THE INVASION OF PRIVACY ACT: THE DISCLOSURE OF MY INFORMATION IN YOUR GOVERNMENT FILE

LIEUTENANT COLONEL EVAN M. STONE*

INTRODUCTION

"We are not unaware of the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files. . . . much of which is personal in character and potentially embarrassing or harmful if disclosed."[1]

Identity theft remains one of the greatest threats to personal privacy. One's personally identifiable information is constantly at risk through the use of the Internet. Online social media, purchases, and web searches all potentially expose personal information. Data collection platforms comb disparate public information repositories, compiling online profiles that often contain enough personal data to put a person's identity at risk. Privacy advocates focus their concern on the Internet but the government's vast collection of personal information has been vulnerable for years from the most unlikely source—the Privacy Act itself. Citizen A has the right to access information contained in his government records even if it contains personal information about citizen B. The Privacy Act does not contain an exemption for third party privacy information contained in a Privacy Act protected file. The Privacy Act needs an amendment to include a third party privacy exemption to close this gaping hole that reveals *my* information in *your* government file.

Americans have always treasured their personal privacy.[2] The United States Constitution prohibits the government from intruding into specific areas of

---

* Lieutenant Colonel, United States Army Judge Advocate General's Corps currently assigned as Executive Director, Armed Forces Tax Council, Office of the Secretary of Defense, Washington, D.C. B.A., Political Science, San Diego State University (1986). J.D., University of San Francisco School of Law (1989). LL.M., Military Law, with Administrative Law specialization, The Judge Advocate General's School, Charlottesville, Virginia (2001). LL.M., Taxation, Georgetown University Law Center (2010). Member of the State Bars of California (1989) and Texas (1999). The author wishes to thank Eric Talbot Jensen, Associate Professor of Law, Brigham Young University Law School for his generous time in reviewing and commenting on this article. The views expressed in this article are those of the author and not The Judge Advocate General's Corps, the United States Army, or the Department of Defense.

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

2. Judge Cooley was the first to describe privacy as "the right to be let alone." Samuel D. Warren & Louis D. Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 195 (1890) (citations omitted). Alan F. Westin characterized privacy in the context of government information as "the claim of individuals . . . to determine for themselves when, how, and to what extent information about them is communicated to others." ALAN F. WESTIN, PRIVACY AND FREEDOM 7 (6th prtg. 1970).

privacy.[3] While the authors of the Bill of Rights wanted to protect homes, thoughts and other privacy aspects, they did not provide a constitutional right to privacy *per se*.[4] Moreover, the founders could not have envisioned how rapidly technology would transform society. In *Olmstead v. United States,*[5] Justice Brandeis argued that the Constitution must be applied wider "than the mischief which gave it birth."[6] Justice Brandeis saw how the law must evolve

---

3. *See* U.S. CONST. amend. I ("Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or of the right of the people peaceably to assemble, and to petition the Government for redress of grievances."); U.S. CONST. amend. II ("[T]he right of the people to keep and bear Arms, shall not be infringed."); U.S. CONST. amend. III ("No Soldier shall, in time of peace, be quartered in any house, without the consent of the Owner; nor in time of war, but in a manner to be prescribed by law."); U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated . . . ."); U.S. CONST. amend. V ("No person . . . shall be compelled in any criminal case to be a witness against himself, nor be deprived of life, liberty, or property, without due process of law . . .").

4. *See* U.S. CONST. (not specifically addressing the right to privacy). However, numerous state constitutions were drafted to expressly recognize a right to privacy. *See, e.g.,* ALA. CONST. art. I, § 22 ("The right of the people to privacy is recognized and shall not be infringed."); ARIZ. CONST. art. II, § 8 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law."); CAL. CONST. art. I, § 1 ("All people are by nature free and independent and have inalienable rights. Among these are enjoying and defending life and liberty, acquiring, possessing, and protecting property, and pursuing and obtaining safety, happiness, and privacy."); FLA. CONST. art. I, § 12 ("The right of the people to be secure in their persons, houses, papers and effects against unreasonable searches and seizures and against the unreasonable interception of private communications . . . shall not be violated."); HAW. CONST. art I, § 6 ("The right of the people to privacy is recognized and shall not be infringed . . . ."); ILL. CONST. art. I, § 6 ("The people shall have the right to be secure in their persons, houses, papers and other possessions against . . . invasions of privacy . . ."); LA. CONST. art. I, § 5 ("Every person shall be secure in his person, property, communications, houses, papers, and effects against unreasonable . . . invasions of privacy."); MONT. CONST. art. II, § 10 ("The right of individual privacy is essential to the well-being of a free society and shall not be infringed. . . . "); S.C. CONST. art. I, § 10 ("The right of the people to be secure . . . against unreasonable invasions of privacy shall not be violated . . . ."); WASH. CONST. art. I, § 7 ("No person shall be disturbed in his private affairs, or his home invaded, without authority of law.").

5. 277 U.S. 438, 466 (1928) (holding that government surveillance by wiretapping the defendant's home telephone did not amount to a search or seizure within the meaning of the Fourth Amendment because there was no physical trespass onto the defendant's property), *overruled by* Katz v. United States, 389 U.S. 347, 352–53 (1967) (holding that the Fourth Amendment protects people, not places), *and* Berger v. New York, 388 U.S. 41, 62–64 (1967).

6. *Olmstead*, 277 U.S. at 473 (Brandeis, J., dissenting). *See also*, United States v. Jones, 132 S. Ct. 945, 949 (2012) (holding that the government's attachment of a Global Positioning System (GPS) device to a vehicle to track movement constitutes a search within the meaning of the Fourth Amendment because it is a trespass on an effect).

along with a technologically changing society.[7] The judicial struggle to adapt the law to protect privacy continues without firm resolution.[8]

Courts are not alone in the struggle to define and protect privacy. Congress simply declared a constitutional right to privacy when it passed the Privacy Act of 1974.[9] The Privacy Act, in its broadest terms, regulates how government agencies collect, maintain, use or disclose private information about American citizens.[10] It also contains a provision allowing the citizen to access his government records.[11] The goal of the Privacy Act was to curb

---

7. Justice Brandeis arguably prophesized the information age of the computer and Internet:

> The progress of science in furnishing the Government with means of espionage is not likely to stop with wire-tapping. Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home.

Olmstead, 277 U.S. at 474 (Brandeis, J., dissenting). *See also* Warren & Brandeis, *supra* note 2, at 205, 210–11 (advocating that the law requires change to keep up with advancing technology). *See also* Henke v. U.S. Dep't of Commerce, 83 F. 3d 1453, 1456 (D.C. Cir. 1996) (reasoning that the use of computer programs, for purposes of the Privacy Act, must be used in practice to retrieve information keyed to individuals in order to qualify as a "system of records." A program simply capable of retrieving information keyed to individuals, but not used for that purpose, does not establish a "system of records" in respect to the Privacy Act.).

8. *Compare* Griswold v. Connecticut, 381 U.S. 479, 484 (1965) (holding that a Connecticut statute forbidding the use of contraceptives violates the right of marital privacy and stating "the Bill of Rights have penumbras, formed by the emanations from those guarantees . . . creat[ing] zones of privacy."), *and* Meyer v. Nebraska, 262 U.S. 390, 400 (1923) (alluding to a right to marital privacy in holding that parents have a right to decide their children's education), *and* Lawrence v. Texas, 539 U.S. 558, 578 (2003) (overruling *Bowers v. Hardwick*, 478 U.S. 186 (1986) and upholding sexual privacy between consenting adults in a private setting), *with* Whalen v. Roe, 429 U.S. 589, 600, 603–04 (1977) (rejecting the zone of privacy argument by physicians challenging a New York statute requiring them to report patient information including name, address, and age to the state for certain prescription drugs susceptible of misuse).

9. Privacy Act of 1974, Pub. L. No. 93-579, § 2(A)(4), 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552(a) (2006)) ("Congress finds that . . . [t]he right to privacy is a personal and fundamental right protected by the Constitution of the United States . . . . ").

10. *See* 5 U.S.C. § 552a(b)–(c) (2006).

11. 5 U.S.C. § 552a(d) (2006).

> Each agency that maintains a system of records shall: (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.

Id.

rampant government overreaching in how it collected and used private information about citizens in the dawning computer age. Congress passed the Privacy Act hoping to protect privacy by creating fair government information practices. Instead, in its haste to protect privacy, Congress created a law that ironically fails to protect private information from fellow citizens causing an invasion of privacy.

What should a government agency records custodian do when citizen A requests access to his file under the Privacy Act but the file also contains personal information about citizen B? The access provision of the Privacy Act tells the custodian that he must release the file to citizen A because there is no statutory exemption that permits the government agency to withhold citizen B's information from citizen A. Simply stated, the Privacy Act lacks an exemption permitting the government agency to withhold personal information about another person based solely upon privacy grounds. Government agencies have struggled with this gap in privacy protection. Similarly, courts have tried to solve the problem, but varied judicial decisions have instead created a confusing and contradictory body of case law.

This article shows how a deficiency in the Privacy Act legislation makes one person's personal privacy vulnerable to another person. The mechanics of the Privacy Act show how this invasion of privacy occurs and highlights the need for a third party privacy exemption. The article proposes an exemption that would allow records custodians and courts to properly balance the competing privacy interests using a set of criteria already in use for analyzing privacy balancing in Freedom of Information Act cases.

The article first reviews the historical, legislative and legal context in which Congress created the Privacy Act. The context reveals how and why it lacks a third party privacy exemption. The article next analyzes two significant cases representing opposing judicial interpretations as to whether the Privacy Act requires disclosure of the third party privacy information to an access requester.[12] The article reviews the Department of the Army's Privacy Policy and compares other federal agencies' policies to underscore how pervasive the problem has become when federal agencies attempt to comply with the third party information disclosure aspect of the Privacy Act. Moreover, the article reviews how the case law has evolved into a confusing semantic struggle to solve this complex problem of third party information in a subject requester's file, which has culminated with a significant decision out of the D.C. Circuit

---

12. *Compare* Voelker v. IRS, 646 F.2d 332, 333 (8th Cir. 1981) (holding that a government agency has no discretion to withhold information from a requester's file absent an exemption), *with* DePlanche v. Califano, 549 F. Supp. 685, 698–99 (W.D. Mich. 1982) (holding that a government agency could withhold information from a requester's file if the information is not about the requester).

Court of Appeals addressing an access requesters information in a third party's file.[13] Though the problem is complex, the solution is simple.

The article proposes the solution that Congress create a new exemption allowing agencies and courts to balance the interests between an access requester and the personal privacy interest of a third party. The article concludes by proposing a privacy exemption and analyzing how it would work in practice.

II. HISTORICAL, LEGISLATIVE AND LEGAL CONTEXT OF THE PRIVACY ACT

A. Social Unrest and Congressional Hearings

Many segments of American society distrusted and openly challenged the legitimacy of government in the 1960s and early 1970s.[14] The Watergate scandal revealed an untrustworthy government.[15] Seymour Hersch exposed a massive CIA domestic spying operation against protesters, civil rights activists, and other dissenters.[16] Citizens were justifiably enraged over government

---

13. *See* Sussman v. U.S. Marshals Serv., 494 F.3d 1106, 1121 (D.C. Cir. 2007) (holding that an agency need only grant access under 5 U.S.C. § 552a(d)(1) to a requester's own record, not to all information pertaining to him which is contained in a system of records).

14. *See generally Special Collections and Archives, May 4 Collection: Documenting the May 1970 Kent State Shootings*, KENT ST. U., http://www.library.kent.edu/page/11247 (last visited May 13, 2013) (discussing the tragic end to a student demonstration against the Vietnam War and the National guard when on May 4, 1970, when the rifle fire from twenty-eight Ohio National Guardsmen left four students dead, one permanently paralyzed, and eight others wounded); *The 1965 Watts Riots*, U. OF S. CA., http://www.usc.edu/libraries/archives/la/watts.html (last visited May 13, 2013) (discussing how a routine traffic stop on Aug. 11, 1965 touched off a six day riot leaving 34 dead, over 1,000 injured, nearly 4,000 arrested, and hundreds of buildings destroyed).

15. *See* Alfred E. Lewis, *5 Held in Plot to Bug Democrats' Office Here*, WASH. POST, June 18, 1972, at A01, *available at* http://www.washingtonpost.com/wp-srv/national/longterm/watergate/articles/061872-1.htm (reporting the break-in and attempted bugging of the Democratic Headquarters in Washington, D.C.); *see also* Malcolm Farnsworth, *Deep Throat: Watergate Timeline of Events*, THE TELEGRAPH (Dec. 19, 2008, 7:53 AM), http://www.telegraph.co.uk/news/worldnews/northamerica/usa/3848570/Deep-Throat-Watergate-timeline-of-events.html (discussing the history of the Watergate scandal to include secret tapes, cover up, and President Nixon's ultimate resignation on Aug. 9, 1974).

16. Seymour M. Hersh, *Huge C.I.A. Operations Reported in U.S. Against Antiwar Forces, Other Dissidents in Nixon Years*, N.Y. TIMES, Dec. 22, 1974, at A1 (exposing an illegal CIA domestic spying operation against antiwar protesters and other dissident groups). This prompted three investigations, all of which confirmed the allegations: The president appointed the Rockefeller commission, the Senate formed the Church Committee, and the House formed the Pike commission. LOCH K. JOHNSON, AMERICA'S SECRET POWER: THE CIA IN A DEMOCRATIC SOCIETY 207–10 (1989). *See also* STEVEN EMERSON, SECRET WARRIORS: INSIDE THE COVERT MILITARY OPERATIONS OF THE REAGAN ERA 33 (1988) ("[I]t seemed that virtually every day Church's hearings brought out new and shocking intelligence abuses, ranging from mail openings to massive investigations of American 'subversives' to secret computer dossiers on 1.5 million citizens. CIA director Richard Helms was even convicted of lying to Congress . . . .").

agencies keeping secret files on Americans who were exercising their freedom.[17] The social turbulence gripping America during this historical period set the stage for The Privacy Act of 1974.

