Note

Defining Disclosure in a Digital Age: Updating the Privacy Act for the Twenty-First Century

Jonathan C. Bond*

Table of Contents

* Law Clerk to the Hon. Jeffrey S. Sutton, U.S. Court of Appeals for the Sixth Circuit. J.D., 2008, The George Washington University Law School; M.Sc., University College London; B.A., Grove City College. I thank Ari Blaut and Brian Thavarajah for helpful comments on earlier drafts and Heather Bloom for outstanding editorial work. I also thank Professor Bradford Clark for his invaluable insight, indispensable guidance, and constant encouragement in this and many other endeavors. All remaining errors, of course, are my own.

Introduction

For most unsuccessful administrative plaintiffs, losing on appeal is the end of a long and arduous ordeal.[1] For John Doe, however, the decision of the administrative agency denying his claim for work-related health benefits was only the beginning of his troubles.[2] Like a number of Peace Corps Volunteers sent abroad,[3] Doe contracted a

---

1 In comparison to the tens of millions of cases that federal administrative agencies adjudicate each year, *see, e.g.*, Cynthia R. Farina, *Statutory Interpretation and the Balance of Power in the Administrative State*, 89 COLUM. L. REV. 452, 503 n.221 (1989), all Article III courts combined heard fewer than 400,000 cases in 2006, only a fraction of which involved appeals of administrative agencies' decisions, *see* ADMIN. OFFICE OF THE U.S. COURTS, 2006 ANNUAL REPORT OF THE DIRECTOR: JUDICIAL BUSINESS OF THE UNITED STATES COURTS 13–28 (2007), *available at* http://www.uscourts.gov/judbus2006/completejudicialbusiness.pdf. In 2004, for example, individuals seeking benefits under the Federal Employees' Compensation Act filed 162,965 administrative claims with the Office of Workers Compensation Programs (the same agency and statute involved in John Doe's lawsuit), *see* OFFICE OF WORKERS' COMP. PROGRAMS, U.S. DEP'T OF LABOR, ANNUAL REPORT TO CONGRESS FY2004, at 13 (2007), *available at* http://www.dol.gov/esa/aboutesa/04owcpmx.pdf, but only a very small number of these claims have been or will be reviewed in federal courts.

2 *See* Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156, 161 (D.D.C. 2006), *vacated on other grounds*, Order at 1, No. 05 Civ. 2449 (D.D.C. Mar. 22, 2007). Because his civil action centered on an allegedly wrongful dissemination of personal information about him, Doe brought suit under an alias, *see id.* at 156 n.1; the court's opinion does not reveal the nature of his illness or where he was serving at the time, *see id.* at 161.

3 According to the most recent available official survey of Peace Corps Volunteers' service-related health issues, conducted by the General Accounting Office in 1991, between ten and thirty percent of all Volunteers experienced medical problems in connection with their service in the Peace Corps. *See* U.S. GEN. ACCOUNTING OFFICE, PEACE CORPS: LONG-NEEDED IMPROVE-

disease during his service overseas.[4] Although he sought and received treatment for his condition, the ailment resurfaced two years later while he was employed by a different federal government entity.[5] This time, however, his request for health benefits was denied by the U.S. Department of Labor's Office of Workers' Compensation Programs ("OWCP").[6] Doe appealed the OWCP's decision, but it was upheld by the Employee Compensation Appeals Board ("ECAB").[7] The ECAB mailed Doe a copy of its decision and retained a copy in its own files, which are officially open to public inspection.[8]

As far as Doe was concerned, the matter was closed.[9] What Doe did not expect was that the ECAB's opinion denying his claim would be posted on the Internet for the "'world' to see."[10] Five years after the decision was issued, Doe discovered that the decision—complete with his name and private medical history—was available on the Department of Labor's public Web site, Westlaw, and other subscription services.[11]

After the ECAB denied his repeated requests to remove his decision from its Web site, Doe brought suit against the Department of Labor under the Privacy Act of 1974.[12] Designed as the counterpart to the Freedom of Information Act ("FOIA"),[13] the Privacy Act pro-

---

MENTS TO VOLUNTEERS' HEALTH CARE SYSTEM 3 (1991), *available at* http://archive.gao.gov/d20t9/144319.pdf.

4 *Doe*, 451 F. Supp. 2d at 161.

5 *Id.*

6 *Id.* The OWCP oversees such claims by former Peace Corps Volunteers. *See id.*

7 *See id.*; Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment at 3, *Doe*, 451 F. Supp. 2d 156 (No. 05 Civ. 2449).

8 *Doe*, 451 F. Supp. 2d at 161.

9 *See* Memorandum of Points and Authorities in Opposition to Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment at 5, *Doe*, 451 F. Supp. 2d 156 (No. 05 Civ. 2449).

10 *See id.* Two weeks before Doe's ECAB decision was issued in 2002, and two years before Doe discovered his ECAB decision online in 2004, the ECAB promulgated a "routine use notice" indicating that its decisions are made publicly available on its Internet Web site. *See* Routine Use Notice, 67 Fed. Reg. 16,815, 16,867–68 (April 8, 2002). The court expressly declined to resolve the question of whether the ECAB's published notification and the materials sent to Doe himself satisfied the Privacy Act's notice requirements pertaining to routine uses. *See Doe*, 451 F. Supp. 2d at 172 n.16.

11 *See Doe*, 451 F. Supp. 2d at 161.

12 Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 (codified in part as amended at 5 U.S.C. § 552a (2006)). Doe's complaint sought both the removal of his record from the government's Internet site and damages. *See Doe*, 451 F. Supp. 2d at 161–62.

13 5 U.S.C. § 552 (2006). A number of commentators have examined the intricate relationship between the Privacy Act and the FOIA in recent years. *See generally* Dean J. Spader, *Conflicting Values and Laws: Understanding the Paradox of the Privacy Act and the Freedom of Information Act*, 19 LEGAL STUD. F. 21 (1995) (examining the opposing values of privacy and

hibits federal government agencies from "disclos[ing]" certain kinds of personally identifiable information.[14] It fails, however, to define "disclose."[15] The meaning of the term is critical for at least three reasons: (1) whether a suit can be brought at all turns entirely on whether an agency's actions amount to disclosure;[16] (2) an agency's liability for damages depends on whether the disclosure was "intentional or willful";[17] and (3) the time an alleged disclosure occurs determines when the statute of limitations begins to run.[18] Without guidance from the statute or the implementing regulations,[19] courts, administrative agencies, and the public are left in the dark as to whether and when agency action violates the statute.

In the simplest cases, the absence of a definition poses no problem. Often there is no dispute that an agency's action would amount to a disclosure, and so the parties' controversy concerns only whether

---

public access to the Privacy Act and the FOIA); Thomas M. Susman, *The Privacy Act and the Freedom of Information Act: Conflict and Resolution*, 21 J. MARSHALL L. REV. 703 (1988); Laura Hawkins, Case Note, *The Privacy Act as a Partial Repeal of the Freedom of Information Act*, 10 T. MARSHALL L. REV. 429 (1985); Susan Marble, Note, *Is the Privacy Act an Exemption 3 Statute and Whose Statute Is It Anyway?*, 52 FORDHAM L. REV. 1334, 1339 (1984) (contending that the Privacy Act and the FOIA "operate most efficiently as independent statutory frameworks"). Notably, although the FOIA and the Privacy Act are similar in a number of respects, *see* Hill v. U.S. Air Force, 795 F.2d 1067, 1069 n.4 (D.C. Cir. 1986); Dinsio v. FBI, 445 F. Supp. 2d 305, 307 n.1 (W.D.N.Y. 2006), the coverage of the two statutes does not overlap perfectly, *see* Louis v. U.S. Dep't of Labor, 419 F.3d 970, 978 n.7 (9th Cir. 2005) (noting difference in scope of certain provisions); David C. Boyle, Note, *Proposal to Amend the United States Privacy Act to Extend Its Protections to Foreign Nationals and Non-Resident Aliens*, 22 CORNELL INT'L L.J. 285, 298–301 (1989) (noting inconsistency between the FOIA, which gives rights to nonnationals, and the Privacy Act, the protections of which seem to stop at the nation's borders).

14 *See* 5 U.S.C. § 552a(b).

15 Although the Privacy Act transforms numerous common words into terms of art with precise meaning for purposes of the Act, neither "disclose" nor "disclosure" is among them. *See id.* § 552a(a) (defining not only terms such as "routine use" and "matching program" but also words such as "maintain," "individual," "record," "[f]ederal personnel," etc., yet providing no definition for "disclose" or "disclosure").

16 The only provision permitting suit for a violation of the disclosure prohibition is § 552a(g)(1)(D), which authorizes a civil action against an agency that "fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual." *Id.* § 552a(g)(1)(D). To bring suit for a disclosure, a plaintiff therefore must show that the disclosure prohibition was violated. *Cf. id.* § 552a(b) (prohibiting agencies from disclosing personally identifiable records).

17 *See id.* § 552a(g)(4).

18 *Id.* § 552a(g)(5).

19 The Privacy Act charges the Office of Management and Budget ("OMB") to "prescribe guidelines and regulations for the use of agencies in implementing" the Act and to "provide continuing assistance to and oversight of the implementation" of the Act. *Id.* § 552a(v). As discussed below, *see infra* notes 44–46 and accompanying text, the regulations OMB has issued provide little meaningful guidance about the meaning of disclosure.

that disclosure was improper. In cases like Doe's, however, the answer is unclear. On the one hand, Doe's ECAB decision was already on file at the agency's headquarters and was available for public inspection to anyone who requested it.[20] On the other hand, publishing the decision in electronic format for the world to see increased its public accessibility by an immeasurable degree.[21] To complicate matters, several private third party publishers had made Doe's decision available electronically to their subscribers.[22]

Cases like *Doe* that present difficult questions of what agency actions constitute disclosure have become increasingly prevalent in recent years. This is especially true as agencies have begun to make vast amounts of data available online.[23] Courts around the country have developed several diverging approaches to the problem,[24] but none is ultimately satisfactory. Specifically, none of the approaches applied to date is both fully consistent with the Privacy Act's current text and yet able to account for the practical realities of modern agency disclosure practices. Moreover, the few approaches that come closest to dealing with these practical realities also involve the most difficult, fact-intensive inquiries by the court and the parties, and they also open the door to what might be termed the "third party disclosure loophole" latent in *Doe*.[25]

---

20 *See* Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156, 161 (D.D.C. 2006), *vacated on other grounds*, Order at 1, No. 05 Civ. 2449 (D.D.C. Mar. 22, 2007).

21 Before its Internet publication, the fact that the decision even existed apparently was known only to the handful of individuals who participated in Doe's administrative proceedings. *See* Defendants' Show Cause Filing at 4, *Doe*, No. 05 Civ. 2449 (D.D.C. Sept. 29, 2006). Afterwards, however, anyone searching for Doe's name using a major search engine would come across the sensitive details of his private medical history. *See* Memorandum of Points and Authorities in Opposition to Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment at 6, *Doe*, 451 F. Supp. 2d 156 (No. 05 Civ. 2449).

22 *See Doe*, 451 F. Supp. 2d at 161.

23 *See* John C. Reitz, *E-Government*, *in* American Law in the 21st Century: U.S. National Reports to the XVIIth International Congress of Comparative Law 733, 734 (John C. Reitz & David S. Clark eds., 2006). In large measure, agencies are *required* by the FOIA to publish a great deal of information "by computer telecommunications or . . . other electronic means." 5 U.S.C. § 552(a)(2). Such information must be redacted, however, "[t]o the extent required to prevent a clearly unwarranted invasion of personal privacy," *id.*, and the FOIA's disclosure requirement is lifted entirely for information falling into one of nine enumerated exceptions, *see id.* § 552(b), one of which exempts "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," *id.* § 552(b)(6). The interplay between these provisions of the FOIA and the Privacy Act reflects the closely interlocking nature of the two statutes and the considerable tension each Act exerts on the other.

24 *See infra* Part II.

25 *See infra* notes 107–11 and accompanying text.

In the end, the absence of a definition of disclosure in the Privacy Act has led to unnecessary confusion and even conflict among federal courts applying the Act, especially where electronic disclosure is involved.[26] This Note proposes an amendment to the Privacy Act to resolve this problem. The proposed amendment defines "disclose" to encompass (1) the direct transmission of a record to a recipient previously unaware of its contents (and not otherwise authorized to know it), and (2) any action by a federal agency that substantially increases the public accessibility of such a record. Beyond resolving the confusion and conflict among the courts, the proposed definition will provide much-needed clarity and guidance to federal agencies and the public while furthering the underlying policy goals at which the Privacy Act was aimed.

Part I outlines the current state of the law pertaining to disclosure under the Privacy Act. After briefly setting out the historical context, purposes, and basic structure of the Privacy Act—and its general prohibition of certain disclosures of government records—Part I explores some of the complications that make the absence of a definition of disclosure problematic. Part II then examines and evaluates ways courts have tried to cope with these complications, efforts which have led to uncertainty and conflicting conclusions.

Part III sets forth the proposed definition of "disclose" under the Privacy Act. It explains how the new definition would operate in practice—both in 'classic' Privacy Act cases and in the 'hard cases' noted in Part II—and identifies the ways it would interact with other provisions of the Act. Finally, Part IV assesses the costs and benefits of the proposed amendment. It first highlights the new definition's key advantages—including clarity, consistency with the Act's purposes, and its minimal impact on the remainder of the statutory framework—all of which derive from its focus on public accessibility resulting from prior agency action. Part IV then addresses five potential challenges to the proposed definition. On balance, the proposed definition represents a substantial step forward in achieving the Pri-

---

26 For a discussion of the implications of rapid technological development in government information-handling practices that affect individual privacy, see generally Ira Bloom, *Freedom of Information Laws in the Digital Age: The Death Knell of Informational Privacy*, 12 RICH. J.L. & TECH. 9 (2006), http://law.richmond.edu/jolt/v12i3/article9.pdf. Changes in technology have also created difficulty in interpreting other key terms of the Privacy Act. *See, e.g.*, Julianne M. Sullivan, Comment, *Will the Privacy Act of 1974 Still Hold Up in 2004? How Advancing Technology Has Created a Need for Change in the "System of Records" Analysis,* 39 CAL. W. L. REV. 395, 403–11 (2003) (analyzing how computer technology affects other threshold definitional requirements of the Act, such as "system of records").

vacy Act's goals while demystifying the task courts increasingly confront.

I. The Current Legal Landscape

A. The Privacy Act's Disclosure Prohibition

The Privacy Act imposes a broad prohibition on the disclosure of certain agency records that contain personally identifiable information.[27] The Act and the disclosure prohibition arose in part as a reaction to the anticommunist investigations of the 1950s and '60s, which led many to appreciate the harm that can be inflicted by disclosing personally identifiable records.[28] Rapid developments in technology also fueled concerns that the government's increased reliance on centralized databases would open the door to abuses of personally identifiable information.[29] Additionally, the passage of the FOIA

---

27 *See* 5 U.S.C. § 552a(b).

28 *See* H. COMM. ON GOV'T OPERATIONS, PRIVACY ACT OF 1974, H.R. REP. NO. 93-1416, at 4–10 (1974), *reprinted in* JOINT COMM. ON GOV'T OPERATIONS, 94TH CONG., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY 297–303 (Comm. Print 1976) [hereinafter SOURCE BOOK]. Indeed, states' efforts (under the pretext of searching for communist infiltrators) to compel then-disfavored groups such as the NAACP to disclose their membership lists to the government—which would in turn make them available to the public, thus leading to almost certain public harassment and reprisals—led the U.S. Supreme Court to recognize and enforce a First Amendment right to anonymous association. *See, e.g.*, Gibson v. Fla. Legislative Investigation Comm., 372 U.S. 539, 543–46, 557–58 (1963); Bates v. City of Little Rock, 361 U.S. 516, 523–24 (1960); NAACP v. Alabama *ex rel.* Patterson, 357 U.S. 449, 462–63 (1958). For more detailed treatments of the background and history of the Privacy Act, see Richard Ehlke, *The Privacy Act After a Decade*, 18 J. MARSHALL L. REV. 829, 829–30, 835–40 (1985); Haeji Hong, *Dismantling the Private Enforcement of the Privacy Act of 1974:* Doe v. Chao, 38 AKRON L. REV. 71, 80–83, 86–93 (2005); John F. Joyce, *The Privacy Act: A Sword and a Shield but Sometimes Neither*, 99 MIL. L. REV. 113, 118–23 (1983); Frederick Z. Lodge, Note, *Damages Under the Privacy Act of 1974: Compensation and Deterrence*, 52 FORDHAM L. REV. 611, 622–28 (1984); Lisa A. Reilly, Case Note, *The Government in the Sunshine Act and the Privacy Act*, 55 GEO. WASH. L. REV. 955, 963 (1987).

