on any individual."[17] As indicated by its broad language, this type of lawsuit

---

[10] These limits are set forth in § 552a(f).

[11] These limits are set forth in § 552a(e).

[12] *See infra* note 25 and accompanying text (describing those agencies which may exempt their records from the Act).

[13] *See infra* note 26 and accompanying text (noting the provisions from which law enforcement agencies may exempt their records).

[14] This is different from the question of the *procedural* mechanism by which the substantive right is protected. This second issue is central to the remainder of this Note, particularly Part III.A., *infra*.

[15] § 552a(e)(6).

[16] § 552a(g)(1) (listing the four types of suits).

[17] § 552a(g)(1)(D). The other three types of lawsuits are of less interest to this Note because they concern violations of substantive provisions that can themselves be waived by qualified agencies. *See supra* notes 12–15 and accompanying text (explaining why these provisions are less relevant to the question of the complete subsection (g) exemption). Specifically, subsections (g)(1)(A) and (g)(1)(B) authorize suits alleging violations of the access and amendment provision, and subsection (g)(1)(C) authorizes suits for violations of subsection (e)(5), another exemptible provision.

may be utilized to allege a violation of any substantive provision of the Privacy Act, including a nonexemptible provision. Additionally, unlike other types of civil lawsuits authorized by the Act, which provide for declaratory and injunctive relief only, subsection (g)(1)(D) allows plaintiffs to recover damages and attorneys' fees against the United States as long as they can demonstrate that the agency's actions were "intentional or willful."[18]

A prototypical example of a (g)(1)(D) lawsuit is *Jacobs v. National Drug Intelligence Center*.[19] The National Drug Intelligence Center (NDIC) qualified as a law enforcement agency that could exempt its records from several provisions of the Act.[20] Pursuant to this authority, NDIC promulgated rules in which it did just that.[21] Because NDIC exempted its records from all exemptible provisions, a lawsuit could only be brought under (g)(1)(D). Gary Jacobs brought suit under this provision, claiming that NDIC violated the third-party disclosure rules of subsection (b) when it sent the press a report that identified Jacobs as a member of a money-laundering scheme.[22] The court agreed, ultimately awarding Jacobs $100,000 for "emotional-stress-based actual damages."[23]

3. General Exemption

As referenced above, not all agencies must comply with all provisions of the Privacy Act.[24] The so-called "general exemption" contained in subsection (j) applies to the Central Intelligence Agency (CIA) as well as any federal agency "which performs as its principal function any activity pertaining to the enforcement of criminal laws . . . ."[25] These agencies, referred to in this Note as "qualified agencies," may exempt "any system of records within the agency from any part of [the Privacy Act] except subsections (b), (c)(1) and (2),

---

[18] *See* § 552a(g)(4) ("In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual . . . .").

[19] 423 F.3d 512 (5th Cir. 2005).

[20] *Infra* note 29.

[21] *See* Privacy Act of 1974; New System of Records, 58 Fed. Reg. 78, 21996 (Apr. 26, 1993) (stating that "the Attorney General has exempted this system" from all exemptible subsections).

[22] *See Jacobs*, 423 F.3d at 513 (describing the plaintiff's allegations).

[23] *See* Jacobs v. Nat'l Drug Intelligence Ctr., 548 F.3d 375, 377 (5th Cir. 2008) (affirming the district court's verdict).

[24] *See supra* notes 12–13 (introducing the concept of agencies permitted to exempt their records).

[25] 5 U.S.C. § 552a(j) (2012).

(e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11)."[26] These nonexemptible provisions include all rules surrounding third party disclosure, publication of notices of records in the Federal Register, and rules regarding the creation of administrative procedures of records maintenance.[27]

The general exemption does not occur automatically. Rather, a qualified agency must affirmatively publish a notice in the Federal Register that it is exempting a particular system of records from those provisions.[28] This notice is typically provided at the same time that the agency gives general notice of the existence of the system of records.[29]

4. The Interplay Between Subsections (g) and (j)

The civil enforcement section (subsection (g)) and general exemption (subsection (j)) independently function in uncontroversial ways. The difficulty arises in the way these two provisions interact. When listing the parts of the Act from which qualified agencies may *not* exempt themselves—the nonexemptible provisions—the section authorizing civil suits, subsection (g), is not listed.[30] This raises the question of whether qualified agencies may exempt their records from subsection (g), and thereby immunize themselves from all lawsuits under the Privacy Act. The ability of a qualified agency to exempt its systems of records from civil lawsuits alleging *any* violation of the Privacy Act—including a nonexemptible provision—is referred to in this Note as "the complete subsection (g) exemption."[31]

---

[26] *Id.* A "system of records" is defined as "a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." § 552a(a)(5).

[27] *See* § 552a(j) (listing sections that are nonexemptible).

[28] *Id.* (stating that in order to exempt its records, an agency must "promulgate rules" doing so).

[29] *See, e.g.*, Privacy Act of 1974; System of Records, 68 Fed. Reg. 16, 3553–55 (Jan. 24, 2003) (introducing the "Criminal Investigation Report System" and exempting it pursuant to subsection (j)).

[30] § 552a(j) (listing sections that are nonexemptible).

[31] It may bear repeating what is at stake in this question and what is not. The issue is whether qualified agencies may exempt their records from the civil remedies provision. The answer to this question only matters as it relates to violations of nonexemptible provisions because qualified agencies may undeniably exempt their records from the substantive requirements of the exemptible provisions. The most important of the nonexemptible provisions is the prohibition on third party disclosure. Thus, it could be said with only minor oversimplification that the question of the complete subsection (g) exemption concerns whether civil remedies are available for qualified agencies' unlawful disclosure of personal information.

B. Agency Responses: Ambiguous Notice

In Part II, this Note argues that federal agencies have the statutory authority to exempt their systems of records from the civil damages provision. Statutory authority, however, does not end the inquiry. Exemption does not occur automatically; rather, agencies must affirmatively exempt their systems of records through publication in the Federal Register.[32] An agency must list the provisions it is exempting its records from, and must provide a reason for exempting its records from each provision.[33] No agency has unequivocally attempted to exempt its records completely from subsection (g). For this reason, this Note is directed not only to courts, but also to agencies, which may need to exempt their records more clearly and completely before courts can consider the legality of doing so.

In some situations, it is obvious that agencies have *not* completely exempted their records from subsection (g). Most fundamentally, they may simply not include subsection (g) among their list of exempted subsections. For example, the Equal Employment Opportunity Commission (EEOC), a qualified agency, states in its regulations that "[p]ursuant to 5 U.S.C. 552a(j)(2), investigatory materials compiled for criminal law enforcement in the Office of Inspector General Investigative Files are exempt from subsections (c)(3), (d)(1), (d)(2), (e)(1), (e)(2), and (e)(3) of the Privacy Act."[34] This list includes all exemptible provisions except subsection (g). Thus, the EEOC's Office of Inspector General has clearly not even attempted to exempt itself from the judicial remedies provisions.

A subtler example of an agency electing not to exempt its records from subsection (g) is observed in the information systems maintained by the Justice Department's Federal Bureau of Investigation (FBI). As an agency almost exclusively dedicated to law enforcement, the FBI has chosen to exempt many of its systems of records from all exemptible provisions.[35] Unlike the EEOC's regulations, subsection (g) is among the listed subsections from which the FBI's records have

---

[32] *See* § 552a(j) ("The head of any [qualified] agency may promulgate rules, in accordance with [general APA requirements] to exempt any system of records within the agency from [any exemptible provision].").

[33] *See* § 552a(j) ("[T]he agency shall include in the statement . . . the reasons why the system of records is to be exempted from a provision of this section.").

[34] Privacy Act of 1974; Publication of Notices and Proposed New Systems of Records, 67 Fed. Reg. 146, 49338 (July 30, 2002).

[35] *See* Exemption of Federal Bureau of Investigation Systems—limited access, 28 C.F.R. § 16.96 (2012) (listing notice and rationales for exemptions for all Federal Bureau of Investigations (FBI) systems).

been exempted.[36] However, a closer look reveals that the exemption is only partial. In listing the reasons for the exemptions for the National DNA Index System, for example, the regulations state that the system is exempted "from subsection (g) *to the extent that this system of records is exempted from the access and amendment provisions of subsection (d)*."[37] In other words, the FBI has exempted itself from civil lawsuit only in cases in which, by definition, the lawsuit would fail on the merits due to exemption from the underlying substantive requirement. It is clear, however, that such a constrained understanding of a subsection (g) "exemption" is equivalent to no exemption at all. It grants agencies an exemption from judicial review of a provision to which they were never subjected.[38] Thus, the FBI has effectively elected to not exempt its records from judicial review, either because it believes it cannot, or because it has made the discretionary election not to exempt.[39]

---

[36] *See, e.g.*, § 16.96(n) ("The following system of records is exempt from 5 U.S.C. 552a . . . (g).").

[37] § 16.96(o) (emphasis added). There is a provision with similar language in the regulations of the Department of Homeland Security. 74 Fed. Reg. 162, 42580 (Aug. 24, 2009) ("Exemptions . . . are justified . . . from subsection (g) to the extent that the system is exempt from other specific subsections of the Privacy Act relating to individuals' rights to access and amend their records contained in the system.").

[38] This confusion between legality and unreviewability is a familiar issue in administrative law. In the context of reviewability under the Administrative Procedure Act, one commentator has described this conflation as "inherently suspect because it renders the concept of unreviewability superfluous: it assumes that the only unreviewable agency actions are ones that would survive review even if the court reached the merits." Ronald M. Levin, *Understanding Unreviewability in Administrative Law*, 74 MINN. L. REV. 689, 734–35 (1990).

[39] In the case of agencies like the FBI, which exempt their records from subsection (g) but appear to subsequently limit themselves to a partial exemption through a narrow statement of rationale, an additional caveat merits mention. The legal relevance of the subsequent limitation is not settled law. Some courts have recognized full exemptions even though the agency's rationale implied that the exception was significantly narrower. *See, e.g.*, Wentz v. Dep't of Justice, 772 F.2d 335 (7th Cir. 1985) (permitting an agency to rely on its exemption in dismissing an amendment suit, even though its rationale only mentioned access suits). However, other courts have been less willing to extend an exemption beyond its explicitly given rationale. *See, e.g.*, Fendler v. U.S. Bureau of Prisons, 846 F.2d 550, 553 (9th Cir. 1988) (stating that the agency had only partially exempted its records from subsection (g) because the agency's stated reasoning for exempting itself from subsection (g) "has nothing to do with enforcement of subsection (e)(5)"); Ryan v. Dep't of Justice, 595 F.2d 954, 958 (4th Cir. 1979) (holding that the agency had not exempted its system from civil review for an unlawful disclosure violation, because the agency had only exempted its records from subsection (g) "to the extent that those provisions would have applied to enforce access under [§] 552a(d)").