In the midst of this social turmoil, the House of Representatives considered creating a massive centralized federal computer data bank called FEDNET.[18] Some representatives raised the concern that the government's files on citizens would invade their privacy. Moreover, a computer expert cautioned: "We would do well to concentrate on the more constructive and larger issue of: How shall we control the development of the automation of all sensitive information files in order to best protect the rights of the individual and avoid a '1984' nation?"[19]

To address these burgeoning concerns, the United States Department of Health, Education & Welfare (HEW) produced a significant report about computers and privacy in 1973.[20] The report focused on the issue of personal information contained inside the growing government automated data systems. The HEW committee recommended legislation establishing a code of fair information practice for all automated personal data systems.[21] The committee also promulgated what it considered principles of fair information practice. These principles can be summarized as:

> (1) No personal-data record-keeping systems whose very existence is secret.
> (2) An individual must have access to records about him and how they are used.
> (3) Individuals must be able to prevent information collected for one purpose to be used for another purpose.
> (4) Individuals must be able to correct or amend their records.
> (5) Organizations must take reasonable precautions to prevent misuse.[22]

While the HEW reports only focused on HEW information practice, the report drew significant attention in Congress.

Soon after the release of the HEW report, Congress began conducting its own hearings into regulating government information practices.[23] The Senate

---

17. *See* Berlin Democratic Club v. Rumsfeld, 410 F. Supp. 144, 147 (D.C. Cir. 1976) (alleging numerous acts of privacy invasion by U.S. Army Intelligence).

18. *The Computer and the Invasion of Privacy: Hearings Before a Subcomm. of the Comm. on Gov't Operations*, 89th Cong. 1-2 (1966) [hereinafter *Hearings*].

19. *Hearings*, *supra* note 18 at 119–21 (statement of Paul Baran, Computer Expert with the Rand Corp., Santa Monica, California).

20. U.S. DEP'T OF HEALTH, EDUC. & WELFARE, RECORDS, COMPUTERS AND THE RIGHTS OF CITIZENS, at viii-xi (1973) [hereafter HEW REPORT].

21. *Id.* at xxiii.

22. *Id.* at 41–42.

Committee on Government Operations summarized examples of what it considered intrusive information practices.[24] The Committee specifically noted that the United States Army committed egregious clandestine information practices such as maintaining unlawful computer databases, conducting unlawful surveillance, and publishing blacklists.[25]

---

23. *E.g.,* COMM. ON GOV'T OPERATIONS, 94TH CONG., 2D SESS., LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY (1976) [hereinafter SOURCE BOOK], *available at* http://www.loc.gov/rr/frd/Military_Law/pdf/LH_privacy_act-1974.pdf.

24. *Special Inquiry on Invasion of Privacy: Hearings Before a Subcomm. of the Comm. on Gov't Operations*, 89th Cong. 112-23 (1965) (examining government questionnaires and tests questions that asked intrusive questions such as: How did your first marriage end? Am I troubled by constipation? Do I go to church every week? Do I believe in the second coming of Christ? Are many of my dreams about sex matters?).

25. Senator Ervin summarized the findings of the Hearings Before the Subcommittee on Constitutional Rights of the Judiciary Committee:

> Despite First Amendment rights of Americans, and despite the constitutional division of power between the federal and state governments, despite laws and decisions defining the legal role and duties of the Army, the Army was given the power to create an information system of data banks and computer programs which threatened to erode these restrictions on governmental power.
>
> Allegedly for the purpose of predicting and preventing civil disturbances which might develop beyond the control of state and local officials, Army agents were sent throughout the country to keep surveillance over the way the civilian population expressed their sentiments about government policies. In churches, on campuses, in classrooms, in public meetings, they took notes, taperecorded, and photographed people who dissented in thought, word or deed. This included clergymen, editors, public officials, and anyone who sympathized with the dissenters.
>
> With very few, if any, directives to guide their activities, they monitored the membership and policies of peaceful organizations who were concerned with the war in Southeast Asia, the draft, racial and labor problems, and community welfare. Out of this surveillance the Army created blacklists of organizations and personalities, which were circulated to many federal, state and local agencies, who were all requested to supplement the data provided. Not only descriptions of the contents of speeches and political comments were included, but irrelevant entries about personal finances, such as the fact that a militant leader's credit card was withdrawn. In some cases, a psychiatric diagnosis taken from Army or other medical records was included.
>
> This information on individuals was programmed into at least four computers according to their political beliefs, or their memberships, or their geographic residence.
>
> The Army did not just collect and share this information. Analysts were assigned the task of evaluating and labeling these people on the basis of reports on their attitudes, remarks, and activities. They were then coded for entry into computer or microfilm data banks.

Congress had been investigating privacy issues, abusive government practices and computers since 1966.[26] The confluence of expansive government information practices and computers alarmed Congress. The Senate wanted fair information practices that respected citizens' privacy and ending what it considered illegal information gathering.[27] Similarly, the House of Representatives wanted to stop the federal government's misuse of information and restore what it called the "constitutional right to privacy."[28] The time was ripe for passage of information privacy legislation.

B. Congress Rushed the Privacy Act into Law

Congress perceived an urgent need for privacy legislation.[29] Both Houses had already passed their own privacy bills on November 21, 1974, but the 93rd Congress was nearing the end of its session.[30] Recognizing the need for some privacy legislation, Congress did not follow the usual legislative process;[31] rather, staff members from both chambers met and hastily drafted a compromise privacy bill known as the "compromise amendment."[32] The staffs presented this amendment to the members of the Senate and House Committees on Government Operations who informally agreed upon it.[33]

S. REP. NO. 93-1183, at 6929 (1974), *reprinted in* SOURCE BOOK, *supra* note 23, at 167. The Army had been spying on citizens as early as World War I. *See* JOSEPH W. BENDERSKY, THE "JEWISH THREAT:" ANTI-SEMITIC POLITICS OF THE U.S. ARMY (2000). "MI4 [Military Influence Section of the Army's Military Intelligence Division] developed surveillance and secret file systems on American citizens and groups that rivaled those of police states." *Id.* at 50.

26. *Hearings*, *supra* note 18, at 1–2 (statement of Hon. Cornelius E. Gallagher, Chairman, Spec. Subcomm.).

27. S. REP. NO. 93-1183 at 6916–17 (1974), *reprinted in* SOURCE BOOK, *supra* note 23, at 154–55 (expressing the Senate's purposes of its privacy bill as: respecting privacy, accountability, responsibility, oversight, open government, prevention of illegal and secret information gathering).

28. SOURCE BOOK, *supra* note 23, at 295–97 (expressing similar concerns as those expressed by the Senate).

29. Zeller v. United States, 467 F. Supp. 487, 498 (E.D.N.Y. 1979) ("All those involved in the legislative process including the Administration, agreed on the need for enactment of some sort of privacy legislation before the congressional recess.") (citations omitted).

30. *Id.* at 498 n.14.

31. *Id.* at 498 ("In order to accelerate the legislative process, the usual procedure of submitting conflicting bills to a conference committee was omitted . . . .") (footnote omitted).

32. *Id.*

33. *Id.* at 498 n.14.

This compromise amendment passed both houses on December 31, 1974 as the Privacy Act.[34] The President signed the Privacy Act into law on January 1, 1975, becoming effective September 27, 1975.[35]

The clear target of the Privacy Act was federal government agencies. The Privacy Act empowered the citizen with the right of access to his federal government agency file along with a civil remedy to enforce that right.[36] The Privacy Act also required an agency to publicly announce its record systems that were meant to store information about citizens.[37] Further, the government agency could only maintain relevant and necessary information.[38] Most importantly, the Privacy Act restricted the government agency from disclosing information to third parties without consent or specific exceptions.[39]

In its rush to enact the Privacy Act, Congress did not reconcile the inherent conflict between an individual's access right and another individual's privacy interest contained in an access requestor's file. In exercising one's access right, it was possible to peer into another's privacy because another person's privacy interest was not among the permissible exemptions to deny information to an access requester. Congress failed to consider the intersection of these competing issues. The legislative history is silent as well. The silence in the

---

> Because of the limited amount of time available between the time of reconvening the Congress after the [Thanksgiving] recess and the end of the session of Congress, members of the Government Operations Committee[s] of the Senate and the House agreed that they would have the different version studied by their respective staffs during the recess.
>
> After the recess the members of the staffs who had made this study reported to the members of the two committees, and after that the members of the two committees met informally and agreed on the amendments [for the compromise bill, S. 3418].

Id. (quoting 120 CONG. REC. 40400 (Dec. 17, 1974)(statement of Sen. Irvin)).

34. Privacy Act of 1974, Pub. L. No. 93-579, § 2(A)(4), 88 Stat. 1896 (codified as amended at 5 U.S.C. § 552(a) (2006)).

35. SOURCE BOOK, *supra* note 23, at 1001–02.

36. 5 U.S.C. § 552a(d)(1) (2006) ("Each agency that maintains a system of records shall upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him . . . to review the record and have a copy made of all or any portion thereof . . . ."); § 552a(g)(1) ("Whenever any agency . . . refuses to comply with an individual request under subsection (d)(1) of this section . . . the individual may bring a civil action against the agency . . . .").

37. § 552a(e)(4) ("Each agency that maintains a system of records shall . . . publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records . . . .").

38. § 552a(e)(1) ("Each agency that maintains a system of records shall maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency . . . .").

39. § 552a(b) ("No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to . . . the prior written consent of, the individual to whom the record pertains . . . .").

legislative history and in the statute itself suggests that Congress simply overlooked the access-privacy conflict because it was focused on reigning in government. The accelerated legislative process, in skipping the usual conference committee, shortchanged the public because Congress should have addressed this issue. Instead, the Privacy Act has a gap—a gap that allows disclosure of *my* personal information contained in *your* government record.

The legislative silence regarding third party privacy causes problems for courts trying to navigate this gap. Without legislative guidance, courts struggle to reconcile the Privacy Act's access provision with the actual protection of citizens' privacy. Often, courts must torture the meaning of statutory definitions to reach a desired outcome. The judicial straining has created a body of confusing and inconsistent case law making it difficult, if not impossible, for agencies to know the proper course of action regarding a Privacy Act access request.[40] Moreover, the pre-existing Freedom of Information Act (FOIA) often further confuses the privacy issue. One must firmly understand how FOIA deals with privacy before considering the Privacy Act gap.

C. The Freedom of Information Act (FOIA)[41]

The FOIA, a statute passed nine years before the Privacy Act, adds to the confusion surrounding the Privacy Act because it requires government agencies to make information available to the public—a seemingly contradictory purpose compared to the Privacy Act.[42]

The FOIA boldly required federal government agencies to release agency records to the public.[43] How does government purport to simultaneously release information and protect privacy? The FOIA protects privacy interests

---

40. *See infra* Part II.A–B.

41. Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250 (1966) (codified as amended at 5 U.S.C. § 552 (2012)).

42. President Lyndon B. Johnson articulated the spirit of the FOIA in his bill-signing statement: "[A] democracy works best when the people have all the information that the security of the Nation permits. . . . [T]he United States is an open society in which the people's right to know is cherished and guarded." SUBCOMM. ON ADMIN. PRACTICE & PROCEDURES OF THE COMM. ON THE JUDICIARY, 93D CONG., 1ST SESS., FREEDOM OF INFORMATION ACT SOURCE BOOK: LEGISLATIVE MATERIALS, CASES, ARTICLES, at 1 (1975) [hereinafter FOIA SOURCE BOOK], *available at* http://www.llsdc.org/attachments/files/184/FOIA-LH.pdf.

43. 5 U.S.C. § 552(a) (2006) (providing that each agency make information available to the public by publishing in the Federal Register, public inspection, or on proper request). This was a bold step because prior to 1966, the government was under no obligation to reveal information to the public. *See* HON. HOLIFIELD, ADMINISTRATION OF THE FREEDOM OF INFORMATION ACT, H.R. REP. NO. 92-1419, at 2 (1972), *reprinted in* FOIA SOURCE BOOK, *supra* note 42, at 8–9 (1975) (explaining that even though the Moss Bill (H.R. 2767) of 1958 withdrew authority for the government to withhold information from the public, some agencies still relied on the 1789 "Housekeeping" law as authority to withhold information).

through exemptions. Congress protected privacy interests within the FOIA by allowing government agencies to withhold personal information that would constitute an unwarranted invasion of privacy.[44]

It is important to understand the distinction between the two statutory protections of privacy: FOIA privacy exemptions can protect privacy "interests" existing within the entire field of agency records, whereas the Privacy Act, as explained below, protects only a small subset of agency records maintained in a "system of records."[45] During the nine years between passage of the FOIA and the passage of the Privacy Act, the FOIA privacy exemptions were the only privacy protection people could rely upon.[46] The 1973 HEW report criticized the FOIA's privacy exemption as a feeble protection of privacy interests because an agency had broad discretion to nonetheless release exempted information.[47]

The FOIA Exemptions 6 and 7(C) govern the protection of privacy interests and remain statutorily unchanged today,[48] but do have a better analytical guide to assess potential release of personal information after the United States Supreme Court decided *U.S. Department of Justice v. Reporters Committee for the Freedom of the Press.*[49] In *Reporters Committee*, the Supreme Court decided the issue of whether disclosure of "rap" sheets containing certain personal information such as date of birth, physical appearance and the history of arrests, charges, convictions and incarcerations could reasonably be expected to constitute an unwarranted invasion of personal privacy within the meaning the FOIA exemption 7(C).[50] Exemption 7(C) exempts records compiled for law enforcement purposes. Contrast Exemption 7(C) with Exemption 6, which exempts personnel, medical files and similar files if the disclosure would constitute a clearly unwarranted invasion of privacy.[51]

In *Reporters Committee,* a news correspondent and an association of journalists requested criminal information ("rap sheets") pertaining to four members of the Medico family, whose family's company had been associated

---

44. 5 U.S.C. § 552(b)(6) ("This section [552(a)] does not apply to matters that are . . . personnel and medical files and similar files the disclosure of which would constitute a clearly unwarranted invasion of personal privacy . . ."); §§ 552(b)(7)(C) ("This section [552(a)] does not apply to matters that are . . . records or information compiled for law enforcement purposes, but only to the extent that the production of such law enforcement records or information . . . could reasonably be expected to constitute an unwarranted invasion of personal privacy . . . .").