Notably, however, the Privacy Act was not Congress's first foray into the field of protecting individuals' privacy in the handling of federal government records. By 1840, census officials had recognized privacy problems implicated by the government's handling (and potential mishandling) of confidential personal data it had collected, and in 1889 Congress enacted legislation subjecting officials who improperly disclosed census information to a substantial fine. *See* Neil M. Richards & Daniel J. Solove, *Privacy's Other Path: Recovering the Law of Confidentiality*, 96 GEO. L.J. 123, 140 (2007).

29 *See* John T. Soma & Richard A. Wehmhoefer, *A Legal and Technical Assessment of the Effect of Computers on Privacy*, 60 DENV. L.J. 449, 451 (1983). Congress stated this concern in its findings contained in the Privacy Act itself. *See* Privacy Act of 1974, Pub. L. No. 93-579, § 2, 88 Stat. 1896, 1896 (1974) (stating that "the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information"); *see also* Savarese v. U.S. Dep't of Health, Educ. &

eventually led to the realization that agencies seeking to comply with that Act might go too far, inadvertently sending sensitive, personal information into the public domain.[30]

To that end, the Privacy Act was adopted in 1974 to prohibit the disclosure of certain records containing personally identifiable information.[31] Like the FOIA, however, the Act also provides a number of exceptions.[32] Specifically, the Privacy Act enumerates twelve categories of disclosure that fall outside the Act's broad proscription.[33] Other than an exemption for disclosures required by the FOIA,[34] the most important exception to the Privacy Act's disclosure prohibition allows disclosures for "routine use[s]" that agencies themselves define.[35] In fact, subject to certain procedural and substantive limits,[36]

Welfare, 479 F. Supp. 304, 308 (N.D. Ga. 1979), *aff'd sub nom.* Savarese v. Harris, 620 F.2d 298 (5th Cir. 1980) (noting that "Congress had as its purpose the control of the unbridled use of highly sophisticated and centralized information collecting technology").

30 *See* Thomas v. U.S. Dep't of Energy, 719 F.2d 342, 345–46 (10th Cir. 1983) (identifying Congress's concerns regarding "misuse" of sensitive information); Joyce, *supra* note 28, at 118–22; Ludmila Kaniuga-Golad, Comment, *Federal Legislative Proposals for the Protection of Privacy*, 8 FORDHAM URB. L.J. 773, 787 (1979–80); *see also* Cochran v. United States, 770 F.2d 949, 954–55 (11th Cir. 1985) (noting the opposite purposes of the FOIA and the Privacy Act and implying that the Privacy Act was adopted to curb abuses of the FOIA).

31 The key provision of the Act provides that "[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains." 5 U.S.C. § 552a(b). The Act also requires agencies, *inter alia*, to permit individuals to view their own records, *see id.* § 552a(d)(1), and to petition agencies to amend their records if they believe the information contained is inaccurate, *id.* § 552a(d)(2). The disclosure prohibition, however, is arguably the centerpiece of the statute. *Cf.* H.R. REP. NO. 93-1416, at 12 (1974), *reprinted in* SOURCE BOOK, *supra* note 28, at 305 (noting that the prohibition on nonconsensual disclosure is "one of the most important, if not the most important, provisions of the [House version of the] bill").

32 The numerous exceptions to the Act's disclosure prohibition have prompted extensive criticism of the Act's efficacy as a safeguard of individual privacy. *See, e.g.*, HARRY HENDERSON, PRIVACY IN THE INFORMATION AGE 60 (rev. ed. 2006); DANIEL J. SOLOVE, THE DIGITAL PERSON: TECHNOLOGY AND PRIVACY IN THE INFORMATION AGE 136–37 (2004) (describing limits on the Act's usefulness as a safeguard of personal privacy).

33 *See* 5 U.S.C. § 552a(b)(1)–(12).

34 *See id.* § 552a(b)(2).

35 *See id.* § 552a(b)(3). The term "routine use" is specifically defined in the statute to mean, "with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected." *Id.* § 552a(a)(7).

36 The Act's drafters imposed three limits on the creation of routine uses. First, routine uses must be published in advance in the Federal Register. *Id.* § 552a(e)(4)(D). Second, the disclosing agency must separately notify individuals who provide information to the government of the routine uses that might be made of their information. *Id.* § 552a(e)(3)(C). Third, such uses must be consistent with the purpose for which the agency originally collected the information. *Id.* § 552a(a)(7). The Third Circuit developed an influential interpretation of the routine use exception's "compatibility" requirement in *Britt v. Naval Investigative Service*, 886 F.2d 544,

the Act's authors envisioned that most questions about the propriety of agency disclosures would be resolved by the agencies themselves through the routine use provision.[37]

What they evidently did not foresee, however, was the difficulty courts, agencies, and private individuals would face in determining what "disclosure" means. Beyond the difficulty this creates for agencies, which need to know whether to promulgate a routine use notice before they disseminate information, the omission is problematic for three additional reasons. First, whether a plaintiff has a cause of action at all depends on whether agency action amounts to disclosure.[38] Second, whether a plaintiff can seek damages for that action depends on whether the violating disclosure was "intentional or willful."[39] Third, when the statute of limitations begins to run turns on which actions transformed an agency's information-handling procedures into

---

548–49 (3d Cir. 1989). The *Britt* formulation is not the only available rubric, however. *Cf.* John W. Finger, Note, *Narrowing the "Routine Use" Exemption to the Privacy Act of 1974*, 14 U. MICH. J.L. REFORM 126, 128 (1980) (proposing a balancing test to assess which routine uses satisfy the Privacy Act's routine use exemption that differs from the test established in *Britt* and followed in several circuits).

37 As the Privacy Act's legislative history reveals, the Act's drafters did not seek to curtail agency disclosures categorically—as doing so would effect a repeal of much of the FOIA—but rather intended that authorized disclosures be limited to appropriate purposes and made known to affected persons in advance. *See* H.R. REP. NO. 93-1416, at 13 (1974), *reprinted in* SOURCE BOOK, *supra* note 28, at 306 (noting that "[t]he Committee does not desire that agencies cease making individually-identifiable records open to the public, including the press, for inspection and copying. On the contrary, it believes that the public interest requires the disclosure of some personal information. . . . The Committee merely intends that agencies consider the disclosure of this type of information on a category-by-category basis and allow by published rule only those disclosures which would not violate the spirit of the Freedom of Information Act by constituting 'clearly unwarranted invasions of personal privacy.'").

38 *See* 5 U.S.C. § 552a(b); *see also supra* note 16 (discussing § 552a(b) in relation to § 552a(g)(1)(D), which authorizes civil suits). In *Scarborough v. Harvey*, for instance, the plaintiffs' claim alleging Privacy Act violations turned critically on the meaning of disclosure under the Act, and specifically on whether a disclosure can occur when the information was already publicly available. *See* 493 F. Supp. 2d 1, 16 n.29 (D.D.C. 2007). In that case, which is still ongoing, the plaintiffs sought damages of $36 million, asserting that various alleged disclosures by several government agencies of records containing false information caused grave harm to the plaintiffs' business reputation and the loss of valuable business opportunities. *See* Amended Complaint at 20, *Scarborough*, 493 F. Supp. 2d 1 (No. 05 Civ. 1427). The court held that the prior public availability of the document did not, as the defendants argued, preclude a finding that a disclosure had occurred. *See Scarborough*, 493 F. Supp. 2d at 16 n.29.

39 *See* 5 U.S.C. § 552a(g)(4). Notably, "the words 'intentional' and 'willful' in § 552a(g)(4) do not have their vernacular meanings," but "instead . . . are terms of art," which "set a standard that is 'somewhat greater than gross negligence.'" White v. Office of Pers. Mgmt., 840 F.2d 85, 87 (D.C. Cir. 1988) (per curiam) (citation omitted). As a result, understanding which specific actions constitute disclosure is essential to determining whether a disclosure meets the "intentional or willful" threshold.

a prohibited disclosure.[40] Given the importance of disclosure's meaning and the extent to which the Act defines so many other key terms,[41] the absence of a definition in the statute is surprising.

To make matters worse, other common sources of statutory meaning are equally unhelpful. While the Act's legislative history offers some explanation for the statute's imprecision,[42] it offers little if any guidance as to what was meant by disclosure.[43] Similarly, the implementing guidelines ("Guidelines") issued by the Office of Management and Budget ("OMB"),[44] generally viewed as the authoritative

---

40 *See* 5 U.S.C. § 552a(g)(5) (establishing a two-year statute of limitations). Knowing which acts constitute disclosure is therefore essential to adjudicating statute of limitations challenges. *See, e.g.*, Oja v. U.S. Army Corps of Eng'rs, 440 F.3d 1122, 1136 (9th Cir. 2006). The Act states that "[a]n action to enforce any liability created under this section may be brought . . . within two years from the date on which the cause of action arises," although it provides for tolling in certain narrow cases of an agency's material and willful misrepresentation. 5 U.S.C. § 552a(g)(5). By the Act's plain terms, it would seem that the statute of limitations should run from when a disclosure occurs: § 552a(g)(5) provides that the statute runs when the "cause of action arises," § 552a(g)(1)(D) creates a cause of action whenever an agency "fails to comply with any . . . provision of [§ 552a]," and an improper disclosure prohibited by § 552a(b) would amount to "fail[ure] to comply" from the moment of disclosure. The District of Columbia Circuit, however—which is acknowledged as the most influential court in FOIA and Privacy Act litigation, *cf.* OFFICE OF INFO. & PRIVACY, U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974: CIVIL REMEDIES § (F)(2) (2004) [hereinafter DOJ OVERVIEW], *available at* http://www.usdoj.gov/oip/1974civrem.htm—has held that the statute of limitations provision in cases seeking damages for disclosure "does not begin to run until the plaintiff knows or should know of the alleged violation," Tijerina v. Walters, 821 F.2d 789, 798 (D.C. Cir. 1987). In any event, the triggering of the statute of limitations still depends on what constitutes disclosure; *Tijerina* merely adds a layer of complexity by establishing the moment when the plaintiff knew or should have known of the acts that amounted to disclosure as the starting point for the limitations period.

41 *See* 5 U.S.C. § 552a(a).

42 The speed with which the final text was drafted and adopted provides a clue to its imprecision and incompleteness. *See* DOJ OVERVIEW, *supra* note 40, LEGISLATIVE HISTORY, *available at* http://www.usdoj.gov/oip/1974leghis.htm ("The Act was passed in great haste during the final week of the Ninety-Third Congress. No conference committee was convened to reconcile differences in the bills passed by the House and Senate. Instead, staffs of the respective committees . . . prepared a final version of the bill that was ultimately enacted."). As a result, the Act is "[h]ardly a model of legislative 'precision and tailoring,'" Pilon v. U.S. Dep't of Justice, 73 F.3d 1111, 1112 (D.C. Cir. 1996), leaving other key concepts like compatibility of purposes for routine uses vague and undefined, *see* U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, 9 F.3d 138, 144 (D.C. Cir. 1993) (Silberman, J.).

43 Because of the manner and speed in which the final Act was compiled from the versions passed by the House and Senate, the committee reports are only of limited value; instead, the most illuminating legislative history is found in a document produced by the committee staffs pertaining to compromise amendments. DOJ OVERVIEW, *supra* note 40, LEGISLATIVE HISTORY, *available at* http://www.usdoj.gov/oip/1974leghis.htm. Nothing in that report, however, sheds light on precisely what "disclosure" means.

44 Privacy Act Implementation, 40 Fed. Reg. 28,947, 28,949–78 (July 9, 1975). The Guidelines are specifically authorized by the Act, *see* 5 U.S.C. § 552a(v), and were issued just six

administrative interpretation of the Privacy Act,[45] offer little clarity about disclosure's meaning. If anything, the Guidelines merely highlight the breadth of possible methods of disclosure.[46] Consequently, absent clear direction from Congress and the implementing agency, courts have been left to their own devices in giving meaning to what is arguably the Privacy Act's most critical term.

B. The Disclosure Prohibition in Practice

Lacking clear guidance from the statute's text, legislative history, or implementing regulations, courts evaluating claims of improper disclosure under the Privacy Act generally require plaintiffs to show three things to prove a disclosure. First, the information disclosed must have been a "record" contained in a "system of records."[47] Second, the record must actually have been retrieved from the system of records by reference to the individual's name or other personal identi-

---

months after the Act's passage, *see* Privacy Act Implementation, 40 Fed. Reg. at 28,948–49 (noting the Privacy Act's date of enactment as December 31, 1974, and issuance of the regulations on July 9, 1975). For a detailed discussion of the OMB's policy role in interpreting the Privacy Act in its first several years, see generally James T. O'Reilly, *Who's on First?: The Role of the Office of Management and Budget in Federal Information Policy*, 10 J. LEGIS. 95 (1983); *see also* 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, 983–86 (1991) (discussing OMB's role in promulgating guidelines and in overseeing federal agencies' compliance with the Privacy Act).

45 Courts generally view the OMB Guidelines as meriting *Chevron* deference. *See, e.g.*, Maydak v. United States, 363 F.3d 512, 518 (D.C. Cir. 2004); Quinn v. Stone, 978 F.2d 126, 133 (3d Cir. 1992); Baker v. Dep't of the Navy, 814 F.2d 1381, 1383 (9th Cir. 1987); Perry v. FBI, 759 F.2d 1271, 1276 n.7 (7th Cir. 1985). Some courts, however, *see, e.g.*, Henke v. U.S. Dep't of Commerce, Civ. A. No. 94-0189, 1996 WL 692020, at *2 (D.D.C. Aug. 19, 1994), *aff'd on other grounds*, 83 F.3d 1445 (D.C. Cir. 1996), including the Supreme Court in one context, *see* Doe v. Chao, 540 U.S. 614, 627 n.11 (2004), have refused to accord unquestioning deference to the Guidelines on specific issues.

46 *See* Privacy Act Implementation, 40 Fed. Reg. at 28,953 ("The phrase 'by any means of communication' means any type of disclosure (e.g., oral disclosure, written disclosure, electronic or mechanical transfers between computers of the contents of a record).").

47 *See Quinn*, 978 F.2d at 131–32 (citing 5 U.S.C. § 552a(b)); Beaulieu v. IRS, 865 F.2d 1351, 1352 (1st Cir. 1989); *see also* Patricia I. Carter, *Health Information Privacy: Can Congress Protect Confidential Medical Information in the "Information Age"?*, 25 WM. MITCHELL L. REV. 223, 242–43 (1999) (noting the effect of the Privacy Act's limited application to "records" within "systems of records"). Each of these terms is expressly defined in the Act. *See* 5 U.S.C. § 552a(a)(4)–(5).

fier.[48] Third, the record (or information obtained from it) must have been disseminated without the individual's consent.[49]

When applying the third element—the requirement that the information must have been disseminated without consent—the courts generally employ a common sense conception of disclosure that corresponds neatly to one-to-one transfers of information.[50] If an agency

---

48 *See* Savarese v. U.S. Dep't of Health, Educ. & Welfare, 479 F. Supp. 304, 308 (N.D. Ga. 1979), *aff'd sub nom.* Savarese v. Harris, 620 F.2d 298 (5th Cir. 1980). The District of Columbia Circuit has recently added to this element, in the specific context of Internet disclosures, a requirement that the retrieval be done by the agency itself. In *McCready v. Nicholson*, the D.C. Circuit expressly affirmed the district court's holding below that "the 'practice of retrieval by name or other personal identifier must be an *agency* practice to create a system of records and not a "practice" by those outside the agency.'" 465 F.3d 1, 13 (D.C. Cir. 2006) (quoting McCready v. Principi, 297 F. Supp. 2d 178, 199 (D.D.C. 2003)). Agreeing with the district court that an Internet Web site—by which third parties, including the public, can access individual records by name or personal identifier—does not meet this standard, the D.C. Circuit concluded that such a Web site does not amount to a system of records, and therefore the retrieval of information through the site is not a prohibited disclosure. *See id.* at 12–13.