C. *Judicial Responses: Hostility Toward the Complete Exemption*

The only two courts of appeals to have directly confronted the question of the complete subsection (g) exemption concluded that agencies lack the statutory authority to so exempt their records. The details of these courts' arguments are discussed (and critiqued) more thoroughly in Part II, but will briefly be discussed in this section.

The D.C. Circuit Court of Appeals became the first federal appellate court to consider the issue in *Tijerina v. Walters*,[40] which concerned a plaintiff who had been deemed unsuitable to sit for the Texas Bar, allegedly because of information disclosed to the Bar Examiners by the Veterans Administration (VA), asserting that Tijerina had committed fraud in a VA housing loan request. The system of records containing Tijerina's information was maintained principally for the purpose of investigating fraud, and for that reason the VA had permissibly exempted the system from all exemptible provisions of the Privacy Act, including subsection (g).[41] The court rejected the government's argument that a qualified agency could completely immunize itself from civil judicial review, holding that "a government agency cannot employ subsection (j) to exempt itself from subsection (g)'s provision for civil liability for violations of the Act."[42] While the court claimed that the plain text of the statute was a sufficient basis on which to ground its opinion,[43] it focused a great deal on what it held to be the strong normative and consequentialist arguments against permitting the full exemption—that permitting the exemption would seriously weaken the Privacy Act's force.[44]

Almost a quarter-century later, the Sixth Circuit in *Shearson v. U.S. Department of Homeland Security*[45] reached the same conclusion, with largely identical reasoning. In *Shearson*, the plaintiff alleged that the Department of Homeland Security and Customs and Border Protection had unlawfully maintained documents about the plaintiff, ultimately leading to her and her daughter's detention.[46] When confronted with the argument that the suit must fail because the agencies had exempted their records from subsection (g), the Sixth Circuit reversed the trial court and held that the agencies "could not properly

---

40 821 F.2d 789 (D.C. Cir. 1987).

41 *Id.* at 795. The VA provided the notice of and justification for the exemption in 47 Fed. Reg. 24011–13.

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

43 This argument, that the complete subsection (g) exemption is foreclosed by the plain meaning of the statute, is critiqued *infra* notes 52–57.

44 These arguments, that the complete subsection (g) exemption would have unwanted consequences, are critiqued *infra* Part III.

45 638 F.3d 498 (6th Cir. 2011).

46 *See id.* at 499–500 (describing plaintiff's allegations).

exempt the [systems of records] from civil liability for violating these sections."[47] Although other courts have articulated a contrary conclusion, that the complete subsection (g) exemption *is* permissible, these statements were all in dicta.[48]

II
A Better Answer—Interpreting the Privacy Act

Part II of this Note looks beyond the current interpretation of the interplay between subsections (g) and (j) and instead focuses on the correct interpretation of those provisions. The question of the legality of the complete subsection (g) exemption has been treated, as it should, largely as a question of statutory interpretation. Despite the seemingly straightforward nature of this inquiry, however, there are a variety of tools used to discern either the "semantic meaning"[49] or the legislative "purpose"[50] of the text, depending on one's jurisprudential fancy. This Note remains agnostic on the relative merits of these mechanisms, and argues that all methods support the complete subsection (g) exemption, albeit to varying degrees.

A. Plain Meaning of the Privacy Act

The plain meaning of subsection (j) would allow eligible agencies to exempt their records from subsection (g) in its entirety. Subsection (j) grants broad exemption authority and then lists the portions of the Privacy Act from which qualifying agencies may *not* exempt their records—subsection (g) is "conspicuously absent from [this] list."[51] Without serious question then, a plain reading of the statute would

---

[47] *Id.* at 506.

[48] In these cases, the courts stated that while qualified agencies are *permitted* to completely exempt their records from subsection (g), the agency in the particular case had not done so. *See, e.g.*, Kimberlin v. Dep't of Justice, 788 F.2d 434, 436 n.2 (7th Cir. 1986) ("Information systems can be exempted from the civil remedies section of the Privacy Act, 5 U.S.C. § 552a(g), pursuant to § 552a(j). However . . . the exemption listed for the inmate commissary account does not apply here."); Ryan v. Dep't of Justice, 595 F.2d 954, 958 (4th Cir. 1979) ("Although the Justice Department could have exempted [its system] from the application of the [§] 552a(g) civil remedies to a § 552a(b) wrongful disclosure violation, it failed to do so as required by [§] 552a(j) and cannot now claim such an exemption."). Perhaps because these statements were ultimately not tied to the outcome of the case, these courts did not discuss the reasoning behind their conclusions.

[49] *See, e.g.*, John F. Manning, *What Divides Textualists from Purposivists?*, 106 Colum. L. Rev. 70, 92 (2006) (noting the textualist view that "a statute may have a clear semantic meaning, even if that meaning is not plain to the ordinary reader without further examination").

[50] *See, e.g.*, Comm'r v. Sternberger, 348 U.S. 187, 206 (1955) (stating that in certain situations, a court should "follow the purpose [of a statute] rather than the literal words").

[51] *See Shearson*, 638 F.3d at 502 (admitting the relevance of the provision's absence before concluding that the provision should nonetheless be nonexemptible).

lead to the conclusion that eligible agencies may exempt themselves from subsection (g) and with it, all civil remedies for Privacy Act violations.

Despite this clarity, two circuit courts of appeals have concluded that even the *plain meaning* of the Privacy Act dictates that subsection (g) may not be fully exempted. In *Tijerina*, the D.C. Circuit boldly declared that permitting a full exemption would "tortur[e] the language of the Act."[52] In *Shearson*, the Sixth Circuit was less forceful, admitting that subsection (g)'s absence from subsection (j) at least "[gave it] pause," but ultimately concluded that it was unconvinced that the statute's plain language pointed towards allowing the exemption.[53] In reaching these somewhat surprising conclusions regarding the plain meaning of the Privacy Act's text, the courts relied in large part on two facts about the language of the Act. While both of these facts are true, they are both nonsequiturs, and fail to lead to the conclusion that the broad exemption authority of subsection (j) should not extend to subsection (g).

The first argument courts and commentators have articulated is that subsection (j) exempts certain agencies' systems of records as opposed to exempting the agencies themselves.[54] This is undoubtedly true.[55] For example, an agency may elect to exempt one system of records, but not another. The focus on systems of records reflects the fact that in the Privacy Act, the "unit of measurement" is a system of records, as opposed to agencies' whole cloth. However, the issue of what may be exempted (unquestionably a system of records) is orthogonal and unrelated to the issue of from what it may be exempted (the issue of subsection (g)). In other words, the "limitation" that agencies may only exempt systems of records is entirely consistent with the textually supported conclusion that agencies may

---

[52] Tijerina v. Walters, 821 F.2d 789, 796 (D.C. Cir. 1987).

[53] *See Shearson*, 638 F.3d at 503 (concluding that Congress's exclusion of subsection (g) from the list is "not instructive").

[54] *See, e.g.*, *Tijerina*, 821 F.2d at 795 ("The language of the Act does not indicate, as the government contends, that an agency . . . may exempt *itself* from all provisions of the Privacy Act. Subsection (j) only permits an agency to exempt a *system of records* from the requirements set out in other provisions of the Act." (emphasis added)); Nakash v. Dep't of Justice, 708 F. Supp. 1354, 1359 (S.D.N.Y. 1988) (emphasizing that subsection (j) applies to *systems of records* and describing the government as arguing that the Department of Justice should be permitted "to exempt itself"); *see also* Maxim Brumbach, Comment and Casenote, *Are You on the List?: Dispelling the Myth of a Total Exemption from the Privacy Act's Civil Remedies in* Shearson v. DHS, 81 U. CIN. L. REV. 1027, 1043 (2013) (calling this line of reasoning "the simplest and strongest" argument against permitting a complete exemption).

[55] *See* 5 U.S.C. § 552a(j) (2012) ("The head of any [qualifying] agency may promulgate rules . . . to exempt any *system of records* . . . ." (emphasis added)).

exempt their systems of records from judicial review. Thus, the argument is a red herring.

The second equally unconvincing argument posits that subsection (g) is a remedial provision, as opposed to a substantive provision.[56] Once again, this is technically a true statement, but it says nothing about whether subsection (g) can be exempted. The argument relies on the tacit assumption that subsection (j) exempts substantive requirements but not remedial provisions. But the statute does not make this distinction. On the contrary, subsection (j) says that a system of records may be exempted "from any *part* of [the Act]."[57] A substantive requirement and a remedial provision are equally "parts" of the Act, and thus, the plain language of subsection (j) applies to both.

B. Legislative History of the Privacy Act

Despite the protestations of the D.C. and Sixth Circuits, the plain meaning of subsections (g) and (j) permits qualifying agencies to exempt themselves from the latter. The legislative history, to the contrary, is more equivocal. Congressional debate surrounding the passage of the Privacy Act was admittedly rushed,[58] and at no time was the question of the interplay between subsections (g) and (j) directly considered.[59] Nevertheless, several courts ruling against the complete subsection (g) exemption have relied on the assertion that the legislative history of the Act in fact points in favor of their view.[60] For that reason, this section of the Note is primarily defensive, arguing against the notion that the exemption is "[in]consistent with [the Act's] underlying purpose and legislative history."[61]

---

[56] *See, e.g.*, *Shearson*, 638 F.3d at 503 ("[Section] 552a(g) provides for civil remedies; it does not impose substantive obligations. Congress's omission of § 552a(g) from the list of non-exemptible provisions in § 552a(j) is therefore not instructive.").

[57] § 552a(j).

[58] *See* DOJ PRIVACY ACT OVERVIEW, *supra* note 4, at 1 ("The Act was passed in great haste during the final week of the Ninety-Third Congress.").

[59] *See, e.g.*, *Nakash*, 708 F. Supp. at 1360 ("There is no discussion in which Congress explicitly states that an agency cannot do what the Government claims the Department of Justice has done [exempt its records from subsection (g)]. Conversely, however, there is absolutely no indication in the extensive debates . . . that Congress even considered such a disturbing possibility.").

[60] *See, e.g.*, Tijerina v. Walters, 821 F.2d 789, 797 (D.C. Cir. 1987) ("The Act's . . . legislative history persuade[s] us that the government is urging a completely anomalous use of the exemption provision . . . ."); *Nakash*, 708 F. Supp. at 1359–61 (admitting that the legislative history is not perfectly clear but concluding that as a whole it leans towards rejection of the complete exemption).

[61] *Nakash*, 708 F. Supp. at 1359.