45. 5 U.S.C. § 552a(a)(5) (2006).

46. *See* FOIA SOURCE BOOK, *supra* note 42, at 12 (revealing that in its initial iteration, FOIA exempted privacy under section 552(b)(6) only).

47. HEW REPORT, *supra* note 20, at 64–66. *See also* Ralph Nader, *Freedom From Information: The Act and the Agencies,* 5 HARV. C.R.-C.L. L. REV. 1, 1-5 (1970) (criticizing the FOIA and its implementation).

48. *Compare* 5 U.S.C. §§ 552(b)(6) (1970), *and* 552(b)(7)(c) (Supp IV. 1975), *with* 5 U.S.C. §§ 552(b)(6) (2006), *and* 552(b)(7)(C) (2006).

49. 489 U.S. 749 (1989).

50. *Id.* at 751–53.

51. § 552(b)(6) (2006).

with organized crime.[52] The FBI provided information pertaining to three of the members who had died, but withheld the rap sheet on the fourth member.[53] The District Court upheld the agency's withholding based on both Exemption 6 and Exemption 7(C), but the court of appeals reversed stating, "an individual's privacy interest in criminal-history information that is a matter of public record [is] minimal at best,"[54] and held that Exemptions 6 and 7(C) did not apply.[55]

The Supreme Court's analysis focused on (1) defining the privacy interest behind the exemptions and (2) defining when an invasion of that interest would be warranted. The court provided, "whether disclosure of a private document . . . is warranted must turn on the nature of the requested document and its relationship 'to the basic purpose of the Freedom of Information Act to open agency action to the light of public scrutiny.'"[56] It found that the "rap sheet" of personal criminal information about the Medico family member was of the type of information that exemption was supposed to protect and disclosure of that information did not shed light on how the government agency works.[57] Thus, the test balances the relative merit of a qualifying public interest in disclosure and a personal privacy interest.[58]

The FOIA applies a "release unless exempted" presumption to the entire field of government agency records. Individual privacy interests are only protected insofar as Exemptions 6 or 7(C) apply using the *Reporters Committee* analysis.[59] The Privacy Act access provision[60] works similarly to the FOIA with respect to subject requesters and the information in their own files. In other words, the Privacy Act applies a "release to the subject requester unless exempted" standard to the subset of agency records maintained in a "system of records." While the FOIA has exemptions for privacy interests, the Privacy Act does not when it comes to an access requester. Because the Privacy Act access provisions work like a mini-FOIA (release unless exempted) as it pertains to the subject requester, the FOIA privacy exemptions and analysis could serve as the model for a third party privacy exemption to the Privacy Act access provision.

A third party privacy exemption for Privacy Act would presume disclosure unless exempted to the access requester according to the plain meaning of the statute.[61] Using the *Reporters Committee* analysis, the records custodian could

52. *Reporters Comm. for Freedom of the Press,* 489 U.S., at 757.
53. *Id.*
54. *Id.* at 758–59.
55. *Id.* at 759.
56. *Id.* at 772 (quoting Dep't of Air Force v. Rose, 425 U.S. 352, 372 (1976)).
57. *Id.* at 773.
58. *Reporters Comm. for Freedom of the Press*, 489 U.S. at 772.
59. *See id.*
60. 5 U.S.C. § 552a(d)(1) (2006).
61. *Id.*, stating:

exempt the third party information if the disclosure would be an unwarranted invasion. Accordingly, a records custodian would look to the record's relationship to a core purpose of the Privacy Act access Provision. The core purposes of the access rule are contained in the Senate and House reports pertaining to their respective original bills.[62] The core purposes of access can be distilled into these:

> (1) Protecting the access requester from invasion of privacy by letting him into his own file to see if information was improperly disclosed;
> (2) Discovering the existence of a government record;
> (3) Insuring accuracy of the information in a government record;
> (4) Mutuality;
> (5) Disarming hostility;
> (6) Insuring accuracy, relevance, timeliness, and completeness as related to making decisions about records/people;
> (7) Ensuring fair treatment.[63]

Distinguishing the FOIA privacy interests and applying its analysis to form the basis of a third party privacy exemption to the Privacy Act access provision is the solution, but the starting point to illustrate the problem lies with the Privacy Act itself.

> Each agency that maintains a system of records shall: (1) upon request by any individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him and upon his request, a person of his own choosing to accompany him, to review the record and have a copy made of all or any portion thereof in a form comprehensible to him, except that the agency may require the individual to furnish a written statement authorizing discussion of that individual's record in the accompanying person's presence.

62. SOURCE BOOK, s*upra* note 23, at 173 (revealing the Senate's access purpose of full protection against abuse of power, which requires the individual to have a right to discover if he is subject of a government file, and if so, to access in order to ensure accuracy and whether there has been improper disclosures.) It is a "desirable adjunct" to insure accuracy, and "objections [to access] are inconsistent with the principle of mutuality necessary for fair information practice." *Id.* [A]ccess "disarm[s] this hostility" and "guarantee[s] the accuracy" through "individual self interest." *Id.* at 174. *See also id.* at 308:

> The Committee believes that this [access] provision is essential to achiev[ing] important objective[s] of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. . . . [and] maintaining . . . accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them. The constant vigilance of individual citizens backed by legal redress is the best means, in the Committee's opinion, of making certain that government treats people fairly.

63. *See id.*

D. The Privacy Act: How It Really Works

The Trigger: What Does the Privacy Act Protect? And When?

A request for an agency record triggers the FOIA, but if the record is maintained in a "system of records," the Privacy Act is triggered first. A "system of records" is "a group of any *records* under the control of any agency from which information is *retrieved by* the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the *individual*."[64] Examples of federal agency systems of records include: income tax records, military health records, household census records, social security records, and postal address records. These systems of records file information by individuals' names (or identifying equivalent) and contain personal information like home addresses, gender, social security number, birth date, height and weight, medical conditions, individual financial information, criminal conduct and much more.

While the Privacy Act and FOIA use the same definition of agency,[65] the Privacy Act's definition of "record" is key to both defining a "system of records" and to understanding the problem raised in this article. The Privacy Act defines record as:

> [A]ny item, collection, or grouping of information *about an individual* that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph. [66]

---

64. § 552a(a)(5) (emphasis added).

65. § 552a(a)(1) (stating "the term 'agency' means agency as defined in section 552(e) of this title . . . ."). *But cf.* Alexander v. FBI, 971 F. Supp. 603, 606–07 (D.D.C. 1997) (rejecting the interpretation that the FOIA definition of agency excludes the President's immediate staff and advisor, and applies the Privacy Act because of the differing purposes).

66. § 552a(a)(4) (emphasis added). *Cf.* SOURCE BOOK, *supra* note 23, at 1025–26 (OMB guidelines broadly interpret the statutory definition but still require it to be about an individual). The OMB guidelines amplify the statute by defining a record as, "any item of information about an individual that includes an individual identifier." *Id.* at 1026. The OMB definition further provides, "[a] record includes any groupings of such items of information . . . [which] do[ ] not distinguish between data and information . . . [and] includes individual identifiers in any form including, but not limited to finger prints, voice prints, and photographs." *Id.* Moreover, the OBM guideline provide, "the phrase 'identifying particular' suggests any element of data . . . or other descriptor . . . which can be used to identify an individual." *Id. But see* Zeller v. United States, 467 F. Supp. 487, 497 (E.D.N.Y. 1979) (noting that OMB's guidelines do not bind courts).

As explained *infra, II.D.*, some courts restrictively use the definition of "record" to exclude information from Privacy Act protection. If the court does not want a requester to have access, it simply rules the information is not "about" the requester. Other courts broadly use the definition of record to include information under the Privacy Act protections. If a court wants the requester to have the information, then the record is characterized as "about" the requester.

The definition of "individual" also illustrates the Privacy Act's restrictive nature. While a record under the Privacy Act can include as little as one item, it must be about an individual. The Privacy Act defines an individual as "a citizen of the United States or an alien lawfully admitted for permanent residence."[67] Under FOIA any "person"[68] can request information because it is a release statute. Under the Privacy Act, the goal is to give the "citizen" access to his own record and to protect that record from third party disclosure. Therefore, the Privacy Act only protects records about citizens or permanent resident aliens.

Any request for information contained in a government agency "system of records" triggers either an access right or a disclosure protection under the Privacy Act.[69] If the requesting person is the individual subject of the record, then the "access rule" applies.[70] Under the access rule, the information must be released unless an exemption exists that would permit the government to deny a person access to his own record.[71] If the requesting person is not the subject of the record, then the "no-disclosure" rule applies.[72] In that case, the information will not be released unless the subject consents or there is an exception. Whether the request invokes FOIA, the Privacy Act, or both, one must always apply the Privacy Act analysis first if the record is maintained in a "system of records." However, both statutes must be analyzed.[73]

---

67. § 552a(a)(2).

68. 5 U.S.C. § 551(2) (2006) (where "person" is defined to include an individual, partnership, corporation, association, or public or private organization other than an agency).

69. § 552a(b), (d). *But see* Albright v. United States, 631 F.2d 915, 918–19 (D.C. Cir. 1980) (holding that records describing how an individual exercises his First Amendment rights can violate the Privacy Act even if the information is not yet in a system of records).

70. *See* Freedom of Information Act, Pub. L. No. 89-487, 80 Stat. 250, 250 (1966) (codified as amended at 5 U.S.C. § 552 (2006)).

71. *Id.* at 250–51.

72. *See* FOIA SOURCE BOOK, *supra* note 42, at 11.

73. U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974, at 92 (2010), *available at* http://www.justice.gov/opcl/1974privacyact.pdf (indicating that an individual's request for his own record should be processed under the Privacy Act and the FOIA regardless of which is cited); *see also* § 552a(t)(1)—(2):

> (1) No agency shall rely on any exemption contained in section 552 of this title to withhold from an individual any record which is otherwise accessible to such individual under the provisions of this section. (2) No agency shall rely on any exemption in this section to withhold from an individual any record which is

E. The Right of Access and its Exemptions

The right of access is a major function of the Privacy Act. The statute provides:

> Each agency that maintains a system of records shall (1) upon request by any *individual* to gain access to *his record* or to *any information pertaining to him* contained in the system, permit him . . . to review the record and have a copy made of all or any portion thereof . . .[74]

The right of access empowers the citizen to enforce the Privacy Act. The citizen is entitled to see what information the government maintains about him. Further, this right is backed up by a legal cause of action to challenge government agency denials of access unless the information is properly exempted.[75] The government can only deny an individual access to his record if an exemption exists. The exemptions are categorized by one special exemption, two general exemptions, and seven specific exemptions.[76]

The Privacy Act, unlike the FOIA, does not contain an independent exemption to protect another person's privacy interest. Neither the original bills nor the compromise bill ever addressed the issue. The bill passed by the Senate only exempted national security information and law enforcement information.[77] The Senate, in its report and debates, favored disclosure to the citizen claiming access.[78] The final bill passed by the House included the

---

> otherwise accessible to such individual under the provisions of section 552 of this title.

74. § 552a(d)(1) (emphasis added).

75. § 552a(g)(1)(B) (stating "[w]henever any agency . . . refuses to comply with an individual request under subsection (d)(1) of this section . . . the individual may bring a civil action against the agency. . . ."); *see also* Cummings v. Dep't of the Navy, 279 F.3d 1051, 1058 (D.C. Cir. 2002) (holding that a former Navy fighter pilot was not barred by the *Feres* Doctrine from bringing a civil action for damages under the Privacy Act).

76. § 552a(d)(5) (specially exempting information reasonably compiled for civil litigation); § 552a(j)(1)–(2) (generally exempting information maintained by the CIA or an agency whose principal function pertains to law enforcement); § 552a(k)(1)–(7) (specifically exempting seven categories of information: classified information, investigatory material compiled for a law enforcement purpose to the extent release would violate an express promise of confidentiality to a source, secret service information, statistical information, investigatory materials compiled for federal employment to the extent release would violate an express promise of confidentiality to a source, materials related to appointment or promotion in the federal service, and armed forces promotion evaluation material to the extent release would violate an express promise of confidentiality to a source).