At first glance, the court's holding in *Nicholson*, issued just two weeks after the court's holding in *Doe v. U.S. Department of Labor*, 451 F. Supp. 2d 156 (D.D.C. 2006), might seem to make *Doe* an easy case: insofar as the challenged disclosure occurred through the ECAB's Web site, the retrieval of records through that Web site surely would not amount to disclosure under *Nicholson*, 465 F.3d at 13. Upon closer examination, however, the clarity disappears. First, it is possible that *Nicholson* would not answer the question in *Doe*. In *Doe,* unlike *Nicholson*, the record at issue was also contained in a different system of records maintained by the ECAB, viz., the agency's hard-copy files that were open to the public, from which the electronic versions presumably were taken. *Doe*, 451 F. Supp. 2d at 161. Indeed, the plaintiff in *Nicholson* made a version of this argument, alleging that summary judgment was improper because further discovery as to whether such an additional system of records existed was necessary. *See Nicholson*, 465 F.3d at 13–14. The D.C. Circuit rejected her request for additional discovery because the record showed clearly that no such separate system of records existed. *See id.* at 14. Had the agency in that case maintained the record in a separate system of records, however, the Circuit's decision seems to imply (and at the very least does not reject the possibility) that the dissemination would have been a prohibited disclosure. In the context of *Doe*, then, it is at least plausible that by publishing on its public Web site records that were already contained in a system of records, the ECAB did disclose Doe's record within the meaning of § 552a(b).

Second, the D.C. Circuit's holding in *Nicholson* does not bind other circuits confronting the same question. It is certainly possible that another court would find that an agency Web site that searches and displays records from the agency's compilation of records would amount to an "agency practice." At the very least, the question is far from clear from both a textual and policy standpoint, which only serves to emphasize the need for greater statutory precision on what constitutes a disclosure.

49 *See* Bartel v. FAA, 725 F.2d 1403, 1408 (D.C. Cir. 1984), *quoted in* Orekoya v. Mooney, 330 F.3d 1, 6 (1st Cir. 2003); Chang v. Dep't of the Navy, 314 F. Supp. 2d 35, 42 n.2 (D.D.C. 2004).

50 *See, e.g.*, Kline v. Dep't of Health & Human Servs., 927 F.2d 522, 524 (10th Cir. 1991); *see also* DOJ OVERVIEW, *supra* note 40, DEFINITIONS § (E)(1), *available at* http://www.usdoj.gov/oip/1974definitions.htm (collecting cases employing a common sense approach with regard to the third element).

transmits a record or its contents to a person who did not previously have access to or knowledge of the information contained in it, a disclosure has occurred.[51] This approach reflects a simple model of how disclosures generally occur: one party, A, gives information to another party, B, that B did not already know. In the rare case where a record is given to a person who the agency can demonstrate already knew of its contents, no disclosure is found.[52]

So far as it goes, this intuitive approach makes sense. Disseminating a record to one already aware of it would do little if any harm to the person described in the record. In this respect, it is also consistent with the Act's text, which only provides a cause of action for damages if the agency acted "in such a way as to have an *adverse effect* on an individual."[53] More fundamentally, this approach comports with the Act's underlying policy. The available evidence suggests that Congress was not, by passing the Act, attempting to impose strict liability on agencies for data-handling.[54] Rather, by creating numerous exceptions to the prohibition on disclosure and by leaving much of the FOIA intact,[55] Congress expressed a strong policy preference in favor of allowing public access to government information where doing so would not seriously infringe individual privacy interests.[56]

---

51 *See Kline*, 927 F.2d at 524.

52 *See, e.g.*, Hollis v. U.S. Dep't of the Army, 856 F.2d 1541, 1545 (D.C. Cir. 1988); Reyes v. Supervisor of Drug Enforcement Admin., 834 F.2d 1093, 1096 n.1 (1st Cir. 1987); Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1341 (9th Cir. 1987); Pellerin v. Veterans Admin., 790 F.2d 1553, 1556 (11th Cir. 1986); FDIC v. Dye, 642 F.2d 833, 836 (5th Cir. 1981).

53 5 U.S.C. § 552a(g)(1)(D) (2006) (emphasis added). Although by its terms the statute provides a minimum damage award of $1,000 when an improper disclosure yielding such "adverse effect" is established, *see id.* § 552a(g)(4)(A), the Supreme Court recently held that a plaintiff alleging improper disclosure in violation of the Act cannot recover a monetary award without first proving "actual damages," Doe v. Chao, 540 U.S. 614, 627 (2004).

54 *See* H.R. REP. NO. 93-1416, at 13 (1974), *reprinted in* SOURCE BOOK, *supra* note 28, at 306; *see also supra* note 37 and accompanying text (discussing the Privacy Act's legislative history). Although recent legislative proposals have aimed to restrict agencies' disclosure practices even further, *see, e.g.*, Identity Theft Prevention Act of 2005, H.R. 220, 109th Cong. § 3 (1st Sess. 2005) (proposing an amendment to the Privacy Act to limit disclosure of social security numbers), proposals continue to surface that would create even more exceptions to the disclosure prohibition, *see, e.g.*, Real Security Act of 2006, S. 3875, 109th Cong. § 2310 (2d Sess. 2006) (proposing exceptions to the Privacy Act for disclosure of certain terrorism or national security-related information); S. 2786, 109th Cong. § 1 (2d Sess. 2006) (proposing a new exception for disclosures of information (1) "regarding assistance provided to individuals in connection with a major disaster or emergency," or (2) "to another government agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for purposes of complying with a Federal or State sex offender registry or notification law").

55 *See* 5 U.S.C. § 552a(b)(2).

56 *See* Cochran v. United States, 770 F.2d 949, 954–55 (11th Cir. 1985) (noting that the Privacy Act's structure, which leaves much of the FOIA in place and creates an exception for

C. Hard Cases: When the Conventional Approach to Disclosure Breaks Down

To be sure, the common sense approach is not without its shortcomings. It may be difficult, time consuming, and expensive for either party in a Privacy Act suit to determine *ex ante* what third parties already know.[57] Determining what was known when by whom may be equally difficult *ex post*. For the most part, however, the conventional approach functions adequately in simple cases—e.g., where A gives a record about B to C that C did not already know about.

But the reality of modern agency information handling increasingly bears little resemblance to this simple paradigm of disclosure that underlies the conventional approach to adjudicating Privacy Act claims. In such cases, the common sense approach courts traditionally follow is of little value. Some of these modern disclosure practices fall within an exception to the Act's broad prohibition, of course, but this is far from universally true.

1. The Complexity of Modern Agency Disclosures

Both because of legal requirements, such as the FOIA, and out of convenience and necessity, agencies increasingly make records and other data publicly available on a much broader scale than in the past, especially through the Internet.[58] Although this complicates the disclosure analysis in several ways, the most important consequence is that agencies constantly make available information through elec-

---

disclosures required by the FOIA, reflects a congressional policy in favor of continued disclosure of information if it does not jeopardize individual privacy); *see also* Martin v. Harrison County Sheriff's Dep't, No.1:06CV62, 2006 WL 3760132, at *5–6 (N.D. W. Va. Dec. 15, 2006) (citing *Cochran*, 770 F.2d at 954–55) (adopting report and recommendation of magistrate judge).

57 If this were not true, it is difficult to imagine how Privacy Act disclosure lawsuits would arise. If an agency officer knew, for instance, that a certain third party already knew the contents of a record, there would be no need to disclose it. If the agency officer was unsure, it might be difficult to discern what the third party knew about the record's contents without revealing part of it. Similarly, if a plaintiff knew a recipient was already aware of the disseminated information before receiving it from an agency, the plaintiff likely perceived no harm.

58 *See* Reitz, *supra* note 23, at 734; Bloom, *supra* note 26, at 6. Besides the constantly decreasing cost of promulgating information electronically, as well as the broader shift towards "e-government," Reitz, *supra* note 23, at 733–34, a key driving force behind agencies' expanding use of Internet publication of data is found in the FOIA. In 1996, Congress amended the FOIA to require large amounts of agency records to be made available on the Internet or similar electronic means. *See generally* Electronic Freedom of Information Act Amendments of 1996, Pub. L. No. 104-231, 110 Stat. 3048 (1996) (amending 5 U.S.C. § 552). Since that time, agencies have gone far beyond required disclosure and have made vast amounts of previously inaccessible data open to the public. *See* Reitz, *supra* note 23, at 734.

tronic means that was *already* open to the public in some form.[59] The question courts must therefore confront is the effect of the prior public accessibility of a record on whether subsequent efforts to disseminate the record amount to "disclosure."[60] In other words, the issue is not merely whether a particular recipient actually knew of the contents of the record he received. Instead, courts must decide what level of prior public accessibility is enough to prevent a future promulgation of that information from constituting disclosure.[61]

The problem is further complicated by the various ways information can be made accessible to the public. First, the prior release can vary in several dimensions. The entity that made it available previously may have been the same agency that allegedly made the new disclosure,[62] another governmental entity,[63] or a private party, such as Westlaw or LexisNexis.[64] The degree of prior accessibility can also vary widely: the material may have been publicly available when the disclosing agency first obtained it,[65] whether thoroughly "aired in the public domain"[66] or merely a matter of public record that remained

---

59 *See* Bloom, *supra* note 26, at 8.

60 *E.g.*, Oja v. U.S. Army Corps of Eng'rs, 440 F.3d 1122, 1129–30 (9th Cir. 2006); Barry v. U.S. Dep't of Justice, 63 F. Supp. 2d 25, 27–28 (D.D.C. 1999).

61 For example, if the Office of Personnel and Management ("OPM") retrieved the President's official personnel record—containing his name and official title—from a qualifying system of records and then released this information in a press release on its Web site, could this press release really constitute a disclosure prohibited by the Privacy Act? Assuming none of § 552a(b)'s exceptions applied—and setting aside the question of whether the President could demonstrate the "adverse effect" necessary to prevail on a damages claim, *see* 5 U.S.C. § 552a(g)(1)(D) (2006)—the answer under the traditional approach is "yes." If the press release were read by a person who did not know the President's name, OPM would have violated federal law, and the President could sue for injunctive relief and damages. The fact that the information at issue—a public official's name and title—is not "personal" or "sensitive" by any ordinary definition would not be enough, under the OMB Guidelines, to keep the release of that information from amounting to a disclosure under existing law. *Cf.* Quinn v. Stone, 978 F.2d 126, 133 (3d Cir. 1992) (noting that "interpreting the Act to cover only personal or sensitive information would be inconsistent with the Privacy Act Guidelines issued by the Office of Management and Budget," as the Guidelines define "record" to mean "*any* item of information about an individual that includes an individual identifier. . . . includ[ing] as little as one descriptive item about an individual" (quoting Privacy Act Implementation, 40 Fed. Reg. 28,947, 28,951–52 (July 9, 1975))). In short, unless public accessibility of the information plays some role in the analysis, the Privacy Act may reach situations its framers surely never intended it to cover.

62 *See, e.g.*, *Oja*, 440 F.3d at 1125–26.

63 *See, e.g.*, *Barry*, 63 F. Supp. 2d at 27.

64 *See, e.g.*, Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156, 161 (D.D.C. 2006).

65 *See, e.g.*, *Quinn*, 978 F.2d at 132–33; Covert v. Herrington, 667 F. Supp. 730, 739 (E.D. Wash. 1987), *aff'd*, 876 F.2d 751 (9th Cir. 1989).

66 *See, e.g.*, *Barry*, 63 F. Supp. 2d at 27–28.

"practically obscur[e]" in fact.[67] Second, the subsequent dissemination can also vary in degree, medium, entity responsible for publication, or some combination of these. When the prior release and subsequent dissemination are considered together, the possible combinations are virtually limitless.[68]

Although many unique permutations are possible, the common thread is that the information allegedly disclosed was already available to the public to some degree, and it was only made *more* accessible to the public by the agency's action. Perhaps the information was officially public but practically obscure, or perhaps it was made widely known through nongovernmental channels and then officially publicized by an agency. But in each case, the government took some step to make already 'public' information 'more public.' Whatever the circumstance, none of these cases bear enough resemblance to the classic disclosure paradigm for that model to be of much assistance. In short, courts now face a complex array of scenarios in which the classic disclosure paradigm simply is inapposite.

2. Gaps in the Statutory Exceptions

To be sure, many Internet and other disclosures that agencies have undertaken in the last decade fall within an exception to the Privacy Act. But not every disclosure is covered by an exception. As noted, one crucial exception to the Privacy Act provides that to the extent the FOIA actually *mandates* the dissemination of given infor-

---

67 *Cf.* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762–63 (1989); *Quinn*, 978 F.2d at 138.

68 Courts around the country have faced just such cases in recent years. In *Barry*, for example, the executive branch posted a record on its public Web site after Congress had made it widely available to the public and discussed it in open hearings. *See Barry*, 63 F. Supp. 2d at 27. The court was faced with the question of whether a disclosure took place, even though not every citizen who saw the record on the agency's Web site was already familiar with the contents of the record. *See id.* Similarly, in *Oja v. U.S. Army Corps of Engineers*, the Ninth Circuit addressed whether a disclosure takes place when a government entity publishes information on its Web site that it had previously published on the same or related Web site. 440 F.3d 1122, 1127–34 (9th Cir. 2006).

Courts also have confronted the question of whether a disclosure occurs when a government agency releases information, originally collected from publicly-accessible sources, to persons outside the agency. In both *Quinn*, 978 F.2d at 133–34, and *Covert*, 667 F. Supp. at 739, for instance, the disclosing agencies argued that the information they obtained was already available in public sources such as local telephone books. Perhaps the most complicated scenario of all is that arising in *Doe v. U.S. Department of Labor*, in which the record at issue had been made publicly accessible in hard copy at the agency's headquarters before being published electronically by private third parties and posted on the government agency's official public Web site. 451 F. Supp. 2d at 161.

mation,[69] the Privacy Act does not prohibit its disclosure.[70] This exception is not all-encompassing, however.

First, the FOIA does not require—and therefore the Privacy Act does not permit—the disclosure of "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy."[71] The threshold requirement—that a file must be a medical, personnel, or similar file—has been read very broadly by the Supreme Court.[72] Once this low threshold is met, a court merely asks if there is some protectable privacy interest that would be threatened by a disclosure, and if so, whether the public interest in disclosure outweighs that privacy interest.[73]

Second, even where the FOIA requires records to be made publicly available, it authorizes agencies, "[t]o the extent required to prevent a clearly unwarranted invasion of personal privacy," to "delete identifying details when it makes available or publishes an opinion, statement of policy, interpretation, staff manual, instruction," and other records.[74] If these details are not redacted, the exception for required disclosures does not apply.[75]

---

69 Under the FOIA as amended, some kinds of records must be disclosed only on request, *see* 5 U.S.C. § 552(a)(3) (2006), some must be made immediately available in real or virtual "FOIA reading rooms," *see id.* § 552(a)(2), and some are explicitly required to be published electronically, *see id.*

70 *See* 5 U.S.C. § 552a(b)(2). The Privacy Act expressly exempts from its disclosure prohibition records that are required to be made available under the FOIA. *See id.*

71 5 U.S.C. § 552(b)(6).