As a general matter, the legislative history these courts cite does not lead to the ultimate conclusion at which they arrive. For example, the district court in *Nakash v. United States Department of Justice* quoted the House Report which states: "Only records maintained by the Central Intelligence Agency and criminal justice records could be . . . exempted. *Even they would be subject to the requirements relating to conditions of disclosure*."[62] Likewise, the D.C. Circuit in *Tijerina* focused on the above emphasized sentence as indicating a congressional intent to "forb[id] agencies to exempt systems of records from disclosure."[63] The court believed that this sentence was evidence that qualified agencies would be subjected to civil judicial review. But this is not what the sentence says at all. It is beyond dispute that qualified agencies are substantively obligated to comply with disclosure requirements.[64] What is at issue—and what is not addressed by the emphasized sentence—is the availability of a judicial damages remedy for a violation of that provision.[65] It would not be irrational for Congress to have believed in the importance of the substantive requirement, and at the same time to have been hesitant to authorize courts to be the arbiters of whether the requirement has been met.[66]

The one statement made during the debate arguably on point is likely unreliable. Representative Bella Abzug, one of the Act's sponsors, spoke in support of an amendment she offered, which would have eliminated the general exemption provisions altogether. Discussing the status quo, which she sought to change through her amendment, she stated:

> By setting up a general exemption guaranteeing and allowing the CIA [among other agencies] to exempt even sensitive records from virtually every provision of the bill, the bill goes far beyond what is necessary to protect such records from disclosure . . . . Why should the agency be exempted from a bar against maintaining political or religious data if other agencies are not, *and why should individuals be denied rights to civil remedies and court review*?[67]

---

[62] *Id.* at 1361.

[63] *Tijerina*, 821 F.2d at 797.

[64] *See supra* notes 14–15 and accompanying text (explaining how the anti-disclosure rules are nonexemptible and thus applicable to all agencies).

[65] For a more detailed discussion of this distinction, see *infra* notes 100–13.

[66] A relatively well-known example of this phenomenon can be seen in the Department of Veterans Affairs, which had historically "barred veterans who were denied disability benefits from seeking judicial review." Nicholas Bagley, *The Puzzling Presumption of Reviewability*, 127 HARV. L. REV. 1285, 1288 (2014). "The absence of review was thought to be an essential feature of an efficient, easy-to-navigate, and nonadversarial process for resolving disability claims." *Id.*

[67] *See* LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, at 938–39 (emphasis added), *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

This statement appears to demonstrate that Representative Abzug believed that the general exemptions, which would eventually become subsection (j), embraced an exemption for civil review, which would eventually become subsection (g). Though the statements of a sponsor might usually hold considerable weight,[68] the context of Representative Abzug's statements, in which she was arguing for a limiting amendment, cast doubt on the veracity of her observations. Abzug was quite reasonably motivated to rhetorically overstate the exemption she was trying to limit. Therefore, although her speech supports this Note's understanding of subsections (g) and (j), one should not ground that understanding solely in this piece of legislative history.

Courts rejecting the complete exemption have also argued that the legislative history evinces a narrow purpose for the general exemption, one that is not furthered by permitting an exemption for civil remedies. In its discussion of what would become the subsection (j) general exemption, the Senate Committee on Government Operations stated that "[i]n particular, it would not be appropriate to allow individuals to see their own intelligence or investigative files. Therefore the bill exempts such information from access and challenge requirements . . . ."[69] One could draw from this excerpt the existence of a discrete and narrow rationale for the existence of subsection (j)—the elimination of the possibility that criminals being investigated by the federal government could get a jump-start on discovery by requesting that the relevant agency turn over its investigative files. But the quoted passage does not suggest, let alone mandate, such a narrow reading. It makes perfect sense that the Committee would choose to highlight the most compelling rationale for the exemption; it does not follow that it is the *only* such rationale. The excerpt is not inconsistent with the assertion that law enforcement agencies have been given flexibility to bypass not only the most obvious burdens of forced disclosure and amendment, but also the less salient burden of judicial review generally.

---

[68] *See, e.g.*, William N. Eskridge, Jr., *The New Textualism*, 37 UCLA L. REV. 621, 636–37 (1990) (ranking sponsor statements second in a "hierarchy of legislative history sources," behind only committee reports).

[69] SENATE COMMITTEE ON GOVERNMENT OPERATIONS, *Report: Protecting Individual Privacy in Federal Gathering, Use and Disclosure of Information*, *in* LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974, at 176, *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf. *See also id.* at 154 (discussing the purpose of the bill).

C. Administrative Deference

In the realm of administrative law, courts possess a built-in tool for resolving textual ambiguity: deference to the interpretations of federal agencies. While there is debate as to how much ambiguity is sufficient to trigger deference,[70] it is clear that assuming some requisite level of ambiguity, a reviewing court should accede to any reasonable agency interpretation.[71]

The Office of Management and Budget (OMB) is tasked to "develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing [the Privacy Act]."[72] In accordance with this mandate, OMB promulgated guidelines for implementation of the Privacy Act, which it published in 1975.[73] Notwithstanding the label of this document as "guidance," the guidelines are given "the deference usually accorded interpretation of a statute by the agency charged with its administration."[74]

Although OMB's position on the complete subsection (g) exemption should resolve a sufficient statutory ambiguity, OMB's precise position is unclear. In discussing general exemptions under subsection (j), the guidelines state that records fitting into this category "may be exempted from the civil remedies provision and, in particular, the judicial review under subsections (g)(1)(b) and (g)(3), civil remedies."[75] At first glance, this appears to definitively resolve the issue in favor of an agency seeking a complete exemption from civil judicial review, and the Department of Justice Guidance has implied that it does.[76] However, it is possible to read this statement as merely author-

---

[70] *See* Cass R. Sunstein & Thomas J. Miles, *Depoliticizing Administrative Law*, 58 DUKE L.J. 2193, 2220–22 (2009) (discussing complexities and uncertainty in court's application of deference doctrines).

[71] *See* Chevron, U.S.A., Inc. v. NRDC, Inc., 467 U.S. 837, 842–43 (1984) (describing the deference which should be awarded to agencies' reasonable interpretations of their governing statutes).

[72] 5 U.S.C. § 552a(v) (2012).

[73] *See* OFFICE OF MGMT. & BUDGET, PRIVACY ACT IMPLEMENTATION: GUIDELINES AND RESPONSIBILITIES, *available at* http://www.whitehouse.gov/sites/default/files/omb/assets/omb/inforeg/implementation_guidelines.pdf (providing guidelines and interpretations of all provisions of the Privacy Act).

[74] Albright v. United States, 631 F.2d 915, 920 n.5 (D.C. Cir. 1980); *accord* Sussman v. United States Marshals Serv., 494 F.3d 1106, 1120 (D.C. Cir. 2007) (quoting *Albright*). While not mentioned by name in these decisions, it is implied that *Chevron v. NRDC*, 467 U.S. 837 (1984), dictates the level of deference that should be given to OMB.

[75] PRIVACY ACT IMPLEMENTATION: GUIDELINES AND RESPONSIBILITIES, *supra* note 73, at 28971.

[76] *See* DOJ PRIVACY ACT OVERVIEW, *supra* note 4, at 270 (citing OMB's guidance for the proposition that "the language of subsection (j) appears to permit" the complete subsection (g) exemption).

izing a *partial* subsection (g) exemption—namely exempting review for violations of substantive provisions from which the agency has exempted its records. Indeed, some courts have expressed the interplay of subsections (g) and (j) in this manner.[77] However, even if the OMB guidance does not itself unambiguously embrace the complete subsection (g) exemption, it does foreclose one particular argument against it: that subsection (j) only applies to substantive, as opposed to remedial, provisions.[78] By stating that agencies may (even partially) exempt their records from civil review, the OMB guidance has definitively denied that subsection (j) is implicitly limited to substantive provisions. As stated above, one line of argumentation offered by the Sixth Circuit tacitly relies on that exact assumption.[79]

D. Interpretations Concerning the Availability of Judicial Review

If subsections (g) and (j) were ordinary statutory provisions, the above analysis would be sufficient for the conclusion that an agency may exempt its records from all those subsections not explicitly listed, including civil judicial review provisions. The plain meaning of the text clearly supports this view, and the legislative history and administrative guidance at worst are equivocal.

However, subsection (g) is not an ordinary statutory provision, but rather concerns the availability of judicial review of an agency's action.[80] A wealth of literature exists on the special manner in which legal text should be interpreted when it concerns the availability of judicial review.[81] In its most famous articulation, the Supreme Court ostensibly adopted a rebuttable presumption in favor of the availa-

---

[77] *See, e.g.*, Shearson v. Dep't of Homeland Sec., 638 F.3d 498, 504 (6th Cir. 2011) ("[A]n agency is permitted to exempt a system of records from the civil-remedies provision if the underlying substantive duty is exemptible under § 552a(j) . . . ."). This would admittedly be an odd and rather useless exemption—given the fact that judicial review could only be prevented when a suit would assuredly lose on the merits anyway. *See supra* note 38 and accompanying text (discussing the illogic of this understanding of the subsection (g) exemption).

[78] *See supra* notes 45–47 and accompanying text (discussing this particular argument made by the Sixth Circuit).

[79] *Id.*

[80] For a discussion of subsection (g)'s characterization as a judicial review provision, see *infra* notes 93–98 and accompanying text.

[81] *See generally* Nicholas Bagley, *The Puzzling Presumption of Reviewability*, 127 HARV. L. REV. 1285 (2014) (challenging the presumption of judicial reviewability of agency action); *see also* Thomas W. Merrill, *Delegation and Judicial Review*, 33 HARV. J. L. & PUB. POL'Y 73, 73 (2010) (noting that broad delegations are often justified based on the presumption of reviewability of agency action); Ashutosh Bhagwat, *Three-Branch Monte*, 72 NOTRE DAME L. REV. 157, 157–59 (1996) (describing and criticizing the Supreme Court's establishment of a distinct set of textual presumptions in the area of review of decisions of nonenforcement).

bility of review, stating that "judicial review of a final agency action by an aggrieved person will not be cut off unless there is persuasive reason to believe that such was the purpose of Congress."[82] The syllogism against the complete subsection (g) exemption is straightforward: *Abbott Laboratories* dictates that ambiguities should be resolved in favor of judicial review.[83] The complete subsection (g) exemption would eliminate judicial review in some cases. Therefore, the Privacy Act should be interpreted so as not to authorize the complete subsection (g) exemption.

It is beyond the scope of this Note to challenge the presumption of reviewability, but it merits mention that the presumption has its critics who attack it as both unfounded[84] and unwise.[85] Even assuming that the presumption does exist, it does not follow that qualifying agencies cannot completely exempt their records from subsection (g). First, notwithstanding the presumption of reviewability, the Supreme Court has recognized the existence of implicit preclusion of judicial review.[86] Because even Congressional silence on the issue of judicial review is not necessarily sufficient to mandate review, an affirmative denial of judicial review, even an ambiguous one, is not enough to absolutely trigger the presumption.