77. SOURCE BOOK, *supra* note 23, at 325–26.

78. *Id.* at 239–52, 753. The Senate was clearly concerned with government overreaching and allowing the citizen maximum notice and access to his own government files.

current exemptions.[79] The House of Representatives likewise favored disclosure to the citizen claiming access.[80] The compromise amendment adopted the House version of the exemptions. Even though the Privacy Act ultimately included ten exemptions to access,[81] Congress did not want to undermine the access rights. In fact, the confidential source exemptions were even discouraged.[82]

Congress did not express any intent regarding a third party privacy exemption; moreover, the momentum favored full disclosure to the access requester. Consequently, there is no exemption for third party privacy in the Privacy Act. Even in a rush, Congress should have considered the issue of a third party privacy exemption.[83] The 1973 HEW Report, upon which

---

There was absolutely no discussion of exemptions beyond law enforcement and national security. Absent an exemption, the citizen should get everything. There was virtually no interpretive discussion of these two general exemptions. The only comment made was that the national defense exemption was not a blanket exemption. The agency in question has the burden of establishing how a system of records would damage national defense before it could exempt the system. The Senate accepted that a government needs its secrets, but beyond that, the government should disclose to the individual. *See id.*

79. SOURCE BOOK, *supra* note 23, at 983.

80. *Id.* at 311–12. The House Report indicates:

> We believe that the government should maintain no secret system of records about its own citizens. We have also made sure that systems may be exempted from certain requirements of the bill only after the head of an agency promulgates rules which are open to public comment . . . . [and] [s]ound reasons of public policy justify exempting . . . records from individual access.

Id.; *see also id.* at 329 (Representative Bella Abzug with concurrence of several others wrote a separate interpretive dissent arguing that the exemptions were too many: "We start with the premise that exemptions . . . are justified only in the face of overwhelming societal interest . . . . Moreover, when exemptions must be made, they must be defined in very specific terms.").

81. § 552a(j)–(k).

82. SOURCE BOOK, *supra* note 23, at 860.

> [I]t is important to note that the House provision would require that all future promises of confidentiality . . . be expressed and not implied promises. . . . [I]t is expected that the Office of Management and Budget will work closer with agencies to insure that Federal investigators make sparing use of the ability to make express promises of confidentiality.

Id.

83. The special exemption for civil litigation appeared as an amendment just before final passage. If this important exemption did not even surface until the House debate, the subtler issue of third party privacy was clearly overlooked. *See* SOURCE BOOK, *supra* note 23, at 249–51, 329–30.

Congress relied, even raised the issue.[84] However, the lack of time and the clamoring public worked against the Privacy Act. Congress simply ran out of time.[85]

F. Prohibition on disclosing to third parties

The other major provision of the Privacy Act protects records from disclosure to third parties absent the individual's consent. The statute provides: "No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual *to whom the record pertains* . . . ."[86]

The "no-disclosure rule" does not apply to a subject requesting access to his own record; it only applies when other people are requesting access to his Privacy Act protected record.[87] It is irrelevant to an access analysis. Nonetheless, some agencies have unsuccessfully argued that the no-disclosure rule and its underlying policy apply to access analyses, essentially operating as a *de facto* exemption.[88] While an appealing argument, the "no-disclosure rule" is not an exemption to the right of access by the subject.

G. The Privacy Act Unwittingly Allows an Invasion of Privacy

The Privacy Act has an ironic gap. While it helped end abusive government agency information practices[89] and made the government more accountable,

---

84. *See* HEW REPORT, *supra* note 20, at 59–61 (noting situations where the privacy of collateral individuals would warrant non-disclosure to the data subject, but that this should not be done unless there is a strong societal need for a specific exemption).

85. *See* Zeller v. United States, 467 F. Supp. 487, 498 (E.D.N.Y. 1979). The Senate and the House passed their respective bills toward the end of November 1974. *Id.* In the waning days of the 93rd Congress, the compromise amendment became the Privacy Act having never made it to a conference committee. *Id.*

86. 5 U.S.C. § 552a(b) (2006) (emphasis added).

87. *Id.*

88. *See* Voelker v. IRS, 646 F.2d 332, 333 (8th Cir. 1981) (arguing that the IRS could not disclose information to an access requester because it would violate the no-disclosure rule of section (b)); *see also* Henke v. U.S. Dep't of Commerce, No. 94-0189, 1996 WL 692020, at *3 (D.D.C. Aug. 19, 1994) (arguing that the Dep't of Commerce could not disclose information to an access requester because section (b) operated as an exemption), *vacated,* 83 F.3d 1453, 1462 (D.C. Cir. 1996) (holding that the information was not even contained in a system of records).

89. Other Legislative and Executive action also curbed government intrusion. *See, e.g.*, STEPHEN DYCUS ET AL., NATIONAL SECURITY LAW 427–47 (Richard A. Epstein et al. eds., 2d ed. 1997) (discussing Executive Orders 11,905, 12,036, and 12,333, which placed new restrictions and oversight on intelligence collection of U.S. persons; and discussing the Hughes Ryan Act of 1974 which imposed restrictions on CIA covert operations). *But see* USA Patriot Act of 2001,

the Privacy Act allows—and may even require—and an invasion of privacy. When an individual requests access to his own agency record, the agency cannot withhold another person's private information contained in the requester's file because the access provision lacks an exemption. This gap in coverage enables an individual to access the privacy information of another. The Privacy Act did restore equilibrium between the citizen and the federal government. It is now time to re-examine the issue in terms of reconciling privacy interests between citizens.

The Privacy Act itself and its legislative history are completely silent on the issue of third party privacy. Consequently, courts navigate this gap by using semantics to reach and justify a desired result. The current judicial approach to the issue reveals how courts arrive at opposite conclusions using the same statute.

II. THE CURRENT JUDICIAL APPROACH TO THIRD PARTY INFORMATION

A. Voelker v. IRS[90]

The *Voelker* case illustrates how a district court and its appellate court handled the third party privacy gap, each following what it thought to be the spirit of the Privacy Act. *Voelker* established an approach favoring disclosure to the access requester. Paul Voelker, an Internal Revenue Service (IRS) attorney, requested access to information "relative to an investigation initiated on [him] on or around March 26, 1974."[91] The government disclosed most of the information, except for certain portions of a collateral report that contained third party information.[92] The court never divulged the exact nature of this third party information in its opinion. The district court ruled in favor of the IRS, stating that it may withhold the third party information.[93] The Court of Appeals for the Eighth Circuit reversed, holding that the government must disclose all information, absent a specific exemption, to a citizen entitled to access rights.[94] The circuit court relied on the plain meaning of the statute.[95]

The *Voelker* case illustrates the third party information gap problem. The government agency tried to protect the third party information by claiming that it did not pertain to Voelker, though physically in his file.[96] The government argued that because it did not pertain to Voelker, the no-disclosure rule prevented release without consent or exception. The

---

Pub. L. No. 107-56, 115 Stat. 272, 278–96 (authorizing broader discretion in government information collection in response to the terrorist attacks of September 11, 2001).

90. 646 F.2d 332 (8th Cir. 1981).

91. *Id.* at 333.

92. *Id.*

93. *Id.*

94. *Id.* at 335.

95. *Id.* at 333–34.

96. *Voelker*, 646 F.2d at 333.

government knew that the access rule allowed Voelker into his records, but the rule lacked an exemption to withhold the third party information located within.[97] The district court adopted the government's creative use of the no-disclosure rule as a functional equivalent of a third party privacy exemption.[98] The court of appeals, however, rejected it.[99]

The Court of Appeal for the Eight Circuit wrote, "[W]e hold that a federal agency does not have discretion to withhold information contained in a requesting individual's record on the ground that the information does not pertain to that individual."[100] This holding clearly shows how the Privacy Act's gap can lead to an invasion of privacy, but the court reasoned if an individual could rightfully access his own record, "it defie[d] logic that to say that information properly contained in a person's record does not pertain to that person, even if it may also pertain to another individual."[101] The Court rightly rejected the "pertaining to" test using a plain reading of the Privacy Act. If a citizen has the right of access, under *Voelker,* only the existing exemptions authorize agency withholding.[102] Protecting third party privacy is not currently one of them.

The *Voelker* court tried to make sense of the legislative history. The court commented, "[I]f Congress had intended to shield from disclosure information in one person's record that pertains to another person, it could have and presumably would have added an exemption . . . ."[103] While it is true Congress did not express the intent to protect third party privacy, it does not follow that the omission was intentional. The legislative silence does not necessarily endorse the *Voelker* comment. Rather, the silence more likely reflects Congress's focused vision on fixing a specific problem and failure to consider the collateral issue of third party privacy. The court really meant it was not going to create an exemption where one did not exist. Either way, *Voelker* stands for the right of access over third party privacy. Admittedly, the legislative history indicates Congress was more inclined to give the individual access than to protect third party information, but only in the context of

97. *See Voelker*, 646 F.2d at 334.

98. *Id.* at 335.

99. *Id.*

100. *Id.* at 334.

101. *Id.*

102. *See id.* at 334 n.2 ("[T]he withheld information in this case was obviously gathered as part of an investigation of Voelker. We thus are not faced with the situation in which irrelevant materials were inadvertently misfiled or otherwise mistakenly placed in the record of the requesting party. We need not decide whether access to that type of information is required by the Privacy Act.").

103. *Voelker*, 646 F.2d at 335.

opening government files to data subjects, not in the context of exposing citizens' privacy to one another.[104]

The *Voelker* court considered the third party personal information but decided that Voelker's right to access outweighed the third party's privacy interests and it applied the plain language of the statute and granted access. [105] The court marshaled selective legislative intent to rationalize the decision.[106] This methodology demonstrates how the court interpreted the gap in favor of attorney Paul Voelker.

The *Voelker* court struggled with solving the third party privacy problem, but it did not have to struggle very hard because the facts favored Voelker. An IRS investigative report on Voelker, inside his own file clearly triggered the access right to records because the report was about him. The court easily found reason to not exempt a government investigative report about a government employee, contained in that employee's file. But suppose the third party privacy interest was more compelling and the requester was arguably a bad actor? Under these facts, the *Voelker* rationale could lead to a significant privacy invasion. In *DePlanche v. Califano*,[107] a court faced just such a situation.

B. DePlanche v. Califano

The *DePlanche* court wrestled with more difficult facts and consequently reached an opposite result than *Voelker*. DePlanche sought the address of his two minor children under FOIA and the Privacy Act.[108] The children lived with their mother after she successfully named DePlanche the father in a paternity suit.[109] DePlanche did not seek visitation rights but the court ordered him to pay child support.[110] The Social Security Administration paid his disability benefits directly to the children's mother to satisfy his obligation and her address appeared inside DePlanche's Social Security claims file.[111]

DePlanche decided he wanted to visit his children so he requested access to his own social security file hoping to learn their address.[112] The mother objected to the Social Security Administration releasing her address, claiming she feared harassment from DePlanche.[113]

---

104. *See generally* SOURCE BOOK *supra* note 23, at 330 (explaining that one area in which societal interest can supersede individual rights in the Privacy Act is "where records are required by law to be maintained for statistical research or reporting purposes and are not, in fact, used to make determinations about identifiable individuals").

105. *Voelker*, 646 F.2d at 333–34.

106. *See id.*

107. 549 F. Supp. 685 (W.D. Mich. 1982).

108. *Id.* at 688.

109. *Id.*

110. *Id.*

111. *Id.*

112. *Id.*

113. *DePlanche*, 549 F. Supp. at 691.

The Social Security Administration denied the FOIA request, citing Exemption 6.[114] After DePlanche filed suit, the Social Security Administration denied his Privacy Act request. The agency claimed the address was not about him nor did it pertain to him. [115]

DePlanche and *Voelker* faced the same legal issue: How can an agency deny an individual access to his own record absent an exemption? Their stark factual differences forced the *DePlanche* court into a greater struggle when confronting the third party privacy gap. Instead of a sympathetic government employee seeking access to his personnel file, in *DePlanche*, an unsympathetic and potentially harassing father sought access to his social security file. Instead of protecting a privacy interest inside a government investigation report, in *DePlanche*, the privacy interest the government sought to protect was the location of children with whom the father had no legal right to visit. *Voelker* weighed the facts in favor of access and held it would not create an exemption that did not exist. *DePlanche* balanced the facts in favor of withholding but misapplied both FOIA and Privacy Act as it tried to justify its balancing within the Privacy Act's inadequacies. The key is that both courts struggled to balance interests between individuals and sought to apply law that does not exist—a privacy exemption. The results in these cases represent two completely different outcomes from the same gap in the law. Both courts selectively cited legislative intent to justify their respective decisions, but the legislative history is silent on the direct point of third party information.

In *DePlanche,* the district court agreed with the agency decision to withhold the address. The court held:

> [T]he children's address may not be disclosed [under the Privacy Act because] it is not part of Plaintiff's record and [it] does not "pertain to him." Second, because it is exempt from required disclosure under FOIA Exemption 6 as a "clearly unwarranted invasion of personal privacy," its release is also prohibited under the Privacy Act without consent.[116]

The *DePlanche* opinion dramatically highlights how the third party privacy gap forced a court to use tortured legal analysis to support a decision it reached by using a simple balancing of interests test.

The *DePlanche* court essentially weighed the privacy interests of each party and decided that the mother's interest in keeping the children's location hidden outweighed DePlanche's right of access to his own social security file.[117] The more daunting task for the court was to justify the withholding

---

114. *DePlanche*, 549 F. Supp. at 688.

115. *Id.*

116. *Id.* at 699.