72 *See* U.S. Dep't of State v. Wash. Post Co., 456 U.S. 595, 602 (1982).

73 *See* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762 (1989). Importantly, this part of the analysis involves questions very similar to those that are reached in determining whether a disclosure has occurred. In *Reporters Committee*, the Supreme Court recognized (and to some degree addressed) the privacy interest that exists in records that are technically public but practically obscure. *See id.* at 762–71. This, in turn, raises the question, addressed in detail below, of why the current framework, especially given the exemption provided by § 552(b)(6), is not sufficient to handle the concerns that arise in cases where disclosure is uncertain. *See* discussion *infra* Parts IV.B.1, IV.B.5.

74 5 U.S.C. § 552(a)(2).

75 *Cf.* Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156, 173–76 (D.D.C. 2006). It is not clear from existing case law whether publication of a record from which identifying details have been redacted would trigger the Privacy Act's disclosure prohibition. Technically, the Privacy Act prohibits disclosure of the record so long as it was contained in a system of records, 5 U.S.C. § 552a(b)—i.e., was retrieved by name or personal identifier, *id.* § 552a(a)(4)—even if that information is not transferred to the recipient of the record. For a cause of action for damages to arise from such disclosure, however, there must be an adverse effect upon the person described in the record, *see id.* § 552a(g)(1)(D), and unless the individual's identity can be discerned from other facts in the record, it is hard to imagine how an adverse effect would arise if identifying details were not included.

Another key exception allows an agency to disclose more information than the FOIA requires if it first establishes a new "routine use."[76] So long as the agency fulfills certain notice requirements,[77] and so long as the new routine use is "compatible with the purpose for which [the information] was collected,"[78] the agency can disclose otherwise prohibited information without fear of civil suit.[79] But although many disseminations of information on agency Web sites might be protected by a routine use notice, this is not true in every case for several reasons.

First, even if agencies always scrupulously fulfilled the requirement that record notice of routine uses be published in the Federal Register before such uses are made,[80] it seems unlikely that they could always satisfy § 552a(e)(3)(C)'s personal notice requirement. Under that provision, an agency that wishes to disclose information pursuant to a routine use must inform the persons providing that personal information of all routine uses that *may* be made of that information.[81] Thus, if an agency wishes to adopt a new routine use of information it has *already* collected, it must first provide personal notice to *every* individual whose information *may* be subject to that routine use.[82]

Second, the routine use may run afoul of the substantive limits imposed by the Act. A routine use can only be created "for a purpose which is compatible with the purpose for which [the information being disclosed] was collected."[83] Given this vague language, whether a particular disclosure is compatible with the purpose of collecting the information is not always easy to discern.[84] The disclosing agency may believe that a particular disclosure is compatible in purpose with the reason the information was gathered, but a reviewing court may disa-

---

76 *See* 5 U.S.C. § 552a(b)(3).

77 *See id.* § 552a(e)(4)(D) (requiring notice of routine use to be published in the Federal Register); *id.* § 552a(e)(3)(C) (requiring separate notice detailing the routine use to the individual whose information it plans to disclose).

78 *Id.* § 552a(a)(7).

79 *See id.* § 552a(b)(3).

80 *Id.* § 552a(e)(4)(D).

81 *Id.* § 552a(e)(3)(C). The personal notice must be printed either "on the form which it uses to collect the information"—in which case it must be provided to the individual at the time the information is collected—or "on a separate form that can be retained by the individual." *Id.*

82 *See id.*

83 *Id.* § 552a(a)(7).

84 *Cf.* Britt v. Naval Investigative Serv., 886 F.2d 544, 548–50 (3d Cir. 1989) (examining the "concrete relationship" between the disclosing agency's reason for gathering the information and for disclosure), *discussed in* U.S. Postal Serv. v. Nat'l Ass'n of Letter Carriers, 9 F.3d 138, 144–46 (D.C. Cir. 1993) (Silberman, J.) (rejecting the Third Circuit's interpretation in *Britt* and instead employing a labor law specific analysis of "compatability").

gree.[85] If so, the routine use exception will not ultimately shield the agency's actions. As a result, liability in such cases will turn on whether its actions amounted to a disclosure.

Moreover, the difficulty courts face in adjudicating whether the public interest in disclosure outweighs an individual's privacy interest or whether a certain use is "compatible" with the purpose for which information was collected may lead them to look for narrower grounds to resolve cases. They may turn to the threshold question of disclosure to avoid these and other thorny issues.

II. In Search of a Solution: Diverging Definitions of Disclosure in Hard Cases

Courts confronting such "hard cases" under the Privacy Act have developed three divergent approaches to determine whether a disclosure has taken place. Each takes a different view of the Privacy Act's core objective, attributes a different amount of importance to prior public availability of records, and strikes a different balance between retaining traditional conceptions of disclosure and recognizing the practical effect of making information a matter of public record. What all three have in common is that none can be squared simultaneously with language in the statute and the practical realities of disclo-

---

85 For instance, in *Doe v. U.S. Department of Labor*, 451 F. Supp. 2d 156 (D.D.C. 2006), the ECAB argued that including details of Doe's medical history in its decision was essential to correctly determining his claim, which involved his right to medical benefits, and that publishing his decision fell within its routine use notice because the ECAB needed to compile a corpus of precedent to aid in the adjudication of future cases. *Id.* at 174. The court rejected this argument, holding that the ECAB's practice of publishing its decisions on its Web site could not be protected by the routine use exception because publishing the plaintiff's name alongside his personal medical information was "both patently unnecessary and plainly incompatible with . . . the purpose for which the plaintiff's medical information and his identity were collected by the ECAB." *Id.* at 175. The court's holding on this point evidently struck a nerve within the Department of Labor: within months of the court's opinion being issued, the Department reached an out-of-court settlement with Doe—acceding to many of his original demands such as the removal of his decision from all electronic government sources, as well as attorneys' fees—in exchange for his support of a request that the court vacate its opinion. *See* Joint Motion to Vacate Court's Order and Memorandum Opinion of September 6, 2006 at 3–5, *Doe*, No. 05 Civ. 2449 (D.D.C. Mar. 20, 2007). Surprisingly, the court granted the parties' request, *see* Order at 1–2, *Doe*, No. 05 Civ. 2449 (D.D.C. Mar. 22, 2007), notwithstanding Supreme Court and D.C. Circuit precedent limiting vacatur due to settlement to very narrow circumstances, *see* U.S. Bancorp Mortgage Co. v. Bonner Mall P'ship, 513 U.S. 18, 29 (1994); Mahoney v. Babbitt, 113 F.3d 219, 223 (D.C. Cir. 1997); *see also* 1992 Republican Senate-House Dinner Comm. v. Carolina's Pride Seafood, Inc., 158 F.R.D. 223, 224 (D.D.C. 1994). In all events, the fact that the Department of Labor took the extraordinary step of seeking the vacatur of the court's opinion suggests the importance that the agency attached to removing an unfavorable precedent constraining the scope of permissible routine uses.

sure. In the end, both the deficiencies of each alternative and the need for national uniformity suggest a statutory solution, which is proposed in Part III.

A. Actual Recipient's Knowledge Standard

The first approach courts have followed, termed here the "actual recipient's knowledge" standard, defines disclosure to mean any dissemination of a record covered by the Act to an individual who did not *actually know* that information before.[86] Where the information in the record was already available to the public before the alleged disclosure took place, courts following this approach find that a disclosure has occurred unless the agency shows that the *specific recipient* actually knew the information at the time of disclosure.[87] The approach thus attributes no special import to whether information was "readily accessible" to the public; only the recipient's own knowledge matters.[88]

This approach offers several important advantages, including consistency with the Act's text and structure,[89] and relative simplicity in

---

86 Quinn v. Stone, 978 F.2d 126, 134 (3d Cir. 1992) (noting that "the [Privacy] Act is not violated where the agency makes available information which is already known by the recipient"); *accord* Kline v. Dep't of Health & Human Servs., 927 F.2d 522, 524 (10th Cir. 1991); Hollis v. U.S. Dep't of the Army, 856 F.2d 1541, 1545 (D.C. Cir. 1988); Pellerin v. Veterans Admin., 790 F.2d 1553, 1556 (11th Cir. 1986).

87 The Third Circuit's decision in *Quinn v. Stone*, 978 F.2d at 134, illustrates this approach at work. There, a state agency was investigating two civilian employees of the U.S. Army for illegally using multiple addresses to obtain more than one hunting license each. *See id.* at 128–30. The Army disclosed the couple's home address information to a state game commissioner, which the couple argued constituted a disclosure. *Id.* at 130–31. The Army argued that even though the address information was a record retrieved from a system of records, no disclosure took place because the information was already available in local telephone directories. *Id.* at 133–34. The court rejected the Army's argument, expressly dismissing the possibility that knowledge of information available to the public could be imputed to all members of the public. *See id.* at 134–35 (noting that the mere fact that information was "readily accessible to the members of the public" did not change the outcome fact that a disclosure took place); *see also* Gowan v. U.S. Dep't of the Air Force, 148 F.3d 1182, 1193 (10th Cir. 1998) (quoting *Quinn* and reversing the district court's holding that matters of public record are not subject to the Privacy Act).

88 *See Quinn*, 978 F.2d at 134.

89 Without a statutory definition to provide guidance, the common sense conception of disclosure—i.e., a dissemination of information to a party not already aware of it—appears to be a natural reading of the Act's language. *Cf.* BLACK'S LAW DICTIONARY (8th ed. 2004) (defining "disclosure" as "[t]he act or process of making known something that was previously unknown; a revelation of facts"). The approach comports with the Privacy Act's structure—as well as that of its counterpart, the FOIA—because only a broad definition of disclosure makes sense of the many exceptions Congress has created. *See Quinn*, 978 F.2d at 134 (noting that an approach that made the existence of a disclosure turn on prior public accessibility of information "would eviscerate the [Privacy] Act's central prohibition . . . against disclosure," and that "[t]o define disclo-

application—at least for reviewing courts analyzing the disclosure *ex post*.[90] But by giving so little weight to prior public availability of information, the actual recipient's knowledge standard undermines the Privacy Act's core purpose to some degree. Unlike the interests protected by the law of defamation,[91] the core privacy interest safeguarded by the Act lies in how many other individuals know, or easily could find out, the particular details that a government record contains about a private citizen.[92] Whether a particular dissemination injures this interest depends on how widely available the information already was and the concomitant risk that others will discover it.[93]

---

sure so narrowly as to exclude information that is readily accessible to the public would render superfluous the detailed statutory scheme of twelve exceptions to the prohibition on disclosure").

90 In contrast to the many difficult analytical labyrinths that have come to characterize FOIA and Privacy Act litigation, *see* Cochran v. United States, 770 F.2d 949, 954–55 (11th Cir. 1985), a court concerned only with what individual recipients of information already knew has a clear, discrete task that courts are accustomed to undertaking, *cf. Quinn*, 978 F.2d at 134 (examining whether the recipients actually had prior knowledge of the information). An approach that gives substantial weight to the degree of public accessibility or awareness of given information, by contrast, could potentially lead the parties and the court into a very burdensome factual inquiry about what the public knows and how easy it is for the public to view specific records. *Cf.* Barry v. U.S. Dep't of Justice, 63 F. Supp. 2d 25, 27–28 (D.D.C. 1999). On the other hand, in cases of Internet disclosure to multiple recipients—such as *Barry*—it may be difficult in practice for courts to determine whether each recipient already knew the record's contents. For example, if an agency posts a record on its Web site, it may be difficult or impossible to identify each separate individual who accessed the record through the Web site, or even to calculate how many individuals did so. Even if those recipients could be counted and identified, they may be spread around the globe, and the cost in time and money of obtaining the testimony of each—whether at trial, through deposition, or even by affidavit—may be too high for the parties to bear.

91 *Cf.* Daniel J. Solove, *A Taxonomy of Privacy*, 154 U. PA. L. REV. 477, 530–52 (2006) (distinguishing the privacy interest in disclosure from the interest in avoiding distortion that arises in common law defamation claims).

92 A number of scholars have explored at length the theoretical underpinnings of a privacy interest in the disclosure of private but true information. *See, e.g.*, *id.* at 530–41 (describing disclosure, exposure, and increased accessibility); Coles, *supra* note 44, at 961–64 (examining the foundations of a "right to disclosural privacy" both in constitutional terms and as basis for Privacy Act's prohibition on disclosure). For a contrary viewpoint grounded in First Amendment concerns, see Eugene Volokh, *Freedom of Speech and Information Privacy: The Troubling Implications of a Right to Stop People from Speaking About You*, 52 STAN. L. REV. 1049, 1050–51 (2000) (arguing that preventing others' disclosure of one's private information infringes First Amendment speech interests).

93 *See* Solove, *supra* note 91, at 539–41. As the Supreme Court recognized in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), even at common law the extent of one's privacy interest in preventing the disclosure of certain information depended "on the degree of dissemination of the allegedly private fact." *Id.* at 763. Extending that principle (in slightly modified form) to the FOIA provisions that exempt from the disclosure requirement any materials that would, if disclosed, impermissibly infringe individual privacy interests, the Court held that where information is officially available to the public but

Additionally, even if this approach were simpler for courts to apply *after* an alleged disclosure has taken place, it assigns to agencies the often impossible task of ascertaining *before* disseminating a record which members of the public already know of the record's contents.[94]

B. Constructive Public Knowledge Standard

A second approach some courts follow, labeled here the "constructive public knowledge" standard, responds to these concerns by taking a very different view. Under this approach, the court concludes that no disclosure takes place when an agency disseminates information that is already contained in public records.[95] Where the allegedly disclosed information was previously a matter of public record—or otherwise openly available to the public—the court thus imputes knowledge of the record to the public at large. Some courts apply a rebuttable presumption that each member of the relevant public was aware of the information.[96] Others effectively impose a conclusive

---

"practical[ly] obscur[e]," the individual privacy interest "is in fact at its apex." *Id.* at 780; *cf.* Bloom, *supra* note 26, at 63 (highlighting the importance of *Reporters Committee* as the first case to mark the difference between practically obscure or uncompiled information and public, amalgamated information). That principle, however, is a double-edged sword. *Cf. Reporters Comm.*, 489 U.S. at 763–64 (distinguishing between information that is "freely available" to the public and that which is "hard-to-obtain" or compile). The degree to which information was previously made accessible to the public at large, even if not to a particular recipient, is relevant both to (1) whether any new harm occurred as a result of disclosure, and (2) whether the subsequent disclosure was made in the "intentional or willful" manner necessary for a plaintiff to be entitled to damages, 5 U.S.C. § 552a(g)(4) (2006). A conception of disclosure that takes no account of the prior public availability or even awareness of information ignores these concerns and transforms the Act's disclosure prohibition into strict liability.

94 Although agencies may be able to keep track of the number of times a specific record is accessed by the public, it would require extraordinary effort and expense to ascertain *before* making such records publicly available how widely known their contents already are. Moreover, agencies presumably do not make the decision of whether and how to publish records on a case-by-case basis. Rather, given the notice requirements for routine use notices, *see supra* note 36 and accompanying text, agencies presumably decide whether to make available an entire system of records or certain information from each of those records.

95 *See, e.g.*, FDIC v. Dye, 642 F.2d 833, 836 (5th Cir. 1981).

96 *See id.* The plaintiff can rebut this presumption by showing that the information, though technically a matter of public record, was not genuinely public information prior to the new disclosure. *See id.* In *Dye*, for example, an FDIC debtor alleged that the FDIC violated the Act by advertising foreclosure sales of his property in a broader geographical area than required by state law. *Id.* at 834–35. The FDIC argued that no disclosure took place because the information it disseminated was already public: by publishing advertisements in the counties where it was required to advertise by law, the FDIC had made the foreclosure sales public in the "extra" territory. *See id.* at 836. The Fifth Circuit agreed with the FDIC, noting that "the release of public information to the same 'public' is not a disclosure." *Id.* The court explicitly acknowledged that there was no evidence that the specific recipients themselves were actually aware of the information the FDIC's advertisements contained. *See id.* But because the information

presumption that official public records are in fact publicly known.[97] Under either approach, the basic premise is the same.