More fundamentally, the argument relying on the presumption of judicial review ignores the key fact that the particular provision at issue here—subsection (g)(1)(D)—not only authorizes judicial review, but also waives sovereign immunity.[87] And waivers of sovereign immunity involve precisely the opposite presumption of that of judicial review generally; these waivers must be "construed strictly in favor of the sovereign," and in order to be effective, the waiver must be "unequivocally expressed."[88] In the context of the Privacy Act, this

---

[82] *See* Abbott Labs. v. Gardner, 387 U.S. 136, 140–41 (1967) (citing six different Supreme Court decisions articulating this position).

[83] *Id*.

[84] *See* Bagley, *supra* note 81, at 1288 (noting "[t]he absence of support for the presumption of reviewability").

[85] *See id.* at 1336 (describing the presumption as "harmful in practice").

[86] *E.g.*, Block v. Cmty. Nutrition Inst., 467 U.S. 340, 349 (1984) ("[T]he presumption favoring judicial review of administrative action may be overcome by inferences of intent drawn from the statutory scheme as a whole.").

[87] Tomasello v. Rubin, 167 F.3d 612, 618 (D.C. Cir. 1999). Moreover, plaintiffs may not bootstrap their Privacy Act claims to other statutes that waive sovereign immunity, such as the Federal Torts Claims Act. *See* Tripp v. United States, 257 F. Supp. 2d 37, 44 (D.D.C. 2003) ("[A] federal statute [like the Privacy Act] which provides for a private right of action against the government cannot, without more, create a duty on the part of the federal government giving rise to tort liability under the FTCA.").

[88] *See* United States v. Nordic Village, Inc., 503 U.S. 30, 33–34 (1992) (making this observation in the context of a bankruptcy proceeding against the Internal Revenue Service).

presumption against the waiver of sovereign review has led the D.C. Circuit to adopt a narrow reading of the civil remedies provision, despite a wider reading being "linguistically possible."[89] For that reason, opponents of the complete subsection (g) exemption cannot rely on any presumptions in favor of judicial review to resolve an interpretive question.

III
Settling Anxieties—The Lack of Judicial Enforcement Is Not a Disaster

With the risk of oversimplification, the shift from Part II to Part III is a shift from a discussion of law to a discussion of policy. Some critics of the complete subsection (g) exemption—both judicial[90] and academic[91]—have argued that not only would it be unlawful to allow the exemption, it would also be disastrous. A thorough defense of the complete subsection (g) exemption must meet these attacks as well; this Note does so in Part III.

The policy-based defense of the complete subsection (g) exemption is accomplished in two parts. First, Part III.A adopts a theoretical focus. It discusses and critiques an incorrect conflation of substantive illegality with the availability of judicial review. Part III.A also outlines compelling reasons why the enforcement of the Privacy Act's dictates might best be left in the hands of the nonjudicial branches. Part III.B turns to specifics, outlining several nonjudicial methods of enforcement of the Privacy Act, and describing their various successes.

A. Theory

1. Civil Suits as a Form of Judicial Review

Part III of this Note posits that the complete subsection (g) exemption is both legally mandated and normatively acceptable, given that nonjudicial institutions can enforce the boundaries of the Privacy Act in lieu of judicial review. This argument presupposes, however, that subsection (g)(1)(D), which authorizes civil lawsuits against the

---

[89] *See Tomasello*, 167 F.3d at 618. In that case, the plaintiff argued that each copy of a document that was disclosed counted as a separate illegal act for which he was entitled to the statutory minimum of $1000. The court was not convinced, and it ruled that the series of disclosures counted as a single act for purposes of calculating damages, citing the canon of narrowly construing waivers of sovereign immunity. *Id.* at 617–18.

[90] *See, e.g.*, Nakash v. Dep't of Justice, 708 F. Supp. 1354, 1360 (S.D.N.Y. 1988) (describing the complete exemption as a "disturbing possibility").

[91] *See, e.g.*, Brumbach, *supra* note 54, at 1042 (describing the complete exemption as a "loophole").

United States government for damages,[92] is a form of judicial review. Injunctive relief in the form of pre-enforcement review of an agency's final action—such as that authorized by the Administrative Procedure Act[93]—might be a more familiar form of judicial control.[94] There are critical differences between that type of ex ante restraint of judicial action and the ex post awarding of damages at issue in subsection (g)(1)(D), including differences in the deterrent effect on agency behavior.[95] Nonetheless, these differences distinguish civil damage suits from injunctive judicial review only in degree.[96] While perhaps the primary goal of damage suits is to compensate victims, these monetary suits share other goals in common with judicial review more generally, including deterrence of wrongdoing and "affirm[ing] the vitality of the rule of law."[97] More fundamentally, monetary damages against officials or the government itself have "become important instruments by which courts can control administrative behavior."[98]

2. Decoupling Substantive Importance from Procedural Remedy

Courts that hold that qualified agencies may not exempt their records completely from subsection (g) put forth consequentialist arguments along with their more "traditional" interpretive reasoning.[99] These courts articulate a fear that by refraining from enforcing the nonexemptible provisions of the Privacy Act, the courts would be in effect blessing and encouraging agencies to violate the law. For example, in *Tijerina v. Walters*, the D.C. Circuit expressed its anxiety that a complete subsection (g) exemption would "defang completely the strict limitations on disclosure that Congress intended to

---

[92] *See* 5 U.S.C. § 552a(g)(4) (stating that if a court finds a violation, "the United States shall be liable to the individual in an amount equal to the sum of . . . actual damages . . . and the costs of the action").

[93] *See* § 706 (authorizing courts to *inter alia* "set aside agency action, findings, and conclusions found to be [unlawful]").

[94] *See, e.g.*, Sackett v. EPA, 132 S. Ct. 1367, 1374 (2012) (authorizing pre-enforcement review of the EPA's issuance of a compliance order).

[95] *See* ADRIAN VERMEULE, THE CONSTITUTION OF RISK 73 (2014) ("[I]t is wrong . . . to assume that there is no difference between ex ante precautionary regulation and a system of ex post sanctions.").

[96] In his seminal work on civil remedies against government, Peter Schuck places damage suits along a spectrum with all other forms of judicial review. PETER H. SCHUCK, SUING GOVERNMENT 14 (1983). Schuck ranks the possible remedial forms by their "judicial intrusiveness." *Id.* Only declaratory judgments are less intrusive than ex post money damages. *Id.*

[97] *Id.* at 22–23.

[98] *Id.* at 52.

[99] For a discussion of this traditional interpretive reasoning, see *supra* Part II.

impose."[100] The Southern District of New York announced a similar consequentialist rationale for denying the complete exemption.[101]

The error of the logic espoused in these cases is the implicit assumption that the value and importance of a substantive right should be proportional to the availability of judicial review. Courts that strike down the subsection (g) exemption go to great lengths to thoroughly defend their conclusion that freedom from unlawful disclosure of information is a vital right from which agencies cannot exempt themselves.[102] At the same time, they ignore the inferential step that this importance somehow removes from the table the possibility of solely nonjudicial enforcement. This is in line with what some academics label the "court-centric" view, in which the judiciary, as opposed to other institutions, "act[s] as a brake on runaway bureaucracies, forcing them to follow the substantive and procedural requirements imposed on them by Congress."[103] This view is stated quite forcefully: For those in the court-centric camp, "[a]ny gap between right and remedy, any lacuna in the remedial regime, disturbs the moral and logical symmetry of the legal order and profoundly disturbs its authority."[104]

Yet, there are those who challenge the court-centric assumption, arguing for a disaggregation of substantive legal norms from the remedial source of the judiciary.[105] In the realm of rights created by statute, this is a rather uncontroversial notion as Congress—the source of the right itself—has almost plenary power to limit its remedy.[106] But even if one conceives of the Privacy Act as a fundamental public law whose

---

[100] *See* Tijerina v. Walters, 821 F.2d 789, 797 (D.C. Cir. 1987) (providing this rationale for rejecting the government's textual argument).

[101] *See* Nakash v. Dep't of Justice, 708 F. Supp. 1354, 1361 (S.D.N.Y. 1988) (focusing on the importance of the anti-disclosure provision and warning that the complete exemption would "weaken" the enforcement of that provision).

[102] *See Tijerina*, 821 F.2d at 796 (explaining why Congress elected to make unlawful disclosure a nonexemptible provision); *Nakash*, 708 F. Supp. at 1360–61 (drawing on legislative history to argue for the importance of the nondisclosure provisions).

[103] *See* J.R. DeShazo & Jody Freeman, *The Congressional Competition to Control Delegated Power*, 81 TEX. L. REV. 1443, 1459–60 (2003).

[104] SCHUCK, *supra* note 96, at 26.

[105] *See, e.g.*, Dawn E. Johnsen, *Faithfully Executing the Laws: Internal Legal Constraints on Executive Power*, 54 UCLA L. REV. 1559, 1562 (2007) (arguing that, because of limits on the ability of Congress and the courts to adequately protect individual rights, an "essential source of constraint" on executive illegality is the community of legal advisors within the executive branch itself).

[106] *See, e.g.*, Alexander v. Sandoval, 532 U.S. 275, 286–87 (2001) (stating that, without a congressionally-created remedy, "a cause of action does not exist, and courts may not create one, no matter how desirable that might be as a policy matter, or how compatible with the statute"); *cf.* Bivens v. Six Unknown Named Agents of Fed. Bureau of Narcotics, 403 U.S. 388, 407 (1971) (Harlan, J., concurring) (noting that "the judiciary has a particular responsibility to assure the vindication of constitutional interests" which may require a

provisions are more akin to constitutional rights,[107] the availability of a judicial forum is not predetermined. Professor Trevor Morrison identifies a range of constitutional questions that are not justiciable.[108] The most obvious example is the political questions doctrine, in which federal courts are instructed to ignore certain cognizable rights claims, directing enforcement of those rights to the political branches.[109] Another example are doctrines concerning the nonretroactivity of "new law," in which courts intentionally withhold remedies arising from newly recognized constitutional rights, even if those rights substantively exist.[110] As Professor Morrison notes, however, the lack of judicial enforcement "does not license [executive branch officials] to ignore the questions or to answer them without regard to the law. Instead, they 'must make a conscious decision to obey the Constitution whether or not their actions can be challenged in a court of law . . . .'"[111] Some have argued that this minimalistic role for the judiciary is in fact a more accurate portrayal of the constitutional understanding at the time of the Framing.[112] Regardless of the perceived scope of nonjusticiability canons and doctrines, the important takeaway is the notion that statutory and constitutional enforcement

broader conception of civil remedies than for violations of statutes, even absent "express congressional authorization").

107 *See* VERMEULE, *supra* note 95, at 17 (noting that, because public law concerns "the relationships . . . between officials and citizens," it can be thought of as being part of "constitutionalism in its widest sense").