117. *Id.* at 689, 693–94 (highlighting that DePlanche was named the father after the mother brought a paternity suit against him; he did not seek visitation rights; he was ordered to pay child support; the mother called the sheriff because he harassed them; other more

under a statute that on its face seems to mandate disclosure absent an exemption. The *DePlanche* court went down the road of strained legal analysis to resolve the conflicting privacy interests.

In *DePlanche*, the court misunderstood the FOIA–Privacy Act relationship because it began the withholding analysis under FOIA. When a request triggers the Privacy Act, as it did here (the agency retrieved the address by the father's social security number), the Privacy Act must be analyzed first. If the Privacy Act access rule applies without exemption, then a FOIA exemption cannot be used to block access.[118] If however, a Privacy Act exemption applies to block access, then one would also apply FOIA analysis to see if any of the information is releasable.[119] If the Privacy Act's no-disclosure-without-consent rule applies, the FOIA would only apply as an exception to the Privacy Act.[120] When a request for an agency record triggers the Privacy Act, applying FOIA first, as did the court in *DePlanche*, is the analytical equivalent of putting the cart before the horse.

The *DePlanche* Court used the FOIA to establish that the address was a protected privacy interest that could be withheld under Exemption 6.[121] The court then reasoned if FOIA Exemption 6 applied, the protected privacy interest would trigger the Privacy Act's no-disclosure rule.[122] Since the mother did not consent to her address being disclosed, the court ruled DePlanche could not have the address even though it was maintained in his file and retrieved by his name.[123] The court even acknowledged its leap in logic, and yet applied the no-disclosure rule nonetheless.[124] The court claimed that the

---

recognized means were available to seek visitation; and the mother vocally objected to the disclosure).

118. 5 U.S.C. § 552a(t)(1) (2006) (providing that FOIA exemptions cannot be used to defeat Privacy Act access).

119. *See* U.S. DEP'T OF JUSTICE, OVERVIEW OF THE PRIVACY ACT OF 1974, *supra* note 73, at 92 ("An individual's access request for his own record maintained in a system of records should be processed under both the Privacy Act and the FOIA regardless of the statute(s) cited."); s*ee also* § 552a(t)(2) (providing that a Privacy Act exemption cannot be used to defeat FOIA release).

120. § 552a(b)(2) (providing an exception to the no-disclosure-without-consent rule in the event that disclosure is "required" by FOIA). Some argue that FOIA never requires disclosure.

121. *DePlanche*, 549 F. Supp. at 699.

122. *Id.* ("If [the address] is exempt from required disclosure because it is a clearly unwarranted invasion of privacy under FOIA's Exemption 6, its release is also prohibited under the Privacy Act's consent requirement."). The court's analysis is wrong for two reasons. First, the address did not have stand-alone Privacy Act part (b) non-disclosure protection. Because the address was retrieved from the father's file by using the father's identifier, part (b) can only apply to the father. The address is not entitled to part (b) protection unless the agency retrieved the address by the children's identifier, which it did not. Second, if the subject by whose identifier is used to retrieve is the requester, the agency is in the realm of access rights and exemptions, not in the realm of third party release and exceptions.

123. *DePlanche*, 549 F. Supp. at 694.

124. *See id.* at 700–01. Specifically, the court states:

legislative intent supported its reasoning.[125] The court's misplaced reasoning illustrates how hard it was trying to justify withholding the address. The legal analysis the court used to distinguish *Voelker* also showed its confusion.[126]

DePlanche was a Privacy Act case, but the court practically ignored the Privacy Act issue after a thorough, but misguided, FOIA analysis.[127] The court simply side-stepped the Privacy Act by holding that the children's address was not a "record" as defined by the Privacy Act.[128] Consequently, if the address was not a Privacy Act protected record, then DePlanche did not have an access right to it under the Privacy Act. Instead of confronting the issue of third party privacy within the access rule, the court retreated to the definition of "record" to avoid the Privacy Act altogether.[129] The court reasoned that the children's address was not "about" DePlanche and consequently not governed by the Privacy Act.[130] Future courts confronting the third party gap would ignore the confusion of the *DePlanche* FOIA rationale but focus instead

---

> Although it could be argued that the children's address does not constitute a "record which is contained in a system of records" under the provision requiring consent, § 552a(b), because the definition of "system of records" requires that the information be retrievable by the name or some other identifier assigned to the individual and the children's address is retrievable by their father's social security number the more meritorious argument is that; "in expounding a statute, we must not be guided by a single sentence or member of a sentence, but look to the provision of the whole law, and to its object and policy."

Id. (citations omitted).

125. *DePlanche*, 549 F. Supp. at 696 ("To permit [p]laintiff access to all the information contained in the claims folder maintained by his account number could conceivably violate the congressional intent underscoring the access provision . . . ."). The court mischaracterized the purpose of the Privacy Act by citing only to purposes behind the no disclosure rule. "[T]he main purpose of the Privacy Act is to forbid disclosure unless [disclosure] is required by FOIA." *Id.* at 695.

126. *Id.* at 696 (declaring *Voelker* distinguishable on its facts and citing a string of inapposite third party no disclosure and confidentiality exemption cases).

127. *Id.* at 694 ("[E]ven though it has been determined that release of this address under FOIA would be a clearly unwarranted invasion of the children's privacy, . . . it is still necessary to determine whether Plaintiff is entitled to obtain disclosure under the Privacy Act."). The court would have likely ignored the Privacy Act altogether but for a technicality in the statute. At that time, 5 U.S.C. § 552a(q) provided that FOIA Exemptions cannot be used to deny an individual access to his own record. The court was using FOIA Exemption 6 to block access, but it did so by interposing the no-disclosure as the reason for denial.

128. *Id.* at 695.

129. *Id.* at 694, 696.

130. *Id.* at 698. ("[L]ogic may seem to prevent specific material in an individual's record from being withheld on the grounds that it does not 'pertain to' that individual, it may be withheld for other reasons, including lack of consent . . . ."). So here, under these facts because consent was denied, logic supports refusal to disclose the address to DePlanche.

on whether the requested information was "about" the requester; in other words, is it even a Privacy Act protected record?

Comparing *Voelker* and *DePlanche* reveals that, regardless of the legal approach, the facts drive the decision in third party privacy information cases. While *Voelker* is a better reasoned decision, if one applies its reasoning to the facts of *DePlanche*, the result would have been to disclose the whereabouts of a mother and children to a potentially stalking father who had no legal visitation rights. Because the Privacy Act was aimed at stopping abusive government, the Privacy Act does not allow for a balancing of privacy interests between citizens.

While unintended, the *DePlanche* court articulated a legal mechanism that allowed future courts to fairly deal with the Privacy Act gap. If a court deems it factually appropriate to give third party information, it calls the information a Privacy Act record to which the requester is entitled (i.e. if it's in the requester's file, it's about the requester). If a court determines the facts do not warrant disclosure of the third party information, it excludes the information from the "record" definition (i.e. it is not "about" the requester, even if the information is in the subject requester's file and retrievable by his name). Courts across the circuits now apply the "is it a record test," both broadly and restrictively adding to the confusion.[131] While this approach may result in the "right" outcome, it is not an intellectually honest approach and results in case law that cannot be followed.

All federal agencies confronting this issue tried to make sense out of the statute and the case law but have created policy and regulations that are similarly confusing and unworkable. *Voelker* involved the Internal Revenue Service. *DePlanche* involved the Social Security Administration. The military department's privacy regulations exemplify the struggle to work with a defective law.

C. The Army Privacy Program

Army Regulation 340-21,[132] drafted in 1985, attempted to close the Privacy Act gap by including principles from both *Voelker* and *DePlanche*. In doing so, the regulation drafters added another layer of confusion. The first sentence of the Army regulation appears to embrace *Voelker's* plain reading of the statute: "Third party information pertaining to the data subject may not be deleted from a record when the data subject requests access to the record unless there is an established exemption."[133] But the next sentence appears to embrace *DePlanche*: "However, personal data such as *SSN and home address* of a third party normally do not pertain to the data subject and therefore may be withheld."[134] Read together, the first sentence does not really follow *Voelker*

131. *See infra* Part II.D.

132. U.S. DEP'T OF ARMY, REG. 340-21, THE ARMY PRIVACY PROGRAM (5 July 1985) [hereinafter AR 340-21].

133. *Id.* at para. 2-6.

134. *Id.*

and when coupled with the second sentence seems to undercut *Voelker* completely. A records custodian trying to decide whether to disclose information can only struggle to make sense of this regulation.

Under *Voelker,* if an individual could access his record, it "defie[d] logic" to create a second "'pertaining to'" test."[135] The Privacy Act grants individual access rights to either an individual's "record *or to any information pertaining to him which is contained in the system*."[136] The first sentence of the Army Regulation implies that an individual can be denied access from his own record even without an exemption *if* the information does not "pertain" to him. Therefore, even the first sentence of the Army regulation is imbued with the "pertaining to" test that *Voelker* soundly rejected.

The second sentence of the Army regulation plainly gives examples of that which normally does not pertain to a data subject such as another person's social security number (SSN) and home address. An individual, who can rightly access his record under the Privacy Act, might be denied third party information under a second "pertaining to" test when the regulation sentences are read together or separately. In its attempt satisfy *Voelker's* holding, the Army's regulation adopts the very test the circuit court in *Voelker* rejected.

Where did the regulation drafters get the "pertaining to" language since *Voelker* plainly rejected applying a "pertaining to" test when an individual has a right of access? They likely misread *DePlanche*. *DePlanche* recognized that the access right was twofold: An individual has the right to access his "agency record" or an individual has the right to access any information system wide that "pertains to" the individual.[137] In its decision, the *DePlanche* court said the children's address was neither a DePlanche record nor did it pertain to him. The Army regulation drafters grabbed the idea that a piece of information inside someone else's file might not pertain to a requester from *DePlanche*, but they merged the two prongs of access which allow an individual access to his record *or* to information that pertains to him into one rule. This oversight is why the drafters included "pertain" in the first sentence and "normally do not pertain" in the second sentence.

This analysis gets more difficult when records are retrieved by multiple names.[138] For example: One soldier runs a light and crashes his car into another soldier in front of three more soldiers. The Military Police (MP) report has the names of everybody and their SSNs. The provost marshal maintains the report in a system of records retrievable by every person's name

---

135. Voelker v. IRS, 646 F.2d 332, 334 (8th Cir. 1981).

136. 5 U.S.C. § 552a(d)(1) (2006) (emphasis added).

137. DePlanche v. Califano, 549 F. Supp. 685, 695 (W.D. Mich. 1982).

138. *See* Topuridze v. U.S. Info. Agency, 772 F. Supp. 662, 666 (D.D.C. 1991) (holding that a record that is dually retrievable may be accessed by a requester even if it pertains to another person). *But see* Sussman v. U.S. Marshals Serv., 494 F.3d 1106, 1121 (D.C. Cir. 2007) (holding that 5 U.S.C. § 552a(d)(1) (2006) does not entitle access to all information pertaining to an access requester that "happens to be contained in a system of records.").

and SSN. The victim soldier had been taken to the hospital unconscious. He now wants to sue the soldier that hit him and requests the MP report. What is the analysis under the Army regulation? It depends on the whim of the records custodian. He could conclude that although the third party information, i.e. names, SSNs, and addresses come up when the victim's identifier retrieves the record, this information does not pertain to him.[139] The custodian could alternatively decide that it does pertain to him because the third parties were involved in the injuries to the data subject victim as a tortfeasor or witness. The regulatory rule is problematic because it gives discretion without guidance causing unpredictable and disparate results.

The regulatory confusion caused by the Privacy Act and the case law is not limited to the Army. The Department of Defense (DOD) had a *Voelker* rule but in 2007 changed to a *DePlanche* rule. The 1999 Department of Defense Directive did not address the third party information issue at all.[140] Its rule was pure *Voelker*, in that it said the agency must release everything unless statutorily exempted.[141] However, in 2007, the new version of the Directive now qualifies the access to the "individual to whom the record pertains."[142] Now, the Department of Defense has officially endorsed a "pertaining to" test as established in *DePlanche* and rejected by *Voelker*.

The Navy's former policy tracked the Department of Defense's former policy, embracing *Voelker* and providing that everything be released unless exempted.[143] However, the Navy promulgated a new policy in 2005 that qualifies access to "records to which they are entitled."[144] There is simply no

---

139. *But see* AR 340-21, *supra* note 132, at para. 2-6. The third sentence of this paragraph provides, "[i]nformation about the relationship between the data subject and the third party would normally be disclosed as pertaining to the data subject." *Id.* This is unhelpful because the victim wants to find the person and might want more than information pertaining to the relationship.

140. U.S. DEP'T OF DEFENSE, DIR. 5400.11, DEP'T OF DEFENSE PRIVACY PROGRAM (Dec. 13, 1999), *available at* http://biotech.law.lsu.edu/blaw/dodd/corres/pdf2/d540011p.pdf (not addressing the third party information issue).

141. U.S. DEP'T OF DEFENSE, DIR. 5400.11-R, DEP'T OF DEFENSE PRIVACY PROGRAM, ch.3, sec C3.1, para. C3.1.4, sub-para. C3.1.4.1, app. 4 (Aug. 1983), *available at* http://www.cac.mil/docs/DOD-5400-11.pdf ("Grant the individual access to the original record . . . without any changes or deletions . . . .").