This approach offers two advantages over the actual recipient's knowledge standard. First, it makes at least some effort to account for the practical effect of prior public availability of information. Second, it focuses to some degree on prior actions of the same agency alleged to have redisclosed the information.[98] This ensures that agencies themselves bear responsibility for the steps they take to make information public. It also enables the agency (*ex ante*) and the court (*ex post*) to determine more easily the prior status of the redisclosed information.[99]

The constructive public knowledge standard ultimately fails for two reasons, however. First, it is difficult, if not impossible, to square with the language of the statute.[100] Second, it often gives too *much*

"was legally published in . . . the adjoining county," the court "f[ound] it a compelling inference that foreclosure sales publicized in [one county] are or naturally become public information in [the] adjoining . . . [c]ounty." *Id.* The court treated this inference as a rebuttable presumption, holding that Dye *could* have responded with evidence that the information contained in the advertisements was not in fact "public information" in the adjoining county. *See id.* Because Dye did not do so, the presumption was not rebutted, and thus the court found no disclosure. *See id.*

97 *See, e.g.*, Lee v. Dearment, No. 91-2175, 1992 WL 119855, at *2 (4th Cir. June 3, 1992); Smith v. Cont'l Assurance Co., No. 91 C 0963, 1991 WL 164348, at *5 (N.D. Ill. Aug. 22, 1991). Although these courts do not explicitly announce that they are applying a conclusive presumption, they do not inquire at all into rebuttal evidence or even indicate that it could have been offered. *See, e.g.*, *Lee*, 1992 WL 119855, at *2. Therefore, such courts collapse the presumption of public knowledge into a conclusion that matters of public record are essentially incapable of being 'redisclosed.' In *Lee*, for example, the Fourth Circuit concluded that no disclosure took place because the information at issue had already been included in a public court filing. *Id.* at *2. The court did not even mention the possibility that Lee had an opportunity to offer evidence showing either that the information was not genuinely "public" or that the insurer was not aware of it until it received the Office of Workers' Compensation Programs' ("OWCP") subsequent disclosure. *See generally id.*

98 *See*, *e.g.*, *Dye*, 642 F.2d at 836; *Lee*, 1992 WL 119855, at *2.

99 An agency considering a new dissemination likely will find it easier to identify what steps it itself has taken previously to distribute a record than to identify which members of the public know of the record. In *Dye,* for instance, the FDIC presumably knew (or could easily ascertain) where it had already advertised Dye's foreclosure sales. *See* 642 F.2d at 834–35. Likewise, in *Lee*, the OWCP likely could have determined from a simple inquiry that it had already released Lee's records by filing them in court. *See* 1992 WL 119855, at *1–2. As a result, agencies will know before they "redisclose" the record whether and to what extent they have already made it a matter of public record. Additionally, courts reviewing alleged disclosures will find it less difficult and time consuming to evaluate specific past agency actions than to inquire how widely known a specific record was in the general population.

100 Nothing in the Privacy Act's language directly suggests the sweeping exception from the disclosure requirement that this approach would impose. *See* 5 U.S.C. § 552a(b) (2006). Of course, one might reasonably infer from the term "disclosure"—as does the actual recipient's

weight to prior agency actions that made information a matter of public record. The legal fiction that members of the public have any real knowledge of all official public records simply strains credulity.[101] Although this problem is accentuated when the standard is framed as imposing a conclusive presumption, a rebuttable presumption may be rebuttable in name but conclusive in practice.[102]

C. Actual Public Knowledge Standard

In between these two approaches is a third standard that some courts have followed,[103] termed here the "actual public knowledge

---

knowledge standard, *see supra* Part II.A—a requirement that the recipient not already know the communicated information. But it stretches the word considerably more to say that it does not encompass revelations of material already a matter of public record.

101 The Supreme Court recognized this very point in *Reporters Committee*, where it sharply distinguished between material that is "freely available" to the public and information that is officially a matter of public record, but in reality a "practical obscurity." U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762–64 (1989)*; see also* DOJ OVERVIEW, *supra* note 40, CONDITIONS OF DISCLOSURE TO THIRD PARTIES § (A), *available at* http://www.usdoj.gov/oip/1974condis.htm (noting that "one might argue that to say that no 'disclosure' occurs for previously published or public information is at least somewhat inconsistent with the Supreme Court's decision in [*Reporters Committee*]"). The Court's later decision in *U.S. Department of Defense v. Federal Labor Relations Authority,* 510 U.S. 487 (1994), further underscores the point. Relying in part on *Reporters Committee*, the Court reiterated the importance of the distinction between officially and genuinely public information: "An individual's interest in controlling the dissemination of information regarding personal matters does not dissolve simply because that information may be available to the public in some form." *Id.* at 500. Applying that broad principle, the Court held that union members who declined to provide their home addresses to their union had a substantial privacy interest in their addresses—sufficient to preclude disclosure under the FOIA—even though that information could also be gathered from public sources, including local phonebooks and voter registration lists. *See id.* at 500–01.

102 Plaintiffs may discover it almost impossible to prove a negative, i.e., to show that matters of public record were not widely known in a given community. To the extent that they can do so, the approach may devolve into the actual recipient's knowledge standard as the parties struggle to demonstrate what specific members of the relevant public knew at what time.

103 This appears to be the approach most frequently employed by the District Court for the District of Columbia, which is arguably the most important trial-level court in interpreting the Privacy Act because § 552a(g)(5) makes the District of Columbia a universal venue for suits under the Act. *See* DOJ OVERVIEW, *supra* note 40, CIVIL REMEDIES § (F)(2)(2004), *available at* http://www.usdoj.gov/oip/1974civrem.htm. For example, in the influential case of *King v. Califano*, 471 F. Supp. 180 (D.D.C. 1979), decided less than five years after the statute was enacted, the court observed that "although the Privacy Act does not define disclosure, the term denotes the imparting of information . . . which was previously unknown to the person to whom it [was] imparted," *id.* at 181. Finding that the information at issue was already "publicly *known* prior to the publication" that allegedly constituted the disclosure, the court concluded that no disclosure had in fact taken place. *Id.* (emphasis added); *cf.* Scarborough v. Harvey, 493 F. Supp. 2d 1, 16 n.29 (D.D.C. 2007) (rejecting the defendant's argument that no disclosure occurred where the information was *merely available* to the public before the alleged disclosure). The D.C. Circuit's approach is somewhat less clear, but it appears to be generally consistent with this

standard." Courts following this approach look to the degree to which the entire public was *actually* aware of the record's contents before the alleged disclosure.[104] Instead of ignoring prior agency actions that make a record publicly known or alternatively treating information's designation as a public record as dispositive, this middle approach focuses on the actual effectiveness of prior steps that resulted in increased public awareness of the record.

By taking account of the practical effect that prior public awareness of a record has on the harm of subsequent redisclosure, this approach strikes a more careful balance between giving prior public

framework. *See, e.g.*, Hollis v. U.S. Dep't of the Army, 856 F.2d 1541, 1545 (D.C. Cir. 1988); *cf.* Pilon v. U.S. Dep't of Justice, 73 F.3d 1111, 1123 n.10, 1124–26 (D.C. Cir. 1996) (finding a disclosure took place, despite agency's claims that the recipient had already come into contact with the record, where the agency failed to offer evidence that the specific recipient "remembered and could reconstruct the document's material contents in detail at the time he received it," but noting that the case did "not present the question of whether an agency may . . . release a document that has already been fully aired in the public domain through the press or some other means").

104 *See, e.g.*, Barry v. U.S. Dep't of Justice, 63 F. Supp. 2d 25, 27–28 (D.D.C. 1999). At issue in *Barry* was a report prepared by the Department of Justice resulting from an investigation of several Immigration and Naturalization Service ("INS") officials—including the plaintiff, Barry—which accused the officials of intentionally misleading members of Congress. *Id.* at 26–27. Although it provided the report to a congressional subcommittee upon request, the Department asked that the report not be released to the public because of the privacy interests of persons, such as Barry, who were described in the report. *Id.* at 27. A member of the subcommittee, however, relayed the report to the media, and soon several prominent newspapers ran articles describing its contents, discussing at length the report's description of Barry's role. *Id.* Ultimately, the subcommittee held a public hearing on the report, during which Barry's involvement was discussed in detail, and made the report itself publicly available prior to the hearing. *Id.* Several days later, the Department published the report officially, and months later made it available on its public Web site. *Id.* Barry then brought suit against the Department under the Privacy Act, alleging that the Department's posting of the report on the Internet constituted an impermissible disclosure. *See id.* (A Privacy Act suit against Congress was barred because Congress is not an "agency" covered by the Act. *See* 5 U.S.C. § 552a(a)(1) (incorporating the FOIA's definition of "agency," which does not include Congress)). The members of Congress who directed the disclosure of Barry's report, however, might be liable in an ordinary tort action. *Cf.* Hutchinson v. Proxmire, 443 U.S. 111, 127–33 (1979) (holding that members of Congress can be liable, notwithstanding the Speech or Debate Clause, for defamatory statements contained in newsletters and press releases made available to the public).

The court thus faced the question of "whether an agency 'discloses' information by posting it on the Internet when it is already public." *Barry*, 63 F. Supp. 2d at 27. Rejecting the plaintiff's invitation to apply the actual recipient's knowledge standard, but declining to give presumptive weight to the fact that the report had already been made a public record, the court looked to the degree to which the report had been aired in public. *See id.* at 27–28. Noting the aggregate public exposure the report had received, *see id.* at 27 (describing prior disclosure through newspaper accounts, public congressional hearings, and formal release by Congress), the court concluded that the plaintiff no longer "had [a] protectable privacy interest in the Report at the time of its posting on the Internet," *id.* at 28. Absent a protectable privacy interest, the court concluded that no disclosure took place, and thus the Act was not violated. *See id.*

disclosure no effect and giving it conclusive force. But although it avoids some of the problems encountered by the other approaches, it encounters several pitfalls of its own. In addition to being difficult to reconcile with the statute's text, it requires the agency (*ex ante*) and the parties and the court (*ex post*) to engage in a complicated, time-consuming, and likely expensive inquiry into exactly how much of the public knew of the disputed record's contents at what time.[105]

Moreover, this approach allows courts to consider the effect of third parties' actions in making a record more widely circulated. At a certain level, this seems consistent with the principle articulated in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press* that what is really at issue in FOIA and Privacy Act disclosure cases is how prevalent knowledge of the record is among the general public, however the public acquired that information.[106] But at the same time, this allows agencies to exploit what might be called a "third party disclosure loophole." Because it excludes from the definition of disclosure an agency's actions that disseminate information already widely circulated among the public, this middle approach creates an incentive for agencies to shield disclosures behind private third parties' actions.[107] Notably, these third parties are also likely to es-

---

105 The court's task under this approach is even more difficult than under the first standard considered: instead of evaluating the single individual recipient's knowledge, the court must determine public awareness, a more amorphous concept, which may require data and expertise not easily at the court's disposal. Even assuming, for example, that a court appointed an expert to conduct appropriate survey research—and setting aside the enormous cost this might generate—the court itself would still face several questions of line-drawing: What proportion of the public must know of certain information for it to be "public"? What subset of the public should be surveyed? How precise must their knowledge be?

106 *Cf.* U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 763 (1989) (noting that "the extent of the protection accorded a private right at common law rested in part on the degree of dissemination" of the record).

107 For example, a government agency that desires to release a record to the public could begin by releasing the record through channels that are officially public but practically obscure. A private (or in some cases, even public) third party—such as a newspaper, *see Barry*, 63 F. Supp. 2d at 27, or legal subscription service, *see* Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156, 161 (D.D.C. 2006)—perhaps even at the behest of the agency, might publish the record and circulate it widely, dramatically increasing public awareness of its contents. Once the information has been thoroughly aired through private channels, the agency can publish the record openly without fear of violating the Act.

A poignant illustration is found in the facts of *Doe*. There, Doe's ECAB decision was released at some time after its issuance to private third party publishers—who in turn posted it on their Internet-based services—and was also published on the ECAB's own Web site. *See id.*; Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment, Exhibit B at 3, *Doe*, 451 F. Supp. 2d 156 (No. 05 Civ. 2449). After the court's decision in *Doe* was issued, the ECAB contended that it should not be required to remove or redact Doe's decision from its own Web site "[b]ecause Doe's ECAB decision is available on commercial legal research services"

cape liability.[108] Although such collusive plots between agencies and private parties may be uncommon,[109] the crucial point is that this approach undercuts the Privacy Act's core purpose by enabling government agencies to disclose information solely because of third parties' actions,[110] effectively making citizens' rights against government invasions of privacy contingent on the conduct of private third parties.[111]

III. Redefining Disclosure for a Digital Age

A. A Proposal to Amend the Privacy Act

All three approaches courts have developed to deal with cases involving disclosure of already-public information ultimately fall short

---

such as Westlaw. Defendants' Show Cause Filing at 3–4, *Doe*, No. 05 Civ. 2449 (D.D.C. Sept. 29, 2006). This illustrates precisely the danger that the third party disclosure loophole presents. By focusing instead on the agency's prior acts in considering whether the information was already public, courts can prevent agencies from hiding behind third parties' actions.

108 In other words, not only would the agency escape liability under the Privacy Act—as it had not engaged in disclosure—but so would the private third party, as the Act applies only to the actions of government agencies, *see* 5 U.S.C. § 552a(a)(1), (b) (2006). Moreover, the private third party would likely escape ordinary tort liability as well. Once the government agency makes the record publicly available—even if it remains unpublicized and practically obscure—it would presumably become a matter of public record, and the third party's republication would be immune from liability. *See* 2 RODNEY A. SMOLLA, LAW OF DEFAMATION § 10:44–48 (2d ed. 1999). Additionally, if the third party were a provider of an "interactive computer service" as defined in 47 U.S.C. § 230(f)(2) (2000), then federal law might shield it from liability for republishing information provided directly by the government, *see* 47 U.S.C. § 230(c)(1), (e)(3).

109 One should not, however, underestimate the political incentives that might drive agencies or their officials to seek to publicize information that would violate the Privacy Act. Indeed, the notion that a government agency or official would seek to disclose sensitive information to achieve political ends was at the heart of the prosecution's motive theory in *United States v. Libby*, 429 F. Supp. 2d 1, 4 (D.D.C. 2006). Moreover, when the individual whose sensitive personal information was revealed brought a *Bivens* suit seeking civil damages, the court dismissed the action on the ground that the Privacy Act constitutes a "comprehensive statutory scheme" that precludes such suits, noting in particular that the "plaintiffs could have stated colorable Privacy Act claims based on some of the alleged disclosures." Wilson v. Libby, 498 F. Supp. 2d 74, 87–88, 91 (D.D.C. 2007).

110 One might object that if the information already was made public by third parties, no further harm can come from government disclosure. As discussed in Part IV.A, *infra*, however, there are reasons that disclosure by the government even of information already publicly revealed could cause additional harm.

111 An analogy might be drawn to the confidential communication privilege that exists between spouses. *See, e.g.*, United States v. Montgomery, 384 F.3d 1050, 1056–57 (9th Cir. 2004) (quoting Wolfle v. United States, 291 U.S. 7, 14 (1934)). Generally speaking, each spouse is a holder of the privilege, and neither can forfeit the other's right to invoke the privilege. *See id.* at 1057–58 (noting consensus of the circuits that both spouses, including the nontestifying spouse, are holders of the privilege). If the independent third party disclosure loophole were permitted, it would be parallel to allowing one spouse to waive the privilege held by the other because of the actions of a third party outside the spousal relationship.

because they fail to combine faithfulness to the statute's text, structure, purpose, and policy with ease of practical administration. Perhaps because none achieves all of these objectives, none commands a clear majority of the lower federal courts. Both the divergence of approaches the courts have taken and the deficiencies of each standard reveal the need for a statutory solution that resolves the underlying ambiguity while comporting with the Privacy Act's purpose and structure.