108 *See* Trevor W. Morrison, Book Review, *Constitutional Alarmism*, 124 HARV. L. REV. 1688, 1695 (2011) ("Officials within the executive branch often face constitutional questions that the federal courts would treat as nonjusticiable on political question or other grounds.").

109 *See, e.g.*, Baker v. Carr, 369 U.S. 186, 210 (1962) (describing and attempting to define the political questions doctrine). *But see* Rachel E. Barkow, *More Supreme than Court? The Fall of the Political Question Doctrine and the Rise of Judicial Supremacy*, 102 COLUM. L. REV. 237 (2002) (expressing the view that the modern Supreme Court has disregarded the political questions doctrine in favor of robust judicial power).

110 *See generally* Richard H. Fallon, Jr. & Daniel J. Meltzer, *New Law, Non-Retroactivity, and Constitutional Remedies*, 104 HARV. L. REV. 1731, 1734–35 (1991). Among other examples of these "new law" doctrines, Fallon and Meltzer identify both the qualified immunity doctrine and the federal habeas corpus nonretroactivity principle as examples of ways in which courts are directed "to deny relief without deciding whether a constitutional violation has in fact occurred." *Id.* at 1735. Indeed, the Supreme Court has reaffirmed the notion that nonretroactivity "is primarily concerned, not with the question of whether a constitutional violation occurred, but with the availability or nonavailability of remedies." Danforth v. Minnesota, 552 U.S. 264, 290–91 (2008).

111 Morrison, *supra* note 108, at 1695–96 (citing Hein v. Freedom from Religion Found., Inc., 551 U.S. 587, 618 (2007) (Kennedy, J., concurring)).

112 *See* Larry D. Kramer, *The Supreme Court 2000 Term Foreword: We the Court*, 115 HARV. L. REV. 4, 74 (2001) ("[T]he idea of depending on courts to stop a legislature that abused its power simply never occurred to the vast majority of participants in the debates [during the Framing].").

can certainly be robust and meaningful even outside of the courts.[113] The logic of these broader and more general nonjusticiability doctrines applies with similar force to the much narrower issue of the enforcement of the Privacy Act against qualified agencies. Therefore, the *Tijerina* decision and others like it are incorrect in their conclusion that the importance of the disclosure rules and other nonexemptible provisions of the Privacy Act is sufficient evidence that the judiciary must be the institution that polices and enforces those rules.

3. Moving Away from the Courts in the Field of Civil Remedies

The distinction between rights and remedy does not collapse when moving from a discussion of appellate-style judicial review to one of ex post remedies for unlawful government action. As stated above, civil remedies are a form of judicial review, and like all judicial review, availability is not predetermined by the existence of a legal wrong.[114] Professors Richard Fallon and Peter Schuck have each advanced robust theories of remedies in which remedial designers must make decisions that implicate multiple functions and goals. Writing with Daniel Meltzer, Professor Fallon notes the existence of two sometimes competing principles of judicial review: on one hand, the availability of a judicial remedy for every rights violation, and on the other, a system of remedies that is "adequate to keep government generally within the bounds of law."[115] This latter principle is the more "unyielding" of the two, and can sometimes "tolerate the denial of particular remedies, and sometimes of individual redress."[116] In Part III.B, this Note argues against the necessity of civil remedies in a manner very consistent with this second principle, as nonjudicial actors may serve as a sufficient check on governmental unlawfulness.

---

[113] Of course, this Note does not argue that the claims that would be foreclosed by the complete subsection (g) exemption are nonjusticiable in a constitutional sense. Rather the argument is that judicial review has been foreclosed through federal legislation and regulation; the comparison to nonjusticiability doctrines is merely one of analogy.

[114] *See* MICHAEL L. WELLS & THOMAS A. EATON, CONSTITUTIONAL REMEDIES: A REFERENCE GUIDE TO THE UNITED STATES CONSTITUTION xviii (2002) ("[T]he policy considerations bearing on what remedies should be available may be quite different from the matters of principle that determine the outcome of disputes over the scope of constitutional rights.").

[115] *See* Fallon & Meltzer, *supra* note 110, at 1778–79 (explaining the logic and sources of both of these principles).

[116] *Id.* at 1779; *see also* Richard H. Fallon, Jr., *Of Legislative Courts, Administrative Agencies, and Article III*, 101 HARV. L. REV. 915, 954 ("[S]overeign prerogatives and functional necessities may preclude judicial review of government lawbreaking.").

Peter Schuck, on the other hand, identifies five separate policy goals of government remedies.[117] One of Schuck's major contributions is his observation that "the form of a public tort remedy profoundly affects how a court can use it to influence official behavior."[118] In other words, the ideal form of an enforcement mechanism does not flow as a matter of deductive logic from a substantive right; rather, the best enforcement method will depend on ultimate policy goals as well as empirical assumptions made about the behavioral tendencies of institutions and actors.[119] The limitation of Schuck's contribution is that he makes this point within the context of judicial remedies alone—thus falling victim to the court-centric model.[120] Expanding the range of possible methods of securing Privacy Act compliance beyond the courtroom walls may allow for the possibility of better optimizing enforcement, along all of the dimensions Schuck identifies.[121]

It should be noted that there is one criterion identified by Schuck by which nonjudicial enforcement of the nonexemptible provisions of the Privacy Act is likely inferior: that of compensating victims of Privacy Act violations. To the extent that a qualified agency's violation of the disclosure provision of the Act directly causes monetary harm to an individual, the complete subsection (g) exemption would permit that violation to go uncompensated. It would be inapposite to compare the level of victim compensation in a no-judicial-review paradigm to a hypothetical situation in which all victims of Privacy Act violations are perfectly compensated for their injuries, as this latter

---

117 They are as follows: "to deter wrongdoing, to encourage vigorous decisionmaking by officials, to compensate victims of official misconduct, to exemplify society's moral principles, and to achieve institutional competence and legitimacy." SCHUCK, *supra* note 96, at 16. It is rarely possible to independently maximize each of these goals, and tradeoffs are required, which implicates a sixth goal: "to achieve the optimal mix of these other preeminent values." *Id.*

118 *Id.* at 13.

119 *See* ADRIAN VERMEULE, JUDGING UNDER UNCERTAINTY: AN INSTITUTIONAL THEORY OF LEGAL INTERPRETATION 233 (2006) ("Whether, and to what extent, judicial review is desirable turns upon a range of empirical and institutional variables, including the agency costs, error costs, and decision costs of the alternative regimes, moral-hazard effects, the optimal rate of legal change, the costs of transition from one regime to another, and the relative capacities of legislatures and courts at updating obsolete constitutional provisions.").

120 *See supra* notes 100–04 and accompanying text (discussing and critiquing the court-centric model).

121 For example, a nonjudicial enforcement regime might better "encourage vigorous decisionmaking by officials." Schuck, *supra* note 96, at 16. Likewise, due to the slow nature of judicial action, nonjudicial enforcement methods might more effectively "deter wrongdoing." *Id.*

world does not exist.[122] Notwithstanding that caveat, it is clear that victim compensation will certainly be higher if the complete subsection (g) exemption were denied.[123] If nonjudicial enforcement is a superior mechanism to enforcement via civil lawsuits, then it must be because of other countervailing factors outside of the realm of compensation.

A commonly noted countervailing factor is the ability and motivation of the executive officer in question to perform her duties with the optimal level of vigor and energy. Judicial review—whether through ex ante injunctions or ex post remedies—substitutes a court's view of the proper behavior of the executive for that of other institutions, including the executive officer herself.[124] If a judge adopts an overly narrow view of the executive's discretion, the ultimate policy goals of the agency would be compromised, interfering with the executive duty to enforce the law.[125] Nor is the problem limited to abstract concerns about separation of powers. To the extent that the overall mission of an agency is the provision and protection of widely shared public rights such as safety, education, or aid, "judicial review can be argued to block legislative or executive measures that are necessary to implement rights or to protect rights against private violation."[126] This risk is exacerbated by the fact that the availability of damage remedies for Privacy Act violations will tend "to favor the highly visible victims

---

[122] Among other limitations, compensation under the Privacy Act requires the potential plaintiff (1) to be aware of the action taken against her and the resulting harm; (2) to have the requisite legal knowledge to realize her rights may have been violated; (3) to have the financial means to proceed with litigation, either with or without an attorney; and (4) to have the desire to bring the suit. *See* SCHUCK, *supra* note 96, at 27 ("Certain social conditions, such as citizens' ignorance of their legal rights and inability to afford litigation, carve deep chasms between legal entitlement and actualization . . . ."). Furthermore, perfect compensation requires judges who are infallible in recognizing when a right has truly been abridged, a situation unlikely to occur. Deficiencies in any of these factors will reduce the overall level of compensation, even were subsection (g) read to be nonexemptible.

[123] For purposes of this Part, this Note assumes that agencies will take advantage of the complete subsection (g) exemption if courts were to make it clear that they had that ability. *But see supra* notes 32–38 (noting that until this point, agencies have not attempted to exempt their records in this way).

[124] *See supra* notes 93–98 and accompanying text (describing both injunctions and ex post remedies as mechanisms of encouraging executive compliance with the judge's understanding of the law).

[125] *See, e.g.*, Katherine Florey, *Sovereign Immunity's Penumbras: Common Law, "Accident," and Policy in the Development of Sovereign Immunity Doctrine*, 43 WAKE FOREST L. REV. 765, 790–94 (2008) (discussing the view that judicial review through damage suits can challenge and distort the "democratic process").

[126] *See* VERMEULE, *supra* note 95, at 70 (noting further that judicial review might therefore lead to the "perverse result" of "increas[ing] the overall incidence of rights-violations").

of official action but to leave the largely invisible and silent victims of official inaction or neglect without recourse."[127]

The preceding considerations are exemplified in the Supreme Court case of *Barr v. Matteo*.[128] In that case, a federal employee sued his supervisor, alleging that the supervisor libeled him in an agency press release.[129] A plurality of the Court agreed with the defendant's assertion that a federal employee acting within his duties should be absolutely immune from civil suit.[130] In defending this position, the Court first noted that the traditional fear—that without judicial review the executive would violate the law at will—had historically proved unfounded.[131] Furthermore, the Court noted reasons why immunity from suit would further public policy: Allowing civil suits for tort violations "would seriously cripple the proper and effective administration of public affairs as entrusted to the executive branch of the government" and "might appreciably inhibit the fearless, vigorous, and effective administration of policies of government."[132] Finally, drawing on the same conceptual disaggregation of right and remedy discussed above,[133] the Court noted that "there are of course other sanctions than civil tort suits available to deter the executive official

---

127 SCHUCK, *supra* note 96, at 65.

128 360 U.S. 564 (1959) (reversing a finding of liability for libel against a government director on the grounds that the actions taken were within his scope of duty).