142. U.S. DEP'T OF DEFENSE, DIR. 5400.11-R, DEP'T OF DEFENSE PRIVACY PROGRAM ch. 3, sec. C3.1, para C3.1.1, sub-para. C3.1.1.2 (May 2007), *available at* http://www.dtic.mil/whs/directives/corres/pdf/540011r.pdf ("Make available to the individual to whom the record pertains all of the personal information contained in the system of records except where access may be denied pursuant to an exemption claimed for the system.").

143. U.S. DEP'T OF NAVY, SEC'Y OF THE NAVY INSTRUCTION 5211.5D, DEP'T OF THE NAVY PRIVACY ACT PROGRAM sec. 11, subsec. (a)(6)(A) (July 17, 1992), *available at* http://www.donico.navy.mil/privacyprotection/resources/docs/privacy/5211_part1.html (Granting "individual access to the original record . . . without any changes or deletions . . . .").

144. U.S. DEP'T OF NAVY, SECRETARY OF THE NAVY INSTRUCTION 5211.5E, DEP'T OF THE NAVY PRIVACY PROGRAM para. 8, sec. (c)(1) (Dec. 28, 2005), *available at* http://www.cnic.navy.mil/navycni/groups/public/@hqffr/documents/document/cnicd_a065

guidance as to what "entitled" means in the Navy's new policy. It could be interpreted as *Voelker*: release everything unless statutorily exempted, or it could be interpreted as *DePlanche*: release unless it does not pertain to the requester.

The 1999 Air Force policy was similar to the Army policy in that it provided for release to an access requestor unless exempted, but allowed withholding of personal information about a third person.[145] The Air Force promulgated a new policy in 2011, which amplifies the prior rule. It provides, "[a] first party requester is *not* entitled to information that is not "about" him or her that is contained in their Privacy Act record; for example, the home address or SSN of a third party." [146] The Air Force regulation seems to have created its own "not about him or her exemption."

The Department of Education (DOE) has also adopted a "pertaining to" test when it comes to access to one's records under the Privacy Act.[147] The DOE regulation tells the records custodian to grant access to a record if the person requesting is "the subject individual."[148] While this sounds like the *Voelker* approach, earlier in the regulation, "subject individual" is defined as, "that individual to whom a record pertains."[149] Thus, once again the records custodian is left with discretion and little guidance to grant or deny based on a "pertaining to" test.

The above regulations show how federal agencies struggle to comply with the plain language of the Privacy Act while protecting third party privacy. Like the courts, the agencies have struggled to balance competing privacy interests. The Army and Air Force take the "disclose unless exempted" approach but then overlay a "pertaining to or about" test as a way to keep back third party privacy information. The DOD, as well as the DOE, now have a straight "pertaining to" test as a condition for release to an access requester, and the Navy's new policy seems to go either way. As noted above, *Voelker* and *DePlanche* came from the IRS and Social Security Administration, respectively. As shown next, these two agencies continue to generate cases stemming from

---

521.pdf ("Allow individuals to have access to and/or copies of all or portions of their record to which they are entitled.").

145. U.S. DEP'T OF AIR FORCE, SEC'Y OF THE AIR FORCE INSTRUCTION 33-332, AIR FORCE PRIVACY ACT PROGRAM ch.4, sec. 4.4, para. 4.4.3, 4.4.4 (Nov. 8, 2000), *available at* http://www.e-publishing.af.mil/shared/epubs/afi33-332.pdf ("Do not delete third-party information from a record when the subject requests access, except as noted in paragraph 4.4.4. . . . Presume that all information in a file pertains to the subject of the file. . . . Do not release third-party personal data (such as SSN and home address). This action is not a denial.").

146. U.S. DEP'T OF AIR FORCE, SEC'Y OF THE AIR FORCE INSTRUCTION 33-332, AIR FORCE PRIVACY ACT PROGRAM ch. 3, sec. 3.5, para 3.5.2 (May 16, 2011) (emphasis in original), *available at* http://www.e-publishing.af.mil/shared/media/epubs/afi33-332.pdf.

147. 34 C.F.R. §§ 5b.1–5b.13 (2012).

148. *Id.* at § 5b.5(c)(1).

149. *Id.* at § 5b.1(m).

this gap in the law. Cases from other agencies such as the Department of Commerce, the FBI and the U.S. Marshals service continue to show how this issue affects the breadth of the federal government. The situation must change.

D. The Evolution of Voelker and DePlanche: What is a Record?

Subsequent courts grappled with the language of the statute and its legislative intent (or lack of intent) much like *Voelker* and *DePlanche*. These courts either applied a plain reading of the statute as in *Voelker*, or defined the information out of "record" as in *DePlanche*. This struggle gave way to a single approach: Is the information a record? At first glance, this approach suggests that *DePlanche's* analysis prevailed. In reality, *DePlanche* just provided a test that offered greater flexibility, but in the end caused further conflict over the definition of "record" under the Privacy Act. Courts now have created a varied body of case law defining "record." The initial statutory gap spawned a labyrinth of case law to navigate. The confusion requires a new exemption to the Privacy Act to uniformly protect third party information.

Voelker found initial support in some of the circuits. The Tenth Circuit Court of Appeals gave access guidance in *Wren v. Harris.*[150] Wren, an administrative law judge with the Social Security Administration, requested various documents from his own agency personnel file.[151] The lower court withheld based on FOIA, without analyzing the Privacy Act.[152] The Tenth Circuit said the court may not withhold under FOIA if, after a Privacy Act analysis, Wren is entitled to access.[153] *Wren* tangentially addressed the issue, but what it said was consistent with *Voelker*. Likewise the Seventh Circuit Court of Appeals, in *Becker v. Internal Revenue Service,*[154] relied on *Voelker* to support two brothers' request to remove outdated newspaper articles about tax protesters from their IRS files. The articles were not about the Becker brothers and they only sought removal, not access, but the court directly cited *Voelker* to support the brothers' right to access.[155] The Tenth and Seventh Circuit cases support the *Voelker* plain meaning approach.

The District of Columbia Circuit is particularly important because it has universal venue for Privacy Act cases.[156] It too has struggled to balance individual privacy interests within the boundaries of an inadequate law. The

---

150. 675 F.2d 1144 (10th Cir. 1982).

151. *Id.* at 1145.

152. *Id.* at 1146.

153. *Id.* at 1147.

154. 34 F.3d 398, 400, 408 (7th Cir. 1994).

155. *Id.* at 408–09, 409 n.27. The court also noted that the IRS argued that the file was an exempted law enforcement file under 5 U.S.C. 552a(k)(2), but the court ruled it was untenable that such unrelated and outdated newspaper stories would be of any possible future enforcement use against the Becker brothers, and therefore held the agency did not meet its burden to justify an exemption. *Id.* at 409.

156. 5 U.S.C. § 552a(g)(5) (2006); *see* SOURCE BOOK, *supra* note 23 at 251, 311.

District Court for the District of Columbia (D.D.C.) relied upon *Voelker* in *Topuridze v. U.S. Information Agency.*[157] In *Topuridze*, the court confronted an access issue where an employee of the United States Information Agency (USIA) requested access to a letter containing third party privacy information maintained in his own agency personnel file.[158] The agency claimed the no-disclosure rule prevented release because the letter could also be retrieved by the author's name.[159] Relying on *Voelker*, the court said, "the exist[ing] case law and the purpose[] of the Privacy Act mandate disclosure of the letter. . . . Had Congress intended a 'dual-record' exemption to the Privacy Act . . . it presumably would have done so."[160] Therefore, the court acknowledged that Congress intended to release all information in an access requester's file to the access requester and there is no exemption for a record that might apply to two different people, which could in theory trigger the no-disclosure without consent rule. The court decided several access cases after *Topuridze* that illustrate the challenge of the Privacy Act gap.

In *Henke v. U.S. Department of Commerce*,[161] the agency denied a contractor's request for access to the identities of government evaluators who rejected her contract proposal. The District of Columbia Court of Appeals ultimately exempted the information under an express promise of confidentiality exemption.[162] However, in refuting a government agency argument that the no-disclosure rule operated as an exemption to access, the court said, "[t]his court agrees [with *Voelker*], and will therefore not create an exemption to the Privacy Act that Congress did not see fit to include itself."[163]

In between *Topuridze* and *Henke*, the D.C. District Court decided *Tobey v. NLRB.*[164] There, the court held that NLRB case records handled by Tobey (a government employee) and retrievable by his name was not his record.[165] Tobey had been removed from a promotion roster based on his performance in these cases and he sought access to the file containing the information which formed the basis for his removal.[166] After *Henke,* in *Haddon v. Freeh*,[167]

---

157. 772 F. Supp. 662, 665 (D.D.C. 1991).

158. *Id.* at 663.

159. *Id.*

160. *Id.* at 665.

161. Henke v. U.S. Dep't of Commerce, No. 94-0189, 1996 WL 692020, at *8 (D.D.C. Aug 19, 1994), *vacated,* 83 F.3d 1453, 1462 (D.C. Cir. 1996) (holding that the information was not even contained in a system of records).

162. Henke v. U.S. Dep't of Commerce, 83 F.3d 1453, 1462 (D.C. Cir. 1996).

163. *Henke*, 1996 WL 692020, at *4.

164. 807 F. Supp. 798 (D.D.C. 1992), *aff'd*, 40 F.3d 469 (D.C. Cir. 1994) ("[T]he information concerning Tobey pertains to official government business, i.e. keeping track of NLRB cases and the agents assigned to handle them. . . . [I]t reveals nothing about [Tobey's] private affairs so as to trigger the protective provisions of the Privacy Act.")

165. *Tobey*, 807 F. Supp. at 779–801.

166. *Id.* at 800.

the D.D.C. again decided that information it did not want to release was not a record. The court denied access to a White House chef who wanted the names and extensions of FBI agents in his agency file after their investigation led to the chef's dismissal.[168] The court held that the information was not a "record" to which Haddon had access rights because the information was not "about" him.[169]

The D.D.C. occasionally relied on both approaches, depending on the facts. In *Topuridze* and *Henke,* the court embraced *Voelker's* notion that where there was no statutory exemption, the court would not create one. However, when the court confronted information it did not want to release (FBI agent names and telephone extensions in *Haddon* and NLRB case agent names in *Tobey*), the court used *DePlanche* to define other peoples' privacy interests out of the definition of record.[170] When the same court embraces both approaches depending on the factual balance, the result is a confusing body of case law.

In *Sussman v. U.S. Marshals Service,*[171] the D.C Circuit Court of Appeals embraced the *DePlanche* approach. The court acknowledged the lack of guidance in the circuit,[172] and held that to qualify as a record, the item must not only contain the requester's name or other identifying particular, but also be "about" him.[173] Moreover, the court held that an agency need only grant access under 5 U.S.C. § 552a(d)(1) to a requester's own record, not to all information pertaining to him which is contained in a system of records.[174] Thus, the ruling also rejects the statutory language that allows "access to his record *or to any information pertaining to him which is contained in the system*."[175]

Sussman sought "[a]ny and all records relating to me, mention[ing] me, or otherwise pertain[ing] to me" from the U.S. Marshals Service.[176] The search returned only one document relating to Sussman until he presented a "Wanted Poster" for Keith Maydak, which listed Sussman as an alias.[177] A second search revealed 813 pages of information relating to Sussman, and the

---

167. 31 F. Supp. 2d 16, 22 (D.D.C. 1998).

168. *Id.* at 18–19.

169. *Id.* at 22.

170. *Cf.* Doe v. U.S. Dep't of Justice, 790 F. Supp. 17, 21 (D.D.C. 1992) (holding that an attorney denied employment with the F.B.I. is exempt from accessing third party information in his pre-employment investigation file when express promises of confidentially were made to sources).

171. Sussman v. U.S. Marshals Serv., 494 F.3d 1106, 1121 (D.C. Cir. 2007).

172. *Id.* at 1120 ("The precise contours of an agency's duty under §552a(d)(1) have never been defined in this circuit.").

173. *Compare id.* at 1121, *with* Voelker v. IRS, 646 F.2d 332, 334 (8th Cir. 1981) ("There is no justification for requiring that information in a requesting individual's record meet some separate 'pertaining to' [test]. . . . ").

174. *Sussman*, 494 F. 3d at 1121 ("[W]e interpret 5 U.S.C. § 552a(d)(1) to give parties access only to their own records, not to all information pertaining to them that happens to be contained in a system of records.").

175. 5 U.S.C. § 552a(d)(1) (2006) (emphasis added).

176. *Sussman*, 494 F.3d at 1109 (alterations in the original).

177. *Id.*

Marshals Service released all but 47 pages.[178] It is not clear whether the Marshals Service retrieved the information using Maydak, Sussman or both, but the court took the opportunity to define an agency's duty under a 5 U.S.C. § 552a(d)(1) access request[179] and denied Sussman information pertaining to him contained in a system of records because the information was contained in Maydak's record.

The court relied on the 1975 OMB guidelines example of not disclosing information to a requester if his information is contained in another person's record and retrieved only by that other person's name.[180] As noted, the reported decision does not mention how the Marshals Service retrieved information relating to Sussman on the second search. One can infer that had the search been only by Maydak, the analysis would be over using the OMB guidelines. But, the court went further by interpreting that the dual prong access rule ("his record" or "any information pertaining to him contained a system of records") to mean in either case, the duty is to only release, "the record."[181] This suggests that even if information pertaining to Sussman was retrieved by Sussman's name (or both Maydak and Sussman), it can and should be denied to Sussman if it does not meet the "about" him test that *Voelker* plainly rejected. Thus, the court simply negates the second access right trigger contained in the plain reading of the statute. [182]

Factually, *Sussman* was not a third party information in an access requester file case; it was the reverse—an access requester's information in a third party's file. Thus *Sussman* did not cite *Voelker*, *DePlanche* or even *Topuridze*, but it impacts all access requests. If a requester is not entitled to his own information in another's file (even if retrieved by his name and it pertains to him, yet it might still not be "about him"), how much more so is a third party's information in an access requester's file not about the requester? By elevating the *Depalnche* "about him" test, and essentially establishing the "what is a record?" approach for the D.C. Circuit, *Sussman* has not really solved the problem; it merely continued it. *Voelker* is still good law in the Eighth Circuit and stands in direct conflict with the D.C. Circuit. A better approach would be a third party privacy exemption that could be used under any fact pattern

178. *Sussman*, 494 F.3d at 1110.