To that end, this Note proposes that the Privacy Act be amended by adding the following definition of "disclose" at 5 U.S.C. § 552a(a)(14):

> (14) the term "disclose" means for an agency or an officer or employee of an agency either—
>
> (A) to disseminate, transfer, or communicate a record or the contents of a record to any person who—
>
> (1) is not an employee or official of the disclosing agency authorized to have access to or know the contents of a record, and
>
> (2) did not, as a result of the agency's prior action, already have access to the record or have knowledge of its contents; or,
>
> (B) to take any action that makes a record or the contents of a record substantially more accessible to members of the public from the agency or its facilities than it was previously accessible from the agency or its facilities.

B. The Proposed Definition in Practice

The new provision offers not one but two definitions of "disclose." Satisfying either is sufficient to prove that a disclosure took place, but each definition will be useful in a different array of cases.[112] The first definition, contained in subpart (A) and modeled on the actual recipient's knowledge standard,[113] is designed to address simple cases of person-to-person disclosure. In a classic Privacy Act case, satisfying subpart (A) will be relatively easy.[114] Although the plaintiff

---

112 Importantly, a court will not be forced to choose which definition to apply: if a plaintiff can satisfy either one, a disclosure has occurred, and the Privacy Act's prohibition on disclosure is triggered. Additionally, nothing would prevent a plaintiff from pleading in the alternative and arguing that both apply, as often would be true.

113 *See supra* Part II.A.

114 For example, if A, an officer in the U.S. Department of Records, gives a record to B that describes C, then a disclosure occurs unless B either is an officer or employee of A's agency

likely also would be able to satisfy subpart (B), the efficiency of pleading and proving a disclosure under subpart (A) will make it unnecessary for the parties or the court to inquire into subpart (B).

The second definition, contained in subpart (B), is aimed at more complex cases. On the one hand, if an agency has not previously done anything to make a record publicly available, then nearly anything that makes the record publicly accessible will amount to a disclosure under subpart (B). This is true regardless of whether the information contained in the records is already actually known by a large portion of the public. On the other hand, if an agency *has* previously made a record accessible to the public in some fashion, then a new effort to disclose the record will only constitute a disclosure if it makes the record substantially more accessible to the public than the record was from the agency's facilities before the new disclosure.

The second proposed definition's core aim is to resolve confusion—in a manner consistent with the Act's purpose and policy—about when and in what cases a given record's prior public availability affects whether subsequent disseminations can amount to disclosure. The only comparison a court has to make is between the *ex post* accessibility of the information from the agency or its facilities and the *ex ante* accessibility from those same sources. The fact that the public already has knowledge from a private source is irrelevant. Additionally, the degree to which the public at large actually knew the disclosed record's contents is also irrelevant, except to the extent that it is probative of the increased public accessibility of the record.

Notably, the approach would not unsettle the outcomes reached in several leading cases in which the courts applied different definitions of disclosure,[115] although this would not be true of every case.[116]

(who is authorized to know the contents of C's record) or already has personal knowledge of the record's contents. In sum, the result in the simple case is left unchanged.

115 In *Quinn v. Stone*, for instance, a court applying this new approach still would find a disclosure because the Army had not previously made the information accessible in any way. *See* 978 F.2d 126, 128–35 (3d Cir. 1992). The record in that case did not show that the agency there, the U.S. Army, previously had communicated the plaintiff couple's address information to the state agency that received it, nor had the Army itself already made that information publicly available in any sense. *See id.* Accordingly, a disclosure would be found under subpart (A). The additional factual inquiry would examine whether the Army had in fact previously made this information publicly available in any sense and to what extent the Army's transmitting of the information to the state game commission, *id.* at 130, increased its public accessibility. Likewise, the result in *FDIC v. Dye*, 642 F.2d 833 (5th Cir. 1981), would be the same. There, the Fifth Circuit found no disclosure applying the constructive public knowledge standard. *See id.* at 836. If the proposed amendment had been in place, no disclosure would have occurred under subpart (A) because Dye did not point to a specific act of the FDIC to transmit the challenged informa-

Its effect on other key provisions of the Act is also minimal. As noted above, the meaning of disclosure is critical in part because of the way it interacts with the Act's statute of limitations provision[117] and the

---

tion to a particular individual recipient. Moreover, no disclosure would have taken place under subpart (B): the Fifth Circuit likely would have found that the FDIC's publishing of Dye's foreclosure sales in an additional, adjoining county, *id.* at 834–35, did not substantially increase the public accessibility of that information, given that the FDIC had already published this information in the adjacent county. Additionally, the Ninth Circuit would have reached the same result in *Oja v. U.S. Army Corps of Engineers*, 440 F.3d 1122 (9th Cir. 2006). There, the Ninth Circuit held that where an agency publishes information at a specific Internet address, removes the information, and then less than a month later republishes identical information at the same address, no new disclosure occurred (although it noted in dicta that a separate disclosure would occur if the information were published at a distinct Web address). *See id.* at 1125, 1133–34. Under the proposed approach, the outcome would be the same, as republication at precisely the same Internet address so soon after removing the information from that address would not appear to increase substantially the information's public accessibility. Whether publishing the information at a different address would amount to such a substantial increase would depend on a variety of other facts, however, such as (1) the difference between the Internet addresses (i.e., whether they were part of the same government agency's domain, e.g., http://www.usdoj.gov, or instead hosted on independent sites) and (2) the relative ease of accessing each address (i.e., if the first address were not susceptible to searching by Internet search engines and Web crawlers, while the second address was open to such searching and indexing, posting on the second site might constitute a disclosure).

116 For instance, *Lee v. Dearment*, No. 91-2175, 1992 WL 119855 (4th Cir. June 3, 1992), would come out differently. Applying a constructive public knowledge approach, the court in that case found that a disclosure did not take place because the information already had been filed in a court's records. *See id.* at *2. But under the proposed approach, by transmitting the information to the insurer, the OWCP likely disclosed that information within the meaning of subpart (A). The case would turn on facts not clear from the Fourth Circuit's opinion, namely, what prior access the insurer already had to the information the OWCP had filed in court. If, for instance, the insurer had been a party to the suit or if the court's documents were published on the public portion of the district court's Web site, it may be that a disclosure would not be found under subpart (A). Likewise, the court's decision in *Barry v. U.S. Department of Justice*, 63 F. Supp. 2d 25 (D.D.C. 1999), also would come out differently, unless additional facts were added to the record. There, the court found no disclosure took place because the information had been aired in the public already by another branch of government and by private third parties. *Id.* at 27–28. Under the proposed approach, a new disclosure would have taken place—under subpart (B)—when the Department of Justice released Barry's record to the public, *id.* at 27, because the Department itself had not previously made the record accessible, and possibly also when it published Barry's record on its Web site, *id*. (This, of course, would depend on how easily accessible Barry's decision was when initially published in hard copy vis-à-vis its ease of accessibility after Internet publication.) Notably, however, the Department very likely would not be liable for damages, as it would be very difficult for Barry to show an "adverse effect" from the Department's disclosure—especially in light of Congress's prior action to publicize the report at issue, *id.* As discussed above, one might conclude from this that the "adverse effect" standard for damages as it already stands is a sufficient safeguard to prevent agencies from facing liability for actions that do not in fact substantially increase public accessibility of information. *See supra* note 53 and accompanying text. At first glance, this might counsel in favor of a rule that attributes significance to prior accessibility from *any* federal government source, not just the agency at issue. Both of these objections are dealt with in Part IV.B, *infra*.

117 *See* 5 U.S.C. § 552a(g)(5) (2006).

provision limiting recovery of damages to "intentional or willful" violations.[118] As the proposed definition does not change the approach courts would take in easy cases that would satisfy subpart (A),[119] neither the statute of limitations nor the damages provision would be affected in such cases.

Moreover, in hard cases where the plaintiff alleges disclosure under subpart (B), the effect on the limitations period and the damages provision are slight. In a case where a record was previously accessible, but the plaintiff alleges that a subsequent agency action substantially increased its accessibility, the plaintiff must file suit within two years of the time she first knew or should have known of the agency's later action.[120] To prevail on a claim for damages, a plaintiff must show that the subsequent agency action increasing the record's accessibility was done willfully or intentionally, which in practice requires only a showing "somewhat greater than gross negligence."[121] Thus, under the proposed approach, the plaintiff would not have to show that the agency *intended* to make his record more accessible or to invade his privacy, but simply that the action resulting in the substantial increase in accessibility was not accidental or inadvertent.

Taken together, the proposed definitions enable courts to continue to resolve simple, conventional cases as they have long done while providing them with a rubric to resolve the hard cases the Privacy Act's authors did not envision. For example, although the court in *Doe v. U.S. Department of Labor* did not have to decide whether a distinct disclosure occurred when Doe's decision was published on the agency's Web site,[122] the proposed approach would provide a framework for it to do so. Setting aside for the moment the publication of Doe's ECAB decision on Westlaw and LexisNexis, the agency did "disclose" his decision under subpart (B) of the proposed amendment when it published it on its public Web site.[123] Although the decision was already a matter of official public record, available for public inspection at the ECAB's headquarters,[124] the extreme obscurity of the decision and the effort required to identify his decision and obtain a

---

118 *Id.* § 552a(g)(4).

119 *See supra* note 114 and accompanying text.

120 *Cf.* Tijerina v. Walters, 821 F.2d 789, 798 (D.C. Cir. 1987).

121 *See* White v. Office of Pers. Mgmt., 840 F.2d 85, 87 (D.C. Cir. 1988) (per curiam).

122 *See* Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156, 162 n.7 (D.D.C. 2006).

123 *See id.* at 161.

124 *See* Defendants' Motion to Dismiss or, in the Alternative, for Summary Judgment, Exhibit B at 3, *Doe*, 451 F. Supp. 2d 156 (No. 05 Civ. 2449).

copy of it from the ECAB's central office in Washington made it far less accessible to the public than when it was first made available on the agency's Web site.

Even when the actions of third party publishers, including Westlaw and LexisNexis, are added back to the equation, the result does not change. Neither Westlaw nor LexisNexis is an "agency" covered by the Privacy Act, and thus their actions cannot trigger the Act.[125] More importantly, under the proposed approach, the efforts of private third parties to publicize a particular record would not affect whether a new disclosure occurs when the *agency* takes steps to make it more public. Instead, agencies will be liable for their own actions irrespective of what third parties have done.

To be sure, adopting the proposed definition does not transform every difficult scenario into an open-and-shut case. It does, however, provide a uniform standard that is consonant with the Act's policy and purposes, that courts can apply without great difficulty, and that pinpoints which particular facts must be found before a Privacy Act disclosure claim can be adjudicated.

IV. The Case for Redefining Disclosure: Costs and Benefits of Updating the Privacy Act

In light of the difficulties courts encounter in trying to fit modern agency information-handling practices into a simplistic, outdated disclosure paradigm, the need for a new approach to disclosure is clear. The solution proposed here is advantageous because it provides a straightforward mechanism to resolve the difficult cases courts increasingly confront while disturbing the remainder of the statutory framework as little as possible. In particular, by focusing on both the relative accessibility of records and government agencies' own actions, the proposal furthers the Privacy Act's underlying policy goals, strikes

---

125 *See* 5 U.S.C. § 552a(a)(1) (2006) (incorporating by reference the definition of "agency" contained in the FOIA, 5 U.S.C. § 552); *see also id.* § 552(f)(1) (defining "agency" as encompassing "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency"). The situation might be different if those third parties acted in concert with the agency. If the ECAB mailed all of its decisions to Westlaw, for example, each such transmission might constitute a disclosure—although this would depend on a variety of factual circumstances. Moreover, if the ECAB and Westlaw had a contract or memorandum of understanding whereby Westlaw actually agreed to publish all of the ECAB's decisions to its subscribers, then the court might ultimately conclude that Westlaw acted on the ECAB's behalf, in light of the prearranged agreement, and for that reason might find the ECAB *did* act to disclose the information through Westlaw's system.

a better balance between giving too much or too little weight to prior disseminations, and closes the third party disclosure loophole.[126] This Part first discusses these key advantages before turning to address five important but ultimately unavailing objections.

A. Advantages of the Proposed Approach

Beyond the general benefits of employing a statutory solution,[127] the particular amendment proposed here offers at least two particular advantages over the existing approaches. The first significant benefit lies in its focus on prior government-created *accessibility*, as opposed to either direct disclosure or the public's actual awareness of the record at issue. This focus is consistent with the OMB's official Guidelines, which indicate that whatever disclosure's precise meaning, it should at least encompass the granting of access to records in addition to their express dissemination.[128]

Additionally, the focus on accessibility abandons the legal fiction that members of the public automatically have any meaningful knowledge of information contained in public records. Imputing such knowledge to the populace, however convenient for courts faced with hard cases, is simply too divorced from reality to be permissible. Focusing instead on how easily the public could have accessed the record before the new dissemination occurred avoids this difficulty by placing the emphasis on the relative *risk* that information would become widely known in the public.

As a result, the proposal strikes a better balance between ensuring agency accountability and realistically assessing the harm caused by redisclosing already public information. On the one hand, the proposal gives more weight than the actual recipient's knowledge standard to prior agency actions making information accessible. The only

---

126 *See supra* notes 107–11 and accompanying text.

127 To the extent that any statutory solution can provide enough clarity to resolve a split among lower courts and offer a workable standard capable of resolving difficult cases, an amendment to the Privacy Act's text provides the preferred means of addressing this uncertainty. By resolving the latent ambiguity through a change in the statute itself, the proposed amendment avoids the need to strain the Act's language to craft an approach consistent with the statute's broader policy. By contrast, if the Supreme Court, for instance, granted certiorari to resolve the circuits' divergent approaches to defining disclosure, it either would have to hew closely to the Act's text and structure—as does the actual recipient's knowledge approach (which, as discussed, is in some tension with the Act's purpose and policy, *see supra* Part II.A)—or it would have to stretch the Act's language to support a constructive or actual public knowledge standard, *see supra* Part II.B–C. A statutory amendment avoids this dilemma.

128 *See* Privacy Act Implementation, 40 Fed. Reg. 28,947, 28,953 (July 9, 1975).

legal reason for giving little weight to such prior disclosures is the Act's current text—which, of course, is no barrier to amendment.

By contrast, giving weight to prior accessibility is consistent with the distinction the Supreme Court recognized in *Reporters Committee* between information that is in fact "freely available" to the public and information that is officially public but a "practical obscurity."[129] Although in that particular case the Court employed the distinction to show that disclosing officially public information can still intrude on individual privacy,[130] the distinction cuts both ways. If prior efforts to make information officially public did not in fact make it widely accessible, then those efforts should not preempt a finding of disclosure. If those prior actions *do* make it substantially easier for the public to obtain the information, however, they are relevant to the privacy interest at stake and should be taken into account when evaluating whether a disclosure has occurred. The proposed approach accomplishes this by making prior accessibility a key part of the disclosure equation.

On the other hand, the proposal gives less weight than the constructive public knowledge standard does to prior agency actions.[131] The same distinction reflected in *Reporters Committee* counsels against giving automatic effect to the prior status of information as a public record. The proposed solution avoids this result by evaluating prior agency actions by reference to their actual effect on the information's accessibility.

Of course, the actual public knowledge standard also strikes a balance between these two extremes. But the amendment proposed here avoids both pitfalls encountered by that approach. First, unlike the actual public knowledge standard, the proposed amendment would not require courts to engage in the difficult task of measuring the public's actual knowledge of a specific record.[132] The measurement problems are indeed substantial, especially from the plaintiff's *ex ante* perspective. An individual plaintiff may find it very difficult, before initiating litigation and engaging in costly discovery, to know with any certainty the degree to which her record was already circulat-

---

129 U.S. Dep't of Justice v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762–64 (1989).

130 *See id.*

131 *See supra* note 98 and accompanying text.