129 *Id.* at 565.

130 *See id.* at 575 ("The fact that the action here taken was within the outer perimeter of petitioner's line of duty is enough to render the privilege applicable . . . .").

131 *See id.* at 576 ("It is perhaps enough to say that fears of this sort have not been realized within the wide area of government where a judicially formulated absolute privilege of broad scope has long existed.").

132 *Id.* at 570–71. Of course, there is an important difference between the type of civil remedy envisioned (and rejected) by the Court in *Barr* and the judicial review available in subsection (g). The former concerned personal liability against the federal officer, while subsection (g) authorizes suits directly against the federal government. 5 U.S.C. § 552a(g)(1) (2012). It may be that suits against the government will not have the same deleterious effects on vigorous decisionmaking as would suits in which an employee's own pocketbook is at stake. *See* SCHUCK, *supra* note 96, at 68–77 (discussing the ways in which personal liability slows and distorts official decisionmaking). Nevertheless, there are reasons to think that even governmental liability may have a non-negligible impact on the activity level and ultimate choices made by lower-level employees. Critics of governmental—as opposed to official—liability have noted that the costs of judicial review includes costs which arise when fear of liability leads to suboptimal executive decisions. *See* Harold J. Krent, *Reconceptualizing Sovereign Immunity*, 45 VAND. L. REV. 1529, 1536 & n.18 (1992) (noting that minimization of these costs is a valid congressional goal of sovereign immunity). The threat of liability may be particularly salient when an agency possesses robust internal disciplinary machinery that can sanction in a variety of ways employees who subject the agency to liability. *See* SCHUCK, *supra* note 96, at 137–38 (outlining the effects of these disciplinary systems).

133 *See supra* notes 99–113 and accompanying text (arguing that the existence and importance of a right does not necessarily compel a judicial forum).

who may be prone to exercise his functions in an unworthy and irresponsible manner."[134]

For an example of how this risk of over-deterrence of agency action might play out in the Privacy Act context, take the facts of *Tijerina v. Walters* itself, the first case to clearly reject the complete subsection (g) exemption.[135] The officer who authorized the allegedly unlawful disclosure in that case believed that doing so was advisable and legal under the "routine use" exemption of the Privacy Act, which permits agency disclosures for certain purposes declared in the agency's regulations.[136] Courts have failed to arrive at a uniform test for the routine-use exemption, and judicial interpretation of the exemption has been relatively unstable.[137] The VA argued before the Court of Appeals that the disclosure fit within its routine use of detecting "a suspected violation or reasonably imminent violation of the law, whether civil, criminal or regulatory in nature . . . ."[138] It maintained that its disclosure was a routine use in that it was meant to aid in the detection of a possible violation of a Texas statute prohibiting individuals from sitting for the bar "unless they have demonstrated good moral character."[139] The court disagreed,[140] despite the fact that the interference of the judiciary in the VA's use of its records might reasonably have made it more difficult for the VA to meet its regulatory goal of criminal enforcement, as well as its statutory duty of effectively providing benefits to veterans,[141] to the best of its ability.[142]

---

134 *Barr*, 360 U.S. at 576.

135 For a description of the case's holding, see *supra* notes 40–42 and accompanying text.

136 *See* Tijerina v. Walters, 821 F.2d 789, 798 (alluding to the "government's argument that the Silverstein letter did not violate subsection (b) of the Act . . . because the disclosure was for a 'Routine Use'"); *see also* 5 U.S.C. § 552a(b)(3) (2012) (permitting disclosure for a "routine use"); § 552a(a)(7) (defining "routine use").

137 *See* Todd Robert Coles, Comment, *Does the Privacy Act of 1974 Protect Your Right to Privacy?: An Examination of the Routine Use Exemption*, 40 AM. U. L. REV. 957, 996–1000 (1991) (discussing two different tests used by courts and describing multiple institutional barriers to effective enforcement of the provision).

138 Notices, Veteran Administration, Amendment of Systems and Revised Systems of Records, 47 Fed. Reg. 24010, 24012 (June 2, 1982).

139 *Tijerina*, 821 F.2d at 798.

140 *See id.* ("Even if Mr. Tijerina would have violated Texas law by sitting for the bar examination, the violation was not conceivably 'reasonably imminent' at the time of the Silverstein letter . . . . Routine Use five by its terms does not justify disclosure on the basis of such remote speculation.").

141 38 U.S.C. § 301(b) (2012).

142 The VA may reasonably have concluded that the threat of disclosure of a fraudulent application would reduce an applicant's incentive to commit fraud. Moreover, a reduction in fraud could increase potential funds available for qualified applicants.

B. Nonjudicial Enforcement of the Privacy Act

In Part III.B, this Note turns to specifics, outlining several different nonjudicial institutions that can adequately police agency compliance with all applicable provisions of the Privacy Act.

1. The Qualified Agency Itself

It may at first blush appear unwise to rely on agencies to police their own behavior.[143] However, the fact that agencies may not be "impartial"—in the sense that they have a stake in the ultimate decision of whether or not their actions are deemed lawful—is not the end of the analysis.[144] Other considerations, including expertise, institutional autonomy, and institutional "energy" or effectiveness, may ultimately lead to the conclusion that the potential rule-breaker itself is best suited to ensure compliance with the law.[145] This self-policing can occur both on a personnel level, in the form of individual employees and leadership identifying and attempting to cure violations,[146] as well as on an institutional level, in the form of agencies promulgating guidance and other rules of behavior to influence the actions of their staffs.[147]

---

[143] There is a perceived conflict of interest in a scheme in which an agency plays a role in policing its own behavior. *See, e.g.*, Fran Quigley, *Torture, Impunity, and the Need for Independent Prosecutorial Oversight of the Executive Branch*, 20 CORNELL J.L. & PUB. POL'Y 271, 273 (2010) (noting a "clear conflict of interest" that exists when the Attorney General—who serves at the pleasure of the President—is responsible for investigating the President or other top officials); *cf.* Caprice L. Roberts, *The Fox Guarding the Henhouse? Recusal and the Procedural Void in the Court of Last Resort*, 57 RUTGERS L. REV. 107, 168 (describing and deeming problematic the process by which Justices decide for themselves whether they will be recused, and arguing that "[c]orrection of this flaw requires that other, non-implicated Justices participate in the decision-making process").

[144] *See* VERMEULE, *supra* note 95, at 115 (describing impartiality as "best understood merely as one competing consideration among many").

[145] *See id.* at 117–30 (describing and providing examples of tradeoffs between impartiality and these other factors).

[146] Recent legal and sociological research has identified a transition in the employment setting "from an absolute expectation of faithful obedience to a more nuanced notion of organizational citizenship" where an "employee exhibits loyalty to the firm by trying to stop . . . misconduct." Orly Lobel, *Citizenship, Organizational Citizenship, and the Laws of Overlapping Obligations*, 97 CALIF. L. REV. 433, 440 (2009).

[147] Much has been written on the benefits of certain institutional and organizational decisionmaking structures in terms of achieving compliance with the law. *See, e.g.*, Kathleen Clark, *The Architecture of Accountability: A Case Study of the Warrantless Surveillance Program*, 2010 BYU L. REV. 357, 367–68 (2010) (discussing the benefits of a system of internal investigations as a mechanism to increase compliance); José A. Tabuena & Jennifer L. Smith, *The Chief Compliance Officer Versus the General Counsel: Friends or Foes? Part II*, 8 No. 6 J. HEALTH CARE COMPLIANCE 13, 16–17 (2006) ("If the chief compliance officer and general counsel are essentially given equal stature, there can be enhanced oversight . . . .").

A great number of agencies have established positions specifically charged with "promot[ing] and support[ing] privacy programs and privacy awareness."[148] These individuals are entrusted not only with day-to-day compliance issues, but also with the more general goal of creating a "privacy culture" by "instill[ing] at every level within agencies" a "concern for privacy and other civil liberties."[149] The Internal Revenue Service (IRS) provides an early example. Following the recommendation of both an internal report and a Government Accountability Office (GAO) investigation, the IRS established the "Office of the Privacy Advocate, the federal government's first privacy advocate position," in 1993.[150] The office has produced a series of documents related to the protection of privacy, including a "Declaration of Privacy Principles," meant to assure that "[t]he privacy rights of taxpayers will be respected at all times."[151] Furthermore, the IRS has amended its internal guidelines (the "Internal Revenue Manual")[152] to implement the Privacy Act and ensure compliance.[153] In addition to the general statement that "IRS employees should follow the legal requirements of the Privacy Act at all times,"[154] the Manual creates a four-tiered continuing education program detailing the differential Privacy Act training required for employees, depending on their level of involvement with matters relevant to the Act.[155]

---

148 *See* Margaret Ann Irving, *Managing Information Privacy in the Information Age*, 53 ADMIN. L. REV. 659, 668 (2001) (discussing the IRS's creation of the Office of the Privacy Advocate).

149 *Privacy and Civil Liberties in the Hands of the Government Post-September 11, 2001: Recommendations of the 9/11 Commission and the U.S. Department of Defense Technology and Privacy Advisory Committee*, *Joint Hearing Before the Subcomm. on Commercial and Admin. Law and Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 108th Cong. 21 (2004) (statement of Hon. John O. Marsh, Jr., Member, U.S. Dep't of Def. Tech. & Privacy Advisory Comm.).

150 Irving, *supra* note 148, at 663–64. Eventually the position was reorganized into the current "Office of Privacy, Governmental Liaison and Disclosure," with the responsibility to "ensure[ ] that your personal information is protected whenever you visit the IRS website." IRS PRIVACY POLICY, http://www.irs.gov/uac/IRS-Privacy-Policy#privacy (last visited Mar. 18, 2015).

151 *See* Irving, *supra* note 148, at 664–67 (discussing and reproducing the declaration).

152 The Internal Revenue Manual "is a compilation of instructions promulgated by the [IRS] for the guidance of its employees when administering the tax laws." Archie W. Parnell, Jr., *The Internal Revenue Manual: Its Utility and Legal Effect*, 32 TAX LAWYER 687, 687 (1979). Guidance documents such as these "can channel the discretion of agency employees, increase efficiency, and enhance fairness . . . ." OFFICE OF MGMT. & BUDGET, Memorandum for the Heads of Executive Departments and Agencies: Issuance of OMB's "Final Bulletin for Agency Good Guidance Practice," M-07-07 (Jan. 18, 2007).

153 IRS, Internal Revenue Manual, at pts. 10–11, *available at* http://www.irs.gov/irm (last visited Mar. 18, 2015).

154 *Id.* § 11.3.14.6.

155 *See id.* § 11.3.14.9.1 (describing the four levels of training required).