179. *Id.* at 1120–21, 1120 n.7 ("While we have occasionally summarized this provision in language that suggests its scope . . . we have never confronted the question directly.") (citation omitted).

180. *Id.* at 1120. *See also*, Privacy Act Implementation, 40 Fed. Reg. 28,949, 28,957 (July 9, 1975) ("If an individual is named in a record about someone else . . . and the agency only retrieves the portion pertaining to him by reference to the other person's name . . . the agency is not required to grant him access.").

181. *Sussman*, 494 F.3d at 1120.

182. *Id.* The court's third rationale asserted that it would be an onerous burden for an agency to comb through multiple data bases and media to find and provide system wide information pertaining to a first party requester. *Id.* at 1120–21.

and avoid such strained holdings as in *Sussman*, that simply defined away part of the access provision in order to avoid disclosing information pertaining to Sussman that could have implicated Maydak's privacy.

The *DePlanche* "what is a record?" approach has arguably taken hold as the standard approach, particularly in light of *Sussman,* but courts still cannot agree on how to define a "record" under the Privacy Act. Varied judicial definitions of "record" further compound the problem and cause another layer of confusion in the case law.

Some circuits have taken a broad approach in defining a record.[183] In *Quinn v. Stone*,[184] the Third Circuit held that the term "record" "encompass[es] *any* information about an individual that is linked to that individual through an identifying particular and is not to be restricted to information that reflects a characteristic or quality."[185] In *Bechhoefer v. United States Department of Justice Drug Enforcement Administration*,[186] the Second Circuit likewise defined a record broadly as including "at the very least, any personal information 'about an individual that is linked to that individual through an identifying particular.'"[187] Ironically, applying this broad definition of record to the *DePlanche* facts would have likely resulted in a release of the address using the very test *DePlanche* created to withhold it. If an access requester brings suit in a circuit where "record" is defined broadly, he will probably prevail. However, other circuits take an opposite view.

Other courts have taken a restrictive approach in defining a record. In *Boyd v. Secretary of the Navy*,[188] the Eleventh Circuit adopted the plain meaning of the Privacy Act statutory definition and added its selection of the legislative intent requiring "some quality or characteristic of the individual."[189] This directly contradicts the OMB guidelines' definition of record.[190] In *Unt v. Aerospace Corp.*,[191] the Ninth Circuit similarly requires "some quality or characteristic" of the individual.[192] This narrow view of record is more in line with *DePlanche*, in that there must be a more direct nexus to the access requester. An access requester who brings suit in one of these circuits could have a more difficult

---

183. Privacy Act Guidelines, 40 Fed. Reg. 28,494, 28,951 (1970) (A "record" can include "any item of information about an individual that includes an individual identifier."). *But see* Zeller v. United States, 467 F. Supp. 487, 497 (E.D.N.Y. 1979) (stating "OMB's guidelines do not bind this court").

184. 978 F.2d 126 (3d Cir. 1992).

185. *Id.* at 133.

186. 209 F.3d 57 (2d Cir. 2000).

187. *Id.* at 62 (reasoning that it was the Congressional intent to have a broad definition of record)(citations omitted).

188. 709 F.2d 684 (11th Cir. 1983) (per curium).

189. *Id.* at 686.

190. *See* Privacy Act Implementation, 40 Fed. Reg. 28,949 (July 9, 1975). The OMB guidance is expansive and does not specifically require a quality or characteristic of an individual as part of the definition of record.

191. 765 F.2d 1440 (9th Cir. 1985).

192. *Id.* at 1449.

time gaining access. The varied standards across the circuits further highlight the problem caused by the Privacy Act's silence.

The D.C. Circuit took the middle ground in *Tobey v. NLRB.*[193] The court rejected the requirement of reflecting a quality or characteristic used by the restrictive approach as "too narrow."[194] The court also rejected the Third Circuit's definition as too broad because it "fails to require that information both be 'about' an individual and be linked to that individual by an identifying particular."[195] *Tobey* refined the definition of record saying, to qualify as a record, an item must contain "information that actually describes the individual in some way."[196]

In addition to the original *Voelker* and *DePlanche* approaches, the current case law across the circuits defines record from one extreme to the other. The "what is a record?" case law is inconsistent and confusing.[197] The problem of the Privacy Act gap remains despite courts trying to bridge the gap. Interestingly, the "what is a record?" dispute began in the Congress itself.[198] Since the issue of defining a record to which an individual had an access right was not satisfactorily resolved, it follows that the issue of a third party privacy exemption was not explored at all.

The Privacy Act allows an invasion of privacy because there is no third party privacy exemption. The courts have found a semantic mechanism to carry out decisions based on a factual assessment of competing privacy interests. The "what is a record?" mechanism treats the symptom but not the cause of the problem. The shear breadth of how different courts define a "record" creates uncertainty and confusion. Now, in the aftermath of *Sussman*, an access requester can be denied information pertaining to himself no matter where it is located if it does not qualify as a "record." A better way to handle the problem would be to amend the Privacy Act to include a new third party privacy exemption.

---

193. 40 F.3d 469 (D.C. Cir. 1994).

194. *Id.* at 472.

195. *Id.*

196. *Id.* at 472. *See also* Sussman v. U.S. Marshals Serv., 494 F.3d 1106, 1121 (D.C. Cir. 2007) (citing Tobey v. NLRB*,* 40 F.3d 469, 474 (D.C. Cir. 1994) for the definition of "record.").

197. *See generally* Jo Ann F. Wasil, *What is "Record" Within Meaning of Privacy Act of 1974 (5 USCS § 552a)*, 121 A.L.R. FED. 465, 473 (2000) (surveying how the same documents can be a record in one circuit, but not in another because of the definition applied).

198. SOURCE BOOK, *supra* note 23, at 304 (restricting the definition of record in the House bill as a collection or grouping of information about an individual); *Id.* at 231–32 (expansively defining the definition of record in the Senate bill as including all personal information including things done by and to the individual); *Id.* at 993–94 (embracing the Senate's version in the compromise bill and keeping the "about" language which was common to both but never defined).

IV. A NEW LEGISLATIVE AND JUDICIAL APPROACH TO THIRD PARTY INFORMATION

A. The Privacy Act Requires a New Third Party Privacy Exemption

Congress should amend the Privacy Act to redress its own omission. The clear initial target of the Privacy Act was government privacy abuse. In adopting the Privacy Act, Congress unquestionably leaned more toward disclosure of broadly defined records than exemption, but the context was curbing government abuse of privacy. Congress did not think through the permutations of competing individual interests at the time it passed the Privacy Act because its sights were on the individual versus the government interests. Today, courts have avoided the real issue. Instead, they try to bridge the gap with congressional intent and definitions that do not exist. Congress should create a new exemption to fix the problem because Congress missed the issue.

Without a new exemption allowing courts to openly balance competing individual privacy interests, the intellectual dishonesty, confusion, and uncertainty will continue. The current practice ensnares records custodians into the seemingly endless maze of government information practice without guidance. As technology becomes even more sophisticated, the "big brother society" envisioned by Congress is fast approaching, if not already here.[199] As technology grows to handle even more information, the gap in protecting third party privacy grows too. The law requires a new change for the new reality in the information age.[200] The Privacy Act needs a mechanism to resolve competing individual privacy interests in government files.

B. A Strong Societal Interest Justifies a New Third Party Privacy Exemption

When Congress considered what information in a citizen's file should be withheld from that citizen, it announced a restrictive standard. Whether a new third party privacy exemption is justified requires analysis under the same standard that supports the existing ten exemptions. Both Houses of Congress favored access over withholding.[201] The Privacy Act itself says that only an

---

199. *See generally* Susan E. Gindin, *Lost and Found in Cyberspace: Informational Privacy in the Age of the Internet*, 34 SAN DIEGO L. REV. 1153 (1997) (discussing how privacy can be invaded electronically through on-line transactions).

200. *See* FRED H. CATE, PRIVACY IN THE INFORMATION AGE 2 (1997) (discussing the ramifications of readily obtainable information concerning health, credit, marital, educational and employment histories; telephone calls made and received; books borrowed, cash withdrawn, credit card transactions, electronic mail, and where one goes on the internet).

201. *See* SOURCE BOOK *supra* note 23, as well as *supra* notes 80, 82–83, and accompanying text.

"important public policy need justifies an exemption."[202] More precisely, the Congress relied on the HEW report that stated, "only a strong societal interest" justifies an exemption.[203] Clearly, the common element of all exemptions is a strong societal need.

In the "information age," citizens need privacy protection from one another more than ever. Identity theft is rampant.[204] It is simplistic to say, as in *Voelker,* that because there is no third party exemption, Congress intended for one person to invade the privacy of another person when requesting access under the Privacy Act.[205] It is equally inappropriate to say, as in *DePlanche*, that the policy supporting the no-disclosure rule should be superimposed into the access rule on a piece of information that does not even trigger Privacy Act protection, in order to deny an access right.[206] Congress has shown interest in protecting individual privacy interests from other individuals through numerous pieces of other legislation over the years.[207] These concerns

---

202. Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896, §§ 2(B)(1), (5). "The purpose of this Act is to . . . permit exemptions . . . only in those cases where there is an important public policy need for such exemption . . . ."

203. HEW REPORT, *supra* note 20, at 60 ("No exemption from … the right of data subjects to have full access to their record should be granted unless there is a clearly paramount and strongly justified societal interest in such exemption. . . .").

204. *See* Lynn Langston, *Identity Theft Reported by Households, 2005–2010*, U.S. DEP'T OF JUSTICE (Nov. 2011), http://bjs.ojp.usdoj.gov/content/pub/pdf/itrh0510.pdf (explaining that there has been an increase in identity theft victimization from 2005 to 2010, largely attributable to an increase in the misuse or attempted misuse of credit card accounts).

205. Voelker v. IRS, 646 F.2d 332, 334 (8th Cir. 1981).

206. DePlanche v. Califano, 549 F. Supp. 685, 694 (W.D. Mich. 1982).

207. *See, e.g.*, Administrative Procedure Act of 1966, 5 U.S.C. §§ 552-559 (2006); Cable Communications Privacy Act of 1984, 47 U.S.C. § 551 (2006); Census Confidentiality Statute of 1954, 13 U.S.C. § 9 (2006); Children's Online Privacy Protection Act of 1998, 15 U.S.C. § 6502 (2006); Communications Assistance for Law Enforcement Act, 47 U.S.C. § 1002 (2006); Federal Information Security Management Act, 40 U.S.C. § 11331 (2006); Justice Systems Improvement Act, 42 U.S.C. § 3789g (2006); Privacy of Customer Information, 47 U.S.C. § 222 (2006); Driver's Privacy Protection Act of 1994, 18 U.S.C. § 2721 (2006); Drug and Alcoholism Abuse Confidentiality Statutes, 42 U.S.C. § 290dd-2 (2006); Electronic Communications Privacy Act of 1986, 18 U.S.C. § 2701 (2006); Electronic Fund Transfer Act, 15 U.S.C. § 1693 (2006); Employee Polygraph Protection Act of 1988, 29 U.S.C. § 2002 (2006); Employee Retirement Income Security Act of 1974, 29 U.S.C. § 1025 (2006); Equal Credit Opportunity Act, 15 U.S.C. § 1691 (2006); Equal Opportunity Employment Act, 42 U.S.C. §§ 2000e-2, e-3 (2006); Fair Credit Billing Act, 15 U.S.C. § 1666 (2006); Fair Credit Reporting Act, 15 U.S.C. § 1681 (2006); Fair Debt Collections Practices Act, 15 U.S.C. § 1692 (2006); Fair Housing Act, 42 U.S.C § 3604 (2006); Family Education Rights and Privacy Act of 1974, 20 U.S.C. § 1232g (2006); Gramm-Leach-Bliley Act, 15 U.S.C. § 6801 (2006) (regulating the privacy of personally identifiable, nonpublic financial information); The Health Insurance Portability and Accountability Act, Pub. L. No. 104-191, 110 Stat. 1936 §§ 1128C(a)(3)(B)(ii), 1128E(b)(3), 264 (1996) (codified as amended at 42 U.S.C. §§ 1320a-7c, 1320a-7e (2006)); Health Research Data Statute, 42 U.S.C. § 242m (2006); Privacy Protection Act of 1980, 42 U.S.C. § 2000aa (2006); Right to Financial

demonstrate the strong need to fix the Privacy Act with a new exemption covering third party privacy interests inside an access requester's file.

The only remaining questions are: What would the exemption look like, and how would it work? One commentator proposed that third party information should receive the no-disclosure protection unless it materially affected the requester.[208] However, this approach does not comport with the Supreme Court's guidance in *Reporters Committee*[209] because it does not consider the core purpose of the statute as a factor in the balancing of interests. Moreover, injecting the no-disclosure rule into the access provision has been rejected for the most part in favor of the "what is a record?" approach. A better approach would be to model a new balancing exemption after FOIA Exemption 6 as applied in *Reporters Committee*. Because FOIA and Privacy Act access rights operate similarly, drafting a third party privacy exemption modeled after FOIA into the access provision would solve the problem.