132 *See supra* note 105 and accompanying text. The problem is not merely one of measurement, but one of line-drawing. In this regard, *Barry v. U.S. Department of Justice* was an easy case, as there the degree of prior public exposure was extreme. *See* 63 F. Supp. 2d 25, 27 (D.D.C. 1999). Not every case, however, is likely to provide facts that lean so clearly to one side.

ing in the public.[133] By contrast, courts faced with assessing the *accessibility* of a record will find that inquiry far easier than the task of measuring the public's actual knowledge.[134] Likewise, the focus on accessibility makes it easier for agencies considering a new dissemination of a record to determine whether it will constitute a disclosure.[135]

Second, because of its focus on prior action by the agency itself—as opposed to the action of public and private entities in the aggregate—the proposed approach closes the independent third party disclosure loophole that the actual public knowledge standard leaves open.[136] Under the proposed amendment, an agency's renewed disclosures are compared only to the same agency's prior acts, not those

---

133 One might object that if the individual plaintiff did not know the information had been made public, she likely would not have suffered any cognizable harm. There are several problems with this argument. First, reputational harm can occur without the plaintiff's own knowledge. Second, in the context of Internet disclosure, the plaintiff may know of some of the damage, but it may only be a fraction of the aggregate harm that has occurred. Moreover, there is always the risk that those who have encountered the information might relay it to others, but this is a risk not easily addressed by the statute: the Privacy Act currently does not apply to private parties, *see* 5 U.S.C. § 552a(b) (2006), and it would represent a radical shift to expand it to do so. Moreover, private tort liability for invasion of privacy is likely unavailable for a plaintiff who finds that a private party has redisclosed information that the government officially released as a public record. *See* DAVID A. ELDER, PRIVACY TORTS § 3.15 (2002) (collecting state and federal cases). Third, Internet dissemination also creates definitional problems of its own: does disclosure occur when information is posted, when it is viewed, when it is saved by the user, or at some other point? For each of these reasons, a standard tying liability to what the plaintiff herself knew about her record's prior public availability is undesirable.

134 *See infra* notes 143–45 and accompanying text.

135 *See supra* note 99.

136 As discussed in Part II.C, the actual public knowledge standard would allow agencies to avoid liability for disclosure by (1) making information officially available to the public in a practically obscure source, (2) waiting for (or even arranging for) a private third party to circulate the information publicly, and (3) republishing the record openly in a manner far easier for the public to access. *See supra* notes 107–11 and accompanying text. In addition to *Doe*, the claims asserted in the pending case of *Scarborough v. Harvey* illustrate that this pattern is not merely hypothetical. *See* 493 F. Supp. 2d 1, 4–9 (D.D.C. 2007). In *Scarborough*, the plaintiffs alleged that the Departments of the Army and Defense and the Small Business Administration violated the Privacy Act by disclosing a "criminal alert notice" ("CAN") intended for other government officials that implicated the plaintiffs in a scheme of fraudulent and criminal conduct involving government contracts. *See id.* According to the plaintiffs, in March 2005, one of the agencies released the CAN to (among other recipients) a private organization of businesses in the plaintiffs' industry—which in turn published it in its trade newsletter (with circulation of more than 5,000 member businesses), *id.* at 5—and between April and June 2005, all three of the agencies disclosed the document's contents repeatedly to other private individuals and entities, *see id.* at 6–8. In a response filed under seal, the agencies argued that no disclosure had occurred because the information was already "available to the public." *Id.* at 16 n.29 (citation omitted). The district court explicitly rejected this argument, concluding that the mere prior public availability of the document did not foreclose the plaintiffs' claims of an invalid disclosure. *See id.*

of third parties, making it impossible for agencies to shield subsequent disseminations behind private entities' actions.

This focus on action by the agency itself, which represents the proposed amendment's second major advantage, also yields several additional benefits. At a basic level, Congress's focus and purpose in passing the Privacy Act was to regulate agencies' actions that result in the disclosure of information.[137] Insofar as the Act evolved in response to prior government efforts to reveal private information and to place a limit on the FOIA's sweeping disclosure mandate,[138] it seems appropriate to limit the Act's concern to prior actions of agencies themselves. By contrast, making the propriety of government disclosure hinge on the action of private parties would, to some extent, transform the Privacy Act from a limitation on government agencies' data-handling procedures into a federal tort statute for invasion of privacy.[139]

Moreover, from a policy perspective, there are meaningful differences between official government disclosure of information and private parties' actions to reveal information (without the sanction of the state). First, disclosure by the government may carry with it, in the minds of the information's recipients, the imprimatur of the state, suggesting that the information is presumptively reliable.[140] Second, government disclosure changes the landscape for future invasion of privacy actions, in effect opening the door to private parties' efforts to relay or amplify the information in the public domain.[141]

---

137 *Cf.* Pilon v. U.S. Dep't of Justice, 73 F.3d 1111, 1124 (D.C. Cir. 1996) (noting that the court's "review of the Privacy Act's purposes, legislative history, and integrated structure convince[d it] that Congress intended the term 'disclose' to apply in virtually all instances to an *agency*'s unauthorized transmission of a protected record, regardless of the recipient's prior familiarity with it" (emphasis added)).

138 *See supra* notes 28–31 and accompanying text.

139 This, in turn, might implicate very complicated questions of how far the First Amendment permits the government to go in regulating private parties' speech. *See* Volokh, *supra* note 92, at 1050–51.

140 The information's reliability might be inferred because the Act also requires the government's information to be accurate, *see* 5 U.S.C. § 552a(e)(5) (2006), because individuals providing information to the government generally are required to do so truthfully, *see, e.g.*, 18 U.S.C. § 1001(a) (2006) (prohibiting any person from providing false or fraudulent information "in any matter within the jurisdiction of the executive, legislative, or judicial branch of the Government of the United States"), and because the government has access to more sources of information than might a private party, such as a newspaper or a weblog publishing the same data, *see* HENDERSON, *supra* note 32, at 33–43.

141 For example, if A discloses information about C to B, and then B rediscloses it to D, then C has causes of action against A and B. If the government, however, makes information about C a matter of public record, and B goes on to repeat the information in a newspaper column or on a Web site, under traditional tort law C likely has no cause of action against B

Finally, from a practical perspective, the proposed approach's focus on prior agency action, like its emphasis on accessibility, is far easier for the parties and the court to administer than the existing approaches. Under the proposed amendment, a court need not assess how widely known a specific record was at the time of an alleged disclosure. Instead, it simply must compare any prior agency actions making the record available with the agency's subsequent actions alleged to constitute a disclosure.[142] If the subsequent actions made the information in the record substantially more accessible to the public, the court should find a disclosure has taken place.

The parties to a suit also benefit from easier determination under the proposed approach. Presumably, it is less difficult for an agency to determine what steps it has already taken to make information available to the public[143]—and thus to evaluate whether action it is considering would substantially increase accessibility[144]—than to assess how 'public' the information already is.[145] Similarly, the task of plaintiffs is also simplified, as they only need be on the lookout for official agency action, not the efforts of third parties, to determine whether they have a claim under the Privacy Act. This, in turn, makes it easier to apply

---

because the information already was public. *Cf.* ELDER, *supra* note 133, § 3.15 (collecting cases on the public record limitation). That has not stopped individuals allegedly harmed by such redisclosures from bringing suit, however. *See supra* note 136.

142 The court will find its fact-finding task simplified in large part because the evidence necessary to assess the accessibility of a record before and after the alleged disclosure will be in the hands of a single (institutional) party, i.e., the agency itself. Thus, instead of attempting to measure the knowledge of the public at large or even of specific individuals potentially spread across the country, the court need only review materials submitted by the agency and determine whether the challenged dissemination made the record at issue substantially more accessible. One might object that it is generally unwise to adopt a rule under which only one party to a case has possession and control over the relevant evidence. In the context of assessing whether a disclosure has occurred under the proposed amendment, however, that problem is minimized because the agency has an overriding incentive to produce evidence of its previous disseminations: if it can show that its prior actions made the record at issue just as accessible as the new challenged dissemination, it can avoid liability altogether because no disclosure will have taken place.

143 *Cf.* 5 U.S.C. § 552a(c)(1) (requiring agencies that disclose information covered by the Privacy Act to "keep an accurate accounting of the date, nature, and purpose of each disclosure of a record to any person or to another agency . . . and the name and address of the person or agency to whom the disclosure is made").

144 Presumably, the agency would not take steps to make information public without some purpose to increase access to that information.

145 Of course, to the extent an agency was unsure of whether the steps it was considering would constitute a disclosure, it would have a strong incentive to adopt a new routine use, requiring compliance with routine use notice procedures—which is exactly the result the Act's drafters had in mind, *see* H.R. REP. NO. 93-1416, at 12–13 (1974), *reprinted in* SOURCE BOOK, *supra* note 28, at 306–07.

the prevailing interpretation of the statute of limitations, which runs from when a plaintiff knew or should have known of the alleged violation.[146]

B. Potential Challenges to the Proposed Amendment

Like any suggestion for change, the amendment will undoubtedly give rise to a number of potential objections. This subsection addresses five such critiques pertaining both to the amendment's method and content. While none of these objections are trivial, each ultimately fails to persuade.

1. "If it ain't broke . . . ": The Disutility of Superfluous Statutory Definitions

First, one might argue that the proposal to amend the Privacy Act to specify the definition of this key term is unnecessary at best. As a general matter, whatever one's theory of statutory construction, interpreting the meaning of specific words must be part of it.[147] Because this is a common and essential task courts undertake when interpreting statutes, it would seem that defining a term so common in legal parlance as "disclose" should not require congressional involvement. In the context of the Privacy Act, where changes in technology and agency practice exacerbate the definitional dilemma, the argument takes on added force. If one adopts a theory of construction that does not fix the meaning of words at a particular point in time, then courts

---

146 *See* Tijerina v. Walters, 821 F.2d 789, 798 (D.C. Cir. 1987). Indeed, this standard for calculating when the limitations period begins to run makes *more* sense under the proposed approach than under the existing statute: defining the time a cause of action arises by reference to when a plaintiff knows or should know about prior disclosure is far more reasonable when official agency action provides a clear point to begin imputing such constructive knowledge to a plaintiff. Presumably, the agency still would be required to provide actual notice to individuals of information it discloses. If this notice proves insufficient, however, a more sweeping notice provision could be imposed—requiring notification to individuals whenever the government releases information about them—a solution that would not even be available if the standard were general public availability (as the government could not reasonably be required to provide individuals notice of private parties' efforts to publish information concerning those individuals).

147 This is true even (or especially) of conventional textualist approaches. *See, e.g.*, ANTONIN SCALIA, A MATTER OF INTERPRETATION: FEDERAL COURTS AND THE LAW 22–23 (Amy Gutmann ed., 1997). Although adherents to competing theories of construction might disagree over how courts should go about searching for the meaning of undefined terms, no theory seriously suggests that this is beyond the scope of courts' competence. *See* WILLIAM N. ESKRIDGE, JR., PHILIP P. FRICKEY & ELIZABETH GARRETT, CASES AND MATERIALS ON LEGISLATION: STATUTES AND THE CREATION OF PUBLIC POLICY 669–816 (3d ed. 2001).

are ideally situated to resolve the problem pertaining to disclosure by updating the term to account for such changed circumstances.[148]

Although not entirely meritless, the argument is unpersuasive when the nature and history of the particular definitional issue are brought into focus. From a theoretical standpoint, there are a number of important reasons both to favor legislative definitions of key terms[149] and to constrain courts to adhere to a definition for a given term once they have defined it.[150] Whether or not one views these reasons as dispositive in every area of the law, they are near their strongest where, as here, a waiver of federal sovereign immunity hinges on the definition chosen in a particular case. The courts' long history of reading waivers of sovereign immunity narrowly[151] counsels strongly in favor of clarity and legislative supremacy in providing content to "disclosure."

So too where the limits of individual privacy turn on the meaning of a single statutory term, the need for clarity and stability is near its apex. As the history and complex interplay of the FOIA and the Privacy Act reflect, the balance between individual privacy and public disclosure is a delicate one.[152] Although the fact that individual interests are at stake might superficially support courts' involvement, the difficult social trade-off involved suggests that such decisions should remain the legislature's province.

From a more practical perspective, agencies governed by the Privacy Act also share the need for clarity and stability. Agencies' information-handling practices are not quickly and easily overhauled, and thus agencies likely face very high administrative costs where courts are permitted to change the meaning of key terms at will. Likewise,

---

148 *See, e.g.*, William N. Eskridge, *Dynamic Statutory Interpretation*, 135 U. PA. L. REV. 1479, 1479 (1987); T. Alexander Aleinikoff, *Updating Statutory Interpretation*, 87 MICH. L. REV. 20, 54–63 (1988); *see also* GUIDO CALABRESI, A COMMON LAW FOR THE AGE OF STATUTES 2 (Lawbook Exch. 1999) (arguing that courts should have the authority to "begin a 'common law' process of renovation" of obsolete laws).

149 From an intuitive perspective, several obvious advantages accrue from employing statutory definitions: legislative control over the creation and alteration of the statute's meaning and scope is preserved, ambiguity (and concomitant issues of due process and fair notice) is (or can be) reduced, and uniformity among courts applying the statute is increased. *Cf.* Nicholas Quinn Rosenkranz, *Federal Rules of Statutory Interpretation*, 115 HARV. L. REV. 2085, 2103–09 (2002) (distinguishing definitional from nondefinitional statutes and discussing several advantages and disadvantages of statutory definitions of terms).

150 *See* Amanda L. Tyler, *Continuity, Coherence, and the Canons*, 99 Nw. U. L. REV. 1389, 1415–18 (2005) (arguing for a strong, but not absolute, theory of statutory stare decisis).

151 *See, e.g.*, Irwin v. Dep't of Veterans Affairs, 498 U.S. 89, 95 (1990).

152 *See supra* notes 13, 29–33, 49–79 and accompanying text.

agencies employing mass communication media such as the Internet to disseminate records, as required in many cases by the FOIA, cannot easily adapt their methods to the balkanized interpretation of a single statutory term. Yet even after three decades, courts have failed to speak in anything close to unison when interpreting this term in the Act.[153]

This, in turn, places needless detrimental pressure on the agencies. If one circuit applies one definition and another circuit applies a different one, agencies cannot chart a safe course when promulgating information through a FOIA-required Web site that can be accessed around the country, from within any circuit. Precisely because the Privacy Act eliminated much of the gray area that originally marked a middle ground between required publication and prohibited disclosure under the FOIA,[154] agencies must now in many cases traverse a tightrope of sorts in setting their information disclosure protocols. Without clear standards to govern their practice, with the possibility of constantly shifting judicial interpretations, agencies cannot plan beyond the short term when establishing their methods of handling information.

2. The Price of Imprecision and the Need for Bright-Line Rules

The very need for clarity, stability, and uniformity, however, gives rise to a second critique of the proposal. If the chief problem is a lack of precision, then why not apply a definition of disclosure that sets a very low, almost trivial threshold under which nearly any government dissemination of records constitutes a disclosure? This would create a bright-line rule—arguably clearer than the "substantial increase in accessibility" test embodied in the amendment proposed here[155]—which would put individuals and agencies on notice while leaving little room for judicial tinkering with disclosure's meaning.

Moreover, not every disclosure thus defined need lead to liability. Courts would still be tasked with determining whether the disclosure was justified, and if it was not, with measuring the actual harm suffered by a plaintiff claiming an improper disclosure.[156] Thus, not only would this alternative provide a bright-line rule, but it would shift the court's analysis, as well as subsequent debate at the agency level, to

---

153 *See supra* Part II.

154 *See supra* notes 27–31 and accompanying text.

155 *See supra* Part III.A.