Other agencies have followed suit. Pursuant to a 1998 directive from President Clinton,[156] federal agencies were responsible for "designat[ing] a senior official within the agency to assume primary responsibility for privacy policy."[157] As reiterated in the Bush Administration Guidance, this individual occupies "a central role in overseeing, coordinating, and facilitating the agency's compliance efforts."[158] All agencies have complied with this directive.[159]

The Department of Homeland Security's (DHS) Chief Privacy Officer (CPO) provides another example. The agency's first CPO, Nuala O'Connor Kelly, began the process of "operationalizing privacy awareness within the very culture of" DHS.[160] Bamberger and Mulligan identify Kelly's ability to maintain the autonomy and integrity of the CPO position as "securing an additional mechanism to ensure that agency actions and commitments affecting privacy were

---

156 Memorandum from Jacob J. Lew, Dir., Office of Mgmt. & Budget, to Heads of Dep'ts and Agencies, Instructions on Complying with President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records," M-99-05 (Jan. 7, 1999), https://www.whitehouse.gov/sites/default/files/omb/memoranda/m99-05.html. The memorandum noted both the need of the federal government to gather "appropriate information about its citizens" but also that "[p]rivacy is a cherished American value." *Id*. In striking a balance between these two potentially conflicting ideals, the memorandum specified nine different privacy-related actions that all agencies and agency heads must take. *Id.*

157 *Id*. at attachment A.

158 Memorandum from Clay Johnson III, Deputy Dir. for Mgmt., Office of Mgmt. & Budget, to Heads of Exec. Dep'ts and Agencies, Designation of Senior Agency Officials for Privacy, M-05-08 (Feb. 11, 2005), https://www.whitehouse.gov/sites/default/files/omb/assets/omb/memoranda/fy2005/m05-08.pdf.

159 *See, e.g.*, DEP'T OF COMMERCE, CHIEF PRIVACY OFFICER AND DIRECTOR OF OPEN GOVERNMENT, DIRECTIVE NUMBER DOO 20-31 (2012), *available at* http://www.osec.doc.gov/opog/dmp/doos/doo20_31.html (prescribing the role of the Commerce Department's Chief Privacy Officer and Director of Open Government); DEP'T OF EDUC.: OFFICE OF MGMT., *Leadership: Chief Privacy Officer*, http://www2.ed.gov/about/offices/list/om/pirms/leadership.html (last visited June 6, 2015) (introducing the Chief Privacy Officer and explaining her duties); DEP'T OF ENERGY: OFFICE OF THE CHIEF INFO. OFFICER, *Privacy*, http://energy.gov/cio/office-chief-information-officer/services/guidance/privacy (last visited June 6, 2015) (discussing the Department of Energy's privacy program); DEP'T OF JUSTICE: OFFICE OF PRIVACY AND CIVIL LIBERTIES, *About the Office*, http://www.justice.gov/opcl/about-office (last visited June 6, 2015) (discussing the history and function of the Department's Office of Privacy and Civil Liberties).

160 *Privacy and Civil Liberties in the Hands of the Government Post-September 11, 2001: Recommendations of the 9/11 Commission and the U.S. Department of Defense Technology and Privacy Advisory Committee*, *Joint Hearing Before the Subcomm. on Commercial and Admin. Law and Subcomm. on the Constitution of the H. Comm. on the Judiciary*, 108th Cong. 49 (2004) (testimony of Nuala O'Connor Kelly, Chief Privacy Officer, U.S. Dep't of Homeland Security) [hereinafter *Joint Hearing on Post-9/11 Privacy and Civil Liberties*].

examined."[161] This mechanism ultimately led to agency outcomes more sensitive to privacy concerns.[162]

In addition to broader programmatic initiatives, agencies may also establish internal procedures whereby the individual decisions of agency personnel are investigated to determine whether there are violations of the Privacy Act. For example, in *Jacobs v. National Drug Intelligence Center*,[163] a Justice Department Inspector General conducted an independent investigation, which concluded that the NDIC employee had violated the Privacy Act, and that discipline was warranted.[164] This particular procedure has a quasi-judicial feel, as it involves both factfinding and recommended sanctions. Furthermore, the sanctions may be more effective than those imposed by a court since they occur much closer in time to the violations than any judicial sanctions could. The Inspector General report was issued in 1999, while the lawsuit—including two separate appeals to the Fifth Circuit—was not completed until 2008.[165]

Another manner by which agencies self-enforce the Privacy Act is through the creation of semi-autonomous bodies whose primary function is privacy oversight. A well-known example is the Department of Defense's (DoD's) Technology and Privacy Advisory Committee (TAPAC).[166] In response to controversy over its Terrorism Information Awareness (TIA) program, the Secretary of Defense tasked TAPAC "to provide him with advice on how, if at all, the TIA program should proceed."[167] Following a lengthy investigative process including over sixty witness interviews, TAPAC made seven recom-

---

[161] Kenneth A. Bamberger & Deirdre K. Mulligan, *Privacy Decisionmaking in Administrative Agencies*, 75 U. CHI. L. REV. 75, 100 (2008).

[162] *See id.* at 94 (noting that DHS's US-VISIT program's privacy impact assessment was "generally lauded as . . . high-quality") (internal citations omitted) (internal quotation marks omitted).

[163] 423 F.3d 512 (5th Cir. 2005).

[164] *Id.* at 514 (5th Cir. 2005) (describing the investigative process and ultimate conclusion of wrongdoing, a conclusion which was echoed by then-Attorney General Janet Reno).

[165] Jacobs v. Nat'l Drug Intelligence Ctr., 548 F.3d 375, 376 (5th Cir. 2008) (holding that the award for "emotional-distress damages" was proper).

[166] The Technology and Privacy Advisory Committee (TAPAC) was an appointed panel of experts "selected on the basis of their preeminence in the fields of constitutional law and public policy relating to communication and information management." 68 Fed. Reg. 11384 (2003).

[167] Paul Rosenzweig, *Proposals for Implementing the Terrorism Information Awareness System*, THE HERITAGE FOUNDATION (Aug. 7, 2003), http://www.heritage.org/research/reports/2003/08/proposals-for-implementing-the-terrorism-information-awareness-system (describing the TIA system and discussing how it could be improved); *see also* Robert Pear, *Survey Finds U.S. Agencies Engaged in 'Data Mining'*, N.Y. TIMES, May 27, 2004, at A24 (noting that the committee was appointed to "quell a political uproar").

mendations for DoD as well as five government-wide recommendations for addressing the concerns of data-mining more generally.[168] These recommendations were all accepted by DoD, "[d]espite their far-reaching scope."[169]

2. *Executive Office of the President*

There exists an immense amount of theoretical and empirical literature on the President's—and the broader Executive Office of the President's (EOP's)—ability to direct, influence, and control the activities of the agencies within the Executive branch.[170] In her famous article, *Presidential Administration*, then-Professor Elena Kagan argued that the President is uniquely equipped to engage in this direction both because of the position's democratic pedigree[171] and its ability to ensure efficient regulation.[172] Recent literature has added to the conversation the observation that executive oversight of agency behavior can also play a beneficial information-forcing function.[173] It is thus hardly surprising that the EOP has played a significant role in ensuring that agencies adequately comply with the Privacy Act.

A major mechanism of EOP's control of agency compliance with the Privacy Act is the OMB's Office of Information and Regulatory

---

168 TECHNOLOGY AND PRIVACY ADVISORY COMMITTEE, SAFEGUARDING PRIVACY IN THE FIGHT AGAINST TERRORISM x–xii (2004) (listing and expounding upon these recommendations).

169 Fred H. Cate, *Government Data Mining: The Need for a Legal Framework*, 43 HARV. C.R.–C.L. L. REV. 435, 481 (2008) (describing in detail the recommendations and stating that they would provide "a significant incentive" for improving privacy protection). Of course, much of the preceding argument relies on an assumption that programmatic policies such as those described will have a meaningful impact on the day-to-day decisions made by agency personnel as they handle personal information. This empirical question is outside the scope of this Note but is an area where additional work would be helpful.

170 *See* Lisa Schultz Bressman & Michael P. Vandenbergh, *Inside the Administrative State: A Critical Look at the Practice of Presidential Control*, 105 MICH. L. REV. 47, 52–62 (2006) (providing an extensive survey of this literature); *see, e.g.*, ERIC A. POSNER & ADRIAN VERMEULE, THE EXECUTIVE UNBOUND: AFTER THE MADISONIAN REPUBLIC 6 (2010) ("Executive agencies have been brought under increasingly firm control by the White House . . . .").

171 *See* Elena Kagan, *Presidential Administration* 114 HARV. L. REV. 2245, 2332–33 (2001) ("[P]residential leadership establishes an electoral link between the public and the bureaucracy.").

172 *See id.* at 2339–40 ("[A] president, by virtue of the attributes of his office, stands in a relatively good position to achieve these operational goals. Because he is a unitary actor, he can act without the indecision and inefficiency that so often characterize the behavior of collective entities.").

173 *See* Catherine M. Sharkey, State Farm *"With Teeth": Heightened Judicial Review in the Absence of Executive Oversight*, 89 N.Y.U. L. REV. 1589, 1622 (2014) (describing how agencies responded to Office of Information and Regulatory Affairs (OIRA) oversight "by hiring additional economists and generally focusing more attention on creating a robust regulatory record of the net benefits of proposed rules").

Affairs (OIRA).[174] In addition to its better-known function of reviewing significant regulatory actions,[175] OIRA provides guidance for agencies on issues of information collection generally and privacy matters specifically.[176] Not only did OMB publish an extensive guidance document implementing the Privacy Act shortly after its passage,[177] but the agency has continued to supplement that guidance with additional documents as new questions and uncertainties arise.[178]

For example, in response to recommendations from a presidentially created task force,[179] OMB issued a 2007 memorandum concerning the problem of security breaches of federal agencies' data systems leading to leaks of personally identifiable information.[180] Following OMB's directive, DHS—to take one example—published a fifty-six-page document outlining the agency's breach notification plan.[181] Referencing the OMB memorandum directly,[182] the plan "est-

---

[174] For an overview of OIRA's executive oversight function, see Harold H. Bruff, *Presidential Management of Agency Rulemaking*, 57 GEO. WASH. L. REV. 533, 557–59 (1989). For a more critical take on OIRA's role in influencing agency action, see Nicholas Bagley & Richard L. Revesz, *Centralized Oversight of the Regulatory State*, 106 COLUM. L. REV. 1260 (2006).

[175] *See, e.g.*, Regulatory Planning and Review, Exec. Order No. 12,866, 58 Fed. Reg. 51,735, 51,740–41 (1993) (requiring all nonindependent executive agencies to "provide OIRA . . . with a list of its planned regulatory actions" and "[a]n assessment of the potential costs and benefits of the regulatory action").