156 As noted above, even under the current text of the Act, the subsection providing for a civil action requires a showing of "adverse effect," 5 U.S.C. § 552a(g)(1)(D) (2006).

the propriety of a specific disclosure where it belongs, instead of using the existence of a disclosure as a proxy.

This alternative's appeal is ultimately illusory, however, for two reasons. First, the alternative is based on a misconception of the typical posture of a Privacy Act suit alleging a disclosure. Focusing on the harm actually suffered by the plaintiff—as this alternative suggests—makes sense where one is primarily concerned with assessing damages for harm that already has materialized. But damages often are not the central form of relief at issue; injunctive relief often plays a critical role.[157] If the core of the analysis were migrated from assessing whether a disclosure took place to measuring harm in advance, a ruling on an injunction would face the extraordinarily hard task of predicting *ex ante* the harm the plaintiff would suffer.

By contrast, the framework proposed here—while slightly more intricate in application—ultimately makes the court's decision of whether to grant injunctive relief much easier. Under the proposed amendment, the court simply inquires whether the agency's action substantially increased the public accessibility of a record in a way that had any adverse effect upon the plaintiff. If so, unless the disclosure is exempted by one of the statutory exceptions or a routine use, an injunction must issue.

Second, even where damages are the primary relief sought, the difficulty of measuring those damages counsels against a bright-line disclosure definition that shifts the court's analysis to damages. Evaluating the concrete harm inflicted by invasion of one's privacy is hard enough to assess in the private context.[158] In the Privacy Act context, courts are dealing with a statutory cause of action that imposes unfamiliar, artificial parameters. Specifically, in any context where dissemination of sensitive information is the cause of harm, the potential redisclosure of information may pose the greatest risk to individual privacy. In purely private situations, that redisclosure can provide part of the basis for damages.[159] This is not true in Privacy Act cases,

---

157 When the disclosure at issue is ongoing, for example—such as posting a record on an Internet Web site, *see, e.g.*, Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156, 161 (D.D.C. 2006)—the plaintiff's primary interest may be preventing continued access to the record. The importance of injunctive relief is heightened further in light of the Supreme Court's recent decision in *Doe v. Chao*, which held that notwithstanding the Privacy Act's guarantee of a statutory minimum damages award, plaintiffs must show "actual damages" to be entitled to monetary recovery. *See* 540 U.S. 614, 627 (2004).

158 *See* 2 J. Thomas McCarthy, The Rights of Publicity and Privacy § 11:28–29 (2d ed. 2007).

159 *See* 1 Smolla, *supra* note 108, § 4:93. If suit cannot be brought against the entity that

where redisclosure by private parties is not part of the equation. Nothing in the statute reaches third parties' actions, and once information is a matter of public record, third parties can relay it without any fear of private tort liability.[160]

Perhaps because plaintiffs would have no other recovery, or perhaps because of the difficulty of independently tracing specific alleged harms to private and public sources, courts may nonetheless attribute what are in fact harms resulting from third parties' actions to governmental dissemination.[161] At the very least, courts will find the analytical task quite difficult. In the end, if the heart of courts' inquiry is transferred to the measurement of damages that courts cannot accurately or meaningfully assess, the courts' decisions are even less likely to reflect a consistent pattern that furthers the policies that animate the Act.

3. Ignoring the Lessons of the Common Law

This consideration of private tort liability for disclosure of private information provides the basis for a third critique. According to this potential objection, the Privacy Act essentially establishes a federal analogue to the common law tort of invasion of privacy, and therefore the meaning of disclosure and other crucial terms should be derived from that body of law. In other words, despite the differences between private and public acts of disclosure that damage individual privacy, the basic terms and concepts should be the same, and therefore courts interpreting the Privacy Act can simply draw from centuries of precedent. Common law precepts and doctrines could provide courts with a set of familiar tools to assist them in identifying when disclosure occurs.

Although there is nothing wrong in principle with drawing on developed doctrines of private tort law to the extent they are apposite and useful, the reality is that the Privacy Act context is simply too different from the private law universe for the rules that govern the latter to be of great assistance. For example, one might argue that the "single publication rule," well-established in the common law of defa-

---

made the initial disclosure, then a plaintiff can hold those who relayed the information liable. *See id.* However, if the information is no longer "private" but has become well known in the general public, liability for redisclosure is unlikely. *See* 2 *id.* § 10:39 (collecting state law cases holding that the facts must be private to give rise to a cause of action).

160 *See* 2 *id.* § 10:44–48.

161 *See supra* Part II.

mation,[162] could greatly assist federal courts struggling to identify discrete disclosures that trigger the Privacy Act.[163] That rule, which evolved in response to the rise of mass media such as newspapers and radio, provides that any one edition of a print publication, any one broadcast, or any one audible communication counts as a single "publication" giving rise only to a single cause of action, no matter how large the audience.[164] The rule is, as its name suggests, tied not just to a single medium, but to a single publication within that medium. While this rule can thus help courts clarify the parameters of disclosure within a single medium, it provides no guidance in cases where information was first disclosed in one medium (e.g., through an official public record) but was subsequently disseminated in a new medium (e.g., the Internet), a scenario increasingly common in Privacy Act cases.[165]

Moreover, the single publication rule is incompatible with the Privacy Act context at a more fundamental level. The incompatibility stems from the basic difference between private tort law—which governs all private actors and treats each independently of the others—and the type of government disclosures that are the focus of the Act. While the rule may make sense in the private law world, in Privacy Act cases it runs directly counter to the policies that animate the Act. On the one hand, a single publication rule would allow liability to attach whenever a new edition of a given publication is published, even if that new edition results in no greater accessibility than its predecessor.[166] On the other hand, such a rule would not cover wider distribution of the same publication.

Imagine, for instance, that an agency creates an electronic edition of its annual report containing personally identifiable information, but does not make that electronic file available except upon an in-person request made at its headquarters. Under a single publication rule, if

---

162 *See* RESTATEMENT (SECOND) OF TORTS § 577A(3) (1977); 1 SMOLLA, *supra* note 108, § 4:93.

163 At least one circuit has reached this conclusion. *See* Oja v. U.S. Army Corps of Eng'rs, 440 F.3d 1122, 1129–34 (9th Cir. 2006) (applying the single publication rule to Internet disclosure in a Privacy Act suit).

164 1 SMOLLA, *supra* note 108, § 4.93.

165 *See supra* notes 60–68 and accompanying text.

166 For example, if a federal agency annually publishes a report containing personally identifiable information that is sent only to libraries (which dispose of the previous year's edition when the new one arrives), each new annual edition would amount to a new disclosure under the current Privacy Act even though it in no way changed the information's accessibility. From a policy perspective, however, there seems to be no reason that liability should attach to such activity.

the agency then posts this electronic file on its public Web site, no new disclosure would appear to take place, and yet this seems precisely the sort of activity the Act was intended to capture.[167]

The point is not that liability should automatically attach in such a circumstance. Rather, the key is that such acts making records much more easily accessible should be scrutinized by agencies and courts for their consistency with the limits and purposes at the heart of the Act. In sum, as the example of the single publication rule illustrates, there are important differences between the nature of private and public disclosure that make it counterproductive for courts applying the Privacy Act to rely on common law doctrine to define crucial terms such as disclosure.

4. Encouraging Administrative Evasion Through Expansion of Routine Uses

A fourth critique that the proposed amendment may provoke is that the standard of disclosure it imposes is either too restrictive on agency action or too unpredictable in its effect for agencies to forecast effectively what actions will be deemed to constitute disclosures. Accordingly, agencies would face compelling incentives to avoid the disclosure issue altogether by promulgating routine uses to govern all of their information dissemination practices. Thus, it would seem that the proposal does nothing to discourage agencies from improper disclosure; instead, it merely requires them to comply with pro forma procedural requirements when they do so.

This critique runs aground because it misunderstands the purposes that underlie the Privacy Act. The scenario the critique imagines—i.e., where agencies promulgate routine use notices to govern (and exempt from liability) all their regular information dissemination protocols—appears to be *exactly* what the Act's drafters intended.[168] Congress's goal was not to put an end to government disclosures of personal information—as doing so would require a drastic overhaul of the FOIA.[169] Instead, it aimed to make disclosure policy transparent and to subject agencies' disclosures to substantive limits.[170]

---

167 *Cf. Oja*, 440 F.3d at 1131–32 (applying the single publication rule to Internet disclosure as opposed to a multiple publication rule); 1 SMOLLA, *supra* note 108, § 4:93.50 (discussing cases applying the single publication rule to the Internet).

168 *See supra* notes 35–37 and accompanying text.

169 *See* H.R. REP. NO. 93-1416, at 13 (1974), *reprinted in* SOURCE BOOK, *supra* note 28, at 306.

170 *See id*.

Even setting the drafters' objectives aside, the result the critique posits is desirable from a policy standpoint in several respects. First, if all (or nearly all) agency disclosures were swept into the routine use category, then the public would have far more complete information of which records were being disclosed to whom and under what circumstances. Second, if agency disclosure policy is set through formal agency proceedings, the potential for political accountability is significantly greater. Third, the routine use notice exception imposes substantive as well as procedural limits, and therefore provides a workable framework for courts to review agencies' use of this exemption.[171] To this extent, it moves some, though not all, of the analysis and debate to the merits—insofar as the propriety of disclosure must be assessed when the court passes on the validity of a routine use notice—without first requiring courts to engage in complicated prognostications as to a plaintiff's damages. In sum, far from undermining the proposal's desirability, the future envisioned by this fourth critique merely demonstrates that the proposal aligns both with the best realistic hopes of the Act's drafters and with desirable policy outcomes.

5. Upsetting the Balance Between the FOIA and the Privacy Act

A fifth and final critique asserts that the proposal advocated here at best ignores, and at worst threatens to destabilize, the intricate interlocking relationship between the Privacy Act and the FOIA. In rejecting a constructive public knowledge approach, the Third Circuit in *Quinn v. Stone* argued that defining disclosure by reference to previous public accessibility of information would both "short-circuit the delicate balancing courts now engage in between the FOIA and the Privacy Act" and "render superfluous the detailed statutory scheme of twelve exceptions to the prohibition on disclosure."[172] In short, the

---

171 *Cf.* Britt v. Naval Investigative Serv., 886 F.2d 544, 547–48 (3d Cir. 1989) (reviewing whether the agency complied with the routine use notice exception). Certainly judicial review is greatly enhanced where a written, published standard can be challenged as opposed to an ad hoc, unwritten agency policy.

172 Quinn v. Stone, 978 F.2d 126, 134 (3d Cir. 1992). The interaction between the FOIA and the Privacy Act to which the *Quinn* court referred includes both (1) the Privacy Act's provision exempting from its scope disclosures required by the FOIA, *see* 5 U.S.C. § 552a(b)(2) (2006), and (2) the FOIA provision prohibiting disclosures of "personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy," 5 U.S.C. § 552(b)(6); *see* Cochran v. United States, 770 F.2d 949, 955 (11th Cir. 1985) (discussing FOIA Exemption 6); Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156, 167 (D.D.C. 2006) (same). The Supreme Court and lower courts have interpreted the threshold requirement of § 552(b)(6) quite broadly, concluding that virtually any information in a covered record that pertains to a particular individual meets this test. *See* U.S. Dep't of State v. Wash. Post Co., 456

critique argues that in an effort to clarify one small aspect of the Privacy Act, the proposed amendment would disrupt many other carefully calibrated, interdependent provisions.

Although the underlying concern is an important one, the critique overstates that concern here. As to the first point articulated in *Quinn*, the proposal does not at all short-circuit the balancing that takes place between the Privacy Act and the FOIA; rather, it incorporates that balancing into the disclosure analysis. Put differently, the principle highlighted in *Reporters Committee*—distinguishing genuinely public information from technically public but practically obscure information[173]—does not obviate the need to address the issue of how accessible information has become. On the contrary, *Reporters Committee* provides support for drawing the distinction between technically and genuinely public information, and in turn it counsels in favor of defining disclosure to take account of this difference.[174] Moreover, although the *Quinn* court was correct to note that balancing often takes place due to the interplay of FOIA Exemption 6 and § 552a(b)(2) of the Privacy Act, it is not true that every hard case would require that balancing.[175]

As to *Quinn*'s second point, the proposal does nothing to render the Privacy Act's scheme of twelve enumerated exceptions superfluous. Many government efforts to disseminate information still will constitute disclosures. The aim of the proposal is not to overhaul the outcome in a large number of cases, but rather to rationalize and clar-

---

U.S. 595, 602 (1982); *see also* OFFICE OF INFO. & PRIVACY, U.S. DEP'T OF JUSTICE, FREEDOM OF INFORMATION ACT GUIDE 541–44 (2007), *available at* http://www.usdoj.gov/oip/foia_guide07.htm (collecting cases on Exemption 6). When Exemption 6 applies, a court must engage in a detailed balancing inquiry, comparing specific private and public interests, detailed at length in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749, 762–75 (1989) (finding no need to apply Exemption 6 because Exemption 7(C) covered the case). The result—as the court in *Quinn*, 978 F.2d at 134, and other courts, *see, e.g.*, *Cochran*, 770 F.2d at 954–55, have noted—is a tightly interlocking statutory framework that reflects a detailed expression of Congress's efforts to balance public interests in disclosure with individual interests in privacy.

173 *See Reporters Committee*, 489 U.S. at 762–64.

174 *See id.*

175 A specific disclosure would only require the court to engage in the Exemption 6 balancing exercise if the disclosure was exempted from the Privacy Act under § 552a(b)(2), that is, if it was permitted because the FOIA actually required it. As discussed above, however, many disclosures may be premised on the routine use exception. In those cases where an agency engages in a disclosure under the mistaken belief that such disclosure falls within an existing routine use notice, the FOIA exception, § 552a(b)(2), presumably could not provide a fallback basis for permitting disclosure (as the agency would not have needed to promulgate a routine use notice if the information actually was required to be disclosed under the FOIA).

ify the analysis courts must engage in when deciding whether the Act's prohibition applies at all. In sum, the proposed amendment neither destabilizes the FOIA-Privacy Act balance nor renders the carefully crafted statutory exceptions redundant.

Conclusion

John Doe's case against the Department of Labor seems to epitomize the scenarios the Privacy Act was created to address.[176] A federal agency that maintained records about him made those records publicly available.[177] None of the substantive exceptions to the Act's disclosure prohibition applied.[178] In short, had the court been compelled to decide if a violation took place, the outcome seems clear.

Because of the unfortunate gap in the Act's key provision, however, a court faced with a case such as Doe's might never reach the heart of the Privacy Act claim.[179] Instead, it would find itself trapped in a labyrinth of statutory uncertainty about the meaning of disclosure. In other words, the court might see where its analysis should end, but it likely would face great difficulty knowing where to begin.

Hard questions like that in *Doe* about the meaning of disclosure have become all too common in Privacy Act litigation.[180] Lacking guidance from the statute's text, its history, or the administrative regulations, courts tried and failed to fashion a reliable and workable approach to determine whether and when a disclosure has taken place that is also compatible with the Act's text and purposes.[181] The problem lies not in a shortage of judicial ingenuity or creativity, however, but insufficient clarity and coherence from Congress. Only by amending the statute to define disclosure in a way that both comports with the Act's broader purposes and also takes account of the realities of modern agency information-handling practices can the problem be resolved. The amendment proposed here achieves that objective, enabling courts to resolve difficult cases in a principled yet practical manner. More importantly, the proposal provides guidance to agencies and private citizens still struggling to cope with the challenges of adapting government to the digital age.

---

176 Doe v. U.S. Dep't of Labor, 451 F. Supp. 2d 156 (D.D.C. 2006).

177 *Id.* at 161.

178 *See id.* at 171–76.

179 As noted, the court in *Doe* will never reach this question because it granted the parties' request to vacate its 2006 opinion in light of a settlement reached by the parties months after the opinion was issued. *See* Order at 1–2, *Doe*, No. 05 Civ. 2449 (D.D.C. Mar. 22, 2007).

180 *See supra* notes 58–85 and accompanying text.

181 *See supra* Part II.