[176] Office of Mgmt. & Budget, *Information Policy: Privacy Guidance*, THE WHITE HOUSE, http://www.whitehouse.gov/omb/inforeg_infopoltech#itpd (last visited June 6, 2015).

[177] OFFICE OF MGMT. & BUDGET, *supra* note 73 (providing detailed guidance for agencies on all aspects of the Privacy Act).

[178] *See* Office of Mgmt. & Budget, *supra* note 176 (providing guidance for specific issues such as administering public websites and providing handbooks for citizens seeking access to public information).

[179] The Identity Theft Task Force was composed of the heads of several agencies and was charged "to further improve the effectiveness and efficiency of the Federal Government's activities in the areas of identity theft awareness, prevention, detection, and prosecution . . . ." Strengthening Federal Efforts to Protect Against Identity Theft, Exec. Order No. 13,402, 71 Fed. Reg. 27,945, 27,946 (May 15, 2006).

[180] Office of Mgmt. & Budget, Memorandum for the Heads of Executive Departments and Agencies: Safeguarding Against and Responding to the Breach of Personally Identifiable Information, M-07-16 (May 22, 2007). The memo instructed all agencies to "develop a breach notification policy and plan" that would provide a decisionmaking structure for dictating to agencies the circumstances under which they must disclose personal information breaches to those who might be affected. *Id.* at 13. Agencies were further reminded of the requirements of existing legislation, including the Privacy Act. *Id.* at 4–6.

[181] DEP'T OF HOMELAND SECURITY, PRIVACY INCIDENT HANDLING GUIDANCE 1 (last revised Jan. 26, 2012), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_guide_pihg.pdf (establishing "governing policies and procedures" for the department).

[182] *See id.* at 6 ("OMB M-07-16 further defines the appropriate reporting, handling, and notification procedures in the event a privacy incident occurs.").

ablishe[d] DHS policy and procedures for DHS personnel to follow upon the detection or discovery of a suspected or confirmed incident involving [personally identifiable information]."[183] Other agencies have likewise complied with OMB's instructions.[184] A Government Accountability Office (GAO) investigation concluded that although compliance has not been absolute, the plans promulgated by agencies "generally adhered to OMB . . . guidance."[185]

OMB was given additional authority to improve Privacy Act compliance in 2002, when Congress passed the Federal Information Security Management Act (FISMA).[186] The Act mandated that OMB "oversee agency information security policies and practices" and followed this general directive with more detailed oversight instructions.[187]

3. Congress (and Congressional Watchdogs)

The legislative branch's ability to control and influence agency action is a theme recurrently explored by political scientists and legal theorists. The so-called "congressional dominance approach" posits that Congress controls the actions of agencies by supplying to them "a system of incentives" where "rewards go to those agencies that pursue policies of interest to the current committee members," while "those agencies that fail to do so are confronted with sanctions."[188] This incentive-sanction system may include such tools as funding, oversight, and control of the appointment process.[189]

Appropriations committees in both the House and Senate possess significant leverage over the ways in which agencies implement policies.[190] Appropriations hearings provide interested lawmakers an opportunity to question agency officials regarding their implementa-

---

183 *Id*.

184 *See, e.g.*, DEP'T OF JUSTICE, DOJ INSTRUCTION: INCIDENT RESPONSE PROCEDURES FOR DATA BREACHES 1 (Aug. 6, 2013) (cancelling and superseding the Department's initial 2008 procedure).

185 *See* GOV'T ACCOUNTABILITY OFFICE, AGENCY RESPONSES TO BREACHES OF PERSONALLY IDENTIFIABLE INFORMATION NEED TO BE MORE CONSISTENT, GAO-14-34, at 11, 16 (Dec. 2013) ("Overall, the agencies we reviewed have developed policies and procedures for responding to a data breach involving [personally identifiable information].").

186 44 U.S.C. § 3541 et. seq. (2012).

187 § 3543(a).

188 Barry R. Weingast & Mark J. Moran, *Bureaucratic Discretion or Congressional Control? Regulatory Policymaking by the Federal Trade Commission*, 91 J. POL. ECON. 765, 768 (1983).

189 *See id.* at 769 (describing the congressional incentive system).

190 *See, e.g.*, DeShazo & Freeman, *supra* note 103, at 1484 (noting a statistically significant correlative effect between membership on an appropriations committee and influence over the decisionmaking of the Fish and Wildlife Service).

tion of, and compliance with, the Privacy Act. For example, Senator Patrick Leahy, who also sits on the Senate's Judiciary Committee, used the occasion of a 2004 Department of Justice Appropriations Hearing to question then-Attorney General John Ashcroft on his Department's system of records and its Privacy Act compliance.[191] Of specific interest to Senator Leahy was the Department's decision to exempt its record from the requirements that its systems of records be kept in a timely manner, as well as other exemptions related to relevance and completeness.[192] Secretary Ashcroft was forced to explain the Department's justification—in much more detail than procedurally required by the Act[193]—for taking advantage of these exemptions.

In addition to committees primarily concerned with appropriations, congressional oversight committees also play a major role in ensuring compliance with the Privacy Act.[194] For example, there was a House Judiciary Committee hearing conducted shortly after the release of the 9/11 Commission Report in 2004.[195] Several head policy officials of national security agencies—the Department of Defense, the Department of Homeland Security, and the temporary National Commission on Terrorist Attacks Upon the United States—were called to testify before the multiple subcommittees.[196] While much of the testimony involved simple responses of clarification, some representatives used the occasion to voice dissatisfaction with the ways in which agencies were utilizing personalized records. For example, in an exchange with DoD representative John Marsh, Jr., Representative Robert Scott focused repeatedly on the distinction he drew between the legitimate function of "law enforcement"—the investigation of

---

191 *Departments of Commerce, Justice, and State, the Judiciary, and Related Agencies Appropriations for Fiscal Year 2004: Hearing Before the Subcomm. of the S. Comm. on Appropriations*, 108th Cong. 150–51 (2003), *available at* http://www.gpo.gov/fdsys/pkg/CHRG-108shrg85911/pdf/CHRG-108shrg85911.pdf.

192 *Id.* at 193–94. As noted, *supra* notes 32–33, an agency must affirmatively exempt its records from any exemptible provision and provide a justification for doing so.

193 The Privacy Act requires that agencies "shall include in the statement required . . . the reasons why the system of records is to be exempted from a provision of this section." 5 U.S.C. § 552a(j) (2012). Agency justifications for taking exemptions are generally very brief and highly conclusory. *See, e.g.*, Exemptions of Bureau of Prisons Systems, 28 C.F.R. § 16.97(b)(4) (justifying an exemption by simply stating that the provision's application would be "highly impractical and inappropriate"); Exemption of U.S. Marshals Service Systems—limited access, as indicated, 28 C.F.R. § 16.101(b)(5) (justifying an exemption by stating that provision "would present a serious impediment to law enforcement" in that it would give persons sufficient warning to avoid warrants).

194 *See infra* text accompanying notes 199–206 (discussing the various ways in which this oversight occurs).

195 *Joint Hearing on Post-9/11 Privacy and Civil Liberties*, *supra* note 160.

196 *Id.* at 11–78 (providing the transcripts of each of these testimonies).

individuals suspected of crimes or imminent criminal activity—and a more generalized information search, which Representative Scott derisively described as: "just going into a database and seeing what pops out."[197] The congressman expressed concern with not only the latter tool as a policy matter, but also its apparent conflict with privacy legislation and regulation.[198]

Congress exercises oversight—and thus helps ensure Privacy Act compliance—not only directly but also through affiliated institutions that investigate and report on its behalf. The GAO is a congressional organization which "conducts investigations of and issues reports about executive branch programs at the request of congressional committee and subcommittee chairs and ranking members."[199] Sometimes described as "Congress's watchdog," the GAO assists in the general oversight broadly discussed above.[200] GAO has taken a rather prominent role in detecting and attempting to rectify agency noncompliance with privacy law, having issued reports on a variety of issues related to this area.

One of these reports was a 2003 publication entitled "Privacy Act: OMB Leadership Needed to Improve Agency Compliance."[201] Despite the report's title, its focus went well beyond OMB, and GAO sought to estimate, explain, and provide solutions for any general noncompliance by agencies of any provision of the Privacy Act. The report concluded that "[w]hile compliance with Privacy Act provisions and related OMB guidance was generally high in many areas, according to agency reports, it was uneven across the federal government—ranging from 100 percent to about 70 percent for the various provisions."[202] More importantly for purposes of this Note, the report moved from a descriptive to a prescriptive role, presenting conclusions on why compliance among agencies was not higher. GAO noted that forum participants thought that compliance would be increased if: (1) OMB issued additional guidance regarding certain substantive areas including electronic databases, coverage of sole proprietors, and

---

197 *Id.* at 61.

198 *See id.* (noting an apparent conflict of the generalized information search with certain regulations published by the FBI).

199 Clark, *supra* note 147, at 373–74.

200 FREDERICK M. KAISER, CONG. RESEARCH SERV., RL30349, GAO: GOVERNMENT ACCOUNTABILITY OFFICE AND GENERAL ACCOUNTING OFFICE 1–3 (2008), *available at* http://www.fas.org/sgp/crs/misc/RL30349.pdf (providing a summary of the Government Accountability Office's (GAO's) creation and function).

201 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-03-304, PRIVACY ACT: OMB LEADERSHIP NEEDED TO IMPROVE AGENCY COMPLIANCE (2003).

202 *Id.* at 3.

computer matches;[203] (2) the management of agencies placed a greater priority on Privacy Act implementation;[204] and (3) agency employees received more expansive training on the Act.[205] Moreover, these recommendations have led to actual changes; in response to a GAO suggestion, the Department of Justice issued its own extremely thorough guidance on the history and implementation of the Privacy Act.[206]

Conclusion

Ultimately this Note is about law enforcement in two different ways. First, it is about a discrete legal question governing law enforcement agencies—how to resolve an apparent ambiguity in whether or not those agencies may exempt their records from Privacy Act judicial review. This Note answers that question by relying on the best reading of the legislation—a reading that is supported by the plain language of the statute.

This Note is about law enforcement in another way as well: How does one enforce the law against an agency where legislation provides explicit limits on its behavior? Too often courts assume that they are the only answer; that they are the only institution with sufficient "fangs" to keep executive officers in check. In doing so, they ignore the existence of other political institutions and their effectiveness in curbing executive illegality. Embracing these nonjudicial sources of legal enforcement may help our political system better ensure that law enforcement in the second sense does not come at the price of law enforcement in the first.

---

[203] *Id.* at 25–26.

[204] *Id.* at 26–27.

[205] *Id.* at 27.

[206] U.S. Dep't of Justice, *supra* note 4; *see also* U.S. Gov't Accountability Office, *supra* note 201, at 25 (noting that forum participants had interest in DOJ providing guidance for the Privacy Act as it had already done for the Freedom of Information Act).