C. The Third Party Privacy Exemption

The Privacy Act access rule is closely analogous to FOIA as it relates to the subject requester in the subset of "system of records." FOIA releases to the public unless exempted and the access rule releases to the individual access requester unless exempted. The FOIA exemptions and the access exemptions are likewise similar. Just as the FOIA exempts certain categories of information from the general public's right to know, so too the Privacy Act exempts from the individual access requester certain categories of information, that for strong public policy reasons, a citizen should not have the ability to access, even if it is his own file.[210] FOIA uses Exemptions 6 and 7(C) to protect personal privacy, but the Privacy Act does not have any similar privacy exemption. The FOIA Exemption 6 should be the model for a new personal privacy exemption under the Privacy Act because of the similarity between FOIA's protecting privacy from the public access, and the new exemption's protecting privacy from a private individual's access. The new Privacy Act exemption should state: "The custodian of record may exempt any record

---

Privacy Act, 12 U.S.C. §§ 3401–3403 (2006); Tax Reform Act, 26 U.S.C. §§ 6103, 6108 (c), 7609 (2006); Telephone Consumer Protection Act, 47 U.S.C. § 227(c) (2006); Video Privacy Protection Act of 1988, 18 U.S.C. § 2710 (2006); Computer Matching Privacy Protection Act of 1988, 5 U.S.C. § 552a(o) (2006).

208. Major John F. Joyce, *The Privacy Act: A Sword and a Shield, but Sometimes Neither*, 99 MIL. L. REV., Winter 1983, at 113, 137.

209. U.S. Dep't of Justice v. Reporters Comm. For Freedom of the Press, 489 U.S. 749, 762 (1989).

210. *Compare* 5 U.S.C. § 552(b)(1) (2006) (exempting information classified by executive order), *with* 5 U.S.C. § 552a(j)(1) (2006) (exempting information maintained by the Central Intelligence Agency); *compare* 5 U.S.C. § 552(b)(5) (exempting agency memoranda for most civil litigation purposes), *with* 5 U.S.C. § 552a(d)(5) (exempting all information made in preparation of civil litigation); *compare* 5 U.S.C. § 552(7), *with* 5 U.S.C. §§ 552a(j)(2), (k)(2) (both exempting Law Enforcement information). FOIA exempts privacy interest in §§ 552(b)(6) and (7)(C), but the Privacy Act does not have such an exemption.

which if disclosed would constitute a clearly unwarranted invasion of another person's privacy."[211]

D. The substantive application of the third party privacy exemption

Any person who requests an agency record from a system of records triggers the Privacy Act. The record custodian must apply the access provision if the requesting person is an individual by whose name or identifier the information was retrieved. Using a broad definition of record, any item retrieved by using the individual's name or identifier would entitle the requester to access unless exempted. If the record custodian concludes that any piece of information, if disclosed, would constitute a clearly unwarranted invasion of another person's privacy, then the agency should not disclose it. The records custodian would rely on the Supreme Court principles in *Reporters Committee*[212] to properly analyze whether disclosure would be a clearly unwarranted invasion of privacy. Rather than balancing the interests and then trying to conform the law to fit the outcome, the balancing of interests would be conducted as part of the Privacy Act analysis.

The Supreme Court's guidance in *Reporters Committee* should control the analysis under the new privacy interest exemption. In *Reporters Committee,* the Supreme Court said, "whether disclosure of a private document . . . is warranted must turn on the nature of the requested document and its relationship to 'the basic purpose of the Freedom of Information Act to open agency action to the light of public scrutiny.'"[213] Following the reasoning in *Reporters Committee,* an agency would balance the nature of the requested information containing a third party's privacy interest against the basic purpose of the Privacy Act's access provision. In short, if the item's relationship to a core purpose behind the access right outweighs the privacy interest, then the requester should gain access. If the privacy interest outweighs the relationship the item has to a core purpose of the access right, then the information should be exempted.[214] In order to properly guide a records custodian, one must articulate the core purposes of access.

---

211. Since Congress set such a high standard for an exemption, the new Privacy Act exemption should follow FOIA Exemption 6 rather than 7(C) because Exemption 6 requires a higher level of invasion before the exemption prevents release. *Compare* 5 U.S.C. § 552(b)(6) (2006) ("would constitute a clearly unwarranted invasion of privacy"), *with* 5 U.S.C. § 552 (b)(7)(C) (2006) ("could reasonably be expected to constitute an unwarranted invasion of privacy").

212. *Reporters Comm. for Freedom of the Press*, 489 U.S. at 772.

213. *Id.* at 772 (quoting Dept. of Air Force v. Ross, 425 U.S. 352 at 372 (1976)).

214. *Id.* (explaining that in the event a subject requester is exempted, the agency would then treat the request as a FOIA requests and conduct an Exemption 6 or 7(C) analysis, but the balance would be against the FOIA basic purpose).

The Privacy Act itself states its general purposes: "The purpose of this Act is to provide certain safeguards for an individual against an invasion of personal privacy by requiring government agencies" to: (1) prevent disclosure and (2) permit access . . . .[215] Recall the core purposes of the access rule contained in the Senate and House reports pertaining to their respective original bills:[216]

> (1) Protecting the access requester from invasion of privacy by letting him into his own file to see if information was improperly disclosed;
> (2) Discovering the existence of a government record;
> (3) Insuring accuracy of the information in a government record;
> (4) Mutuality;
> (5) Disarming hostility;
> (6) Insuring accuracy, relevance, timeliness, and completeness as related to making decisions;
> (7) Ensuring fair treatment.[217]

E. The Procedural Application of the Third Party Exemption

Using FOIA Exemption 6 and *Reporters Committee* as the substantive model, the new exemption will require a records custodian to balance the core access purposes of the Privacy Act against the third party's personal privacy interest.[218] Using this model, a Privacy Act officer can similarly approach the third party information exemption. The Privacy Act record custodian would follow these steps when a request triggers the Privacy Act access rule.

---

215. The Privacy Act of 1974, Pub. L. No. 93-579, 88 Stat. 1896 §§ 2(B)(1), (3).

216. *See* SOURCE BOOK, s*upra* note 23, at 173 (revealing the Senate's access purposes: "[F]ull protection against abuses of the power of government" requires the individual to have a "right to discover if he is subject of a government file," and if so, to access it in order to "assure the accuracy of it and to determine whether there has been improper disclosure." Further, it is a "desirable adjunct" to insure accuracy, and "objections [to access] . . . are inconsistent with the principle of mutuality necessary for fair information practice." *Id.* at 173–74. Additionally, "rights of access and challenge" disarm hostility and guarantee accuracy through "individual self interest." *Id.* at 174). *See also id.* at 308 (revealing the House of Representatives purposes: "The committee believes that this [access] provision is essential to achiev[ing] . . . important objective[s] of the legislation: Ensuring that individuals know what Federal records are maintained about them and have the opportunity to correct those records. . . [and] maintaining accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to individuals in making determinations about them. The constant vigilance of individual citizens backed by legal redress is the best means, in Committee's opinion, of making certain that government treats people fairly.").

217. *Id.*

218. U.S. DEP'T OF JUSTICE, FOIA Counselor, *Exemption 6 and Exemption 7(c): Step-by-Step Decisionmaking*, Vol. X, No. 2, at 7 (Spring 1989), *available at* http://www.justice.gov/oip/foia_updates/Vol_X_2/page4.html. (The Dep't of Justice suggests a step-by-step analysis to the FOIA privacy exemptions in light of *Reporters Committee* which could also apply to the new Privacy Act exemption.).

Step One: Assuming the "Privacy Act" is triggered, does the access rule apply?[219] If it does, then proceed to step two. If it does not, then do not disclose.[220]

Step two: Is there a personal privacy interest of a third party involved? If not, then disclose unless otherwise exempted. If there is a privacy interest, proceed to step three.

Step three: Is the private information related to a core purpose of access? If not, then do not disclose under the new third party privacy exemption. If it is related, then proceed to step four.[221]

Step four: Balance the third party privacy interest against the relationship the requested item has to the core access purposes. The balancing process would require the custodian to balance the relative interests. The information should be disclosed to the requester unless the type of invasion is clearly unwarranted and more substantial than the benefit to access.

F. Reconsidering Voelker and DePlanche While Applying the New Exemption

Reconsidering *Voelker* and *DePlanche* under the new model would achieve the same results but under an intellectually honest analysis. Mr. Voelker and Mr. DePlanche both requested their government files retrieved by their names or identifiers satisfying step one. Both cases had a third party privacy interest at stake. In *Voelker*, it was something contained in an investigation report and in *DePlanche*, it was the location of his children. Whether the information is related to a core purpose of access is where the cases would diverge. Mr. Voelker's request arguably satisfies a majority of them, whereas Mr. DePlanche's request arguably satisfies none of them. Under step three, DePlanche would be exempted, but Voelker would move on to step four. Finally, under step four, a court could overtly strike the balance between Mr. Voelker's access purposes and the privacy interest. The same result would occur in both cases, but there would be no need for judicial gerrymandering. Suppose that Mr. DePlanche could establish a core access purpose in knowing

---

219. See 5 U.S.C. § 552a(d)(1) (2006) for rules governing access.

220. Craig D. Feiser, *Privatization and the Freedom of Information Act: An Analysis of Public Access to Private Entities under Federal Law,* FED. COMM. L.J., 1999–2000, at 21, 61–62. As a corollary to the new exemption, the definition of record should be uniformly construed as broadly as possible. Otherwise, courts could still sidestep the Privacy Act by applying the "records approach" with a narrow definition.

221. *See* U.S. Dep't of Justice v. Reporters Comm. For Freedom of the Press, 489 U.S. 749, 775 (1989). It can be argued that there are so many core purposes to access that this step will always be satisfied by the access requester as compared to FOIA, which according to *Reporters Committee*, has only one core purpose of shedding light on how the government operates. If such is the case, then the record custodian would easily pass through step three into the balancing of step four. It would still have the effect of screening access requesters totally outside the realm of legitimate access requests.

the address of his children. Under the balancing test of step four, he would still likely lose as the privacy interest in the address is arguably weightier.

G. Reconsidering Sussman applying the new exemption

In *Sussman*, the D.C Circuit Court of Appeals did not reveal the substance of the withheld information or how it was retrieved making the ultimate result under the new exemption uncertain. However, the new exemption analysis would be sound and avoid the stark conflict of statutory interpretation between circuits created by trying to grapple with the privacy interest gap.[222] If the information was not retrieved by Sussman's name, then the first prong would not be satisfied and the access right would not be triggered. But if either Sussman's name or both Sussman's and Maydak's names were used, then apply a standard broad definition of record and proceed to prong two—is there a Maydak privacy interest? If not, then release to Sussman, but if there is proceed to prong three—is the information related to core purposes of the Privacy Act? If not, then do not release, but if there is, proceed to prong four and balance the relative privacy interest of Maydak against the core purpose for releasing to Sussman. In the end, the result would be a consistent application of law and avoidance of conflicting approaches and statutory interpretation.

CONCLUSION

A person's privacy has always been relative to technology. The law must keep pace with the new instruments of invasion. In 1890, Warren and Brandeis pointed to flash photography as the new threat.[223] The Supreme Court tried to adapt the plain meaning of the Fourth Amendment in 1928 to wiretapping, but then reversed itself thirty-nine years later.[224] The Internet and information age present new threats to privacy in general. Congress tried to get ahead of this when it enacted the Privacy Act at the dawn of this age, but the threats have now gained the upper hand.

---

222. *Compare Voelker* v. IRS, 646 F.2d 332, 333 (8th Cir. 1981) (The statute "clearly states that an individual is entitled to his record, as well as to other information that pertains to him."), *with* Sussman v. U.S. Marshals Serv., 494 F.3d 1106, 1121 (D.C. Cir. 2007) ("[W]e interpret 5 U.S.C. § 552a(d)(1) to give parties access only to their own records, not to all information pertaining to them that happens to be contained in a system of records.").

223. Warren & Brandeis, *supra* note 2, at 195.

224. Olmstead v. United States, 277 U.S. 438, 466 (1928) (holding that government surveillance by wiretapping the defendant's home telephone did not amount to a search or seizure within the meaning of the Fourth Amendment because there was no physical trespass onto the defendant's property), *overruled by* Katz v. United States, 389 U.S. 347, 352-53 (1967) (holding that the Fourth Amendment protects people not places), and Berger v. New York, 388 U.S. 41, 62–64 (1967). *See also*, United States v. Jones, 132 S. Ct. 945 (2012) (holding that the government's attachment of a GPS devise to a vehicle constitutes a search or seizure within the meaning the Fourth Amendment because it is a trespass on an effect).

The Privacy Act, along with other congressional and executive laws, stopped many government agency abuses, but in the process left a gaping hole, plainly visible now that government overreaching has settled down. The gap regarding third party privacy presents itself as citizens exercise their access rights and agencies confront the issue of mixed personal information in the same agency record. The courts' attempts to bridge the gap has left a legacy of confusing case law. Agencies have likewise drafted confusing regulations based on the case law. The wide range of results and constant litigation over the right of access versus the right of privacy clearly show that the time has come to confront the issue. The problem should be handed back to Congress because the current gap in the Privacy Act does not lend itself to a judicial cure.

Only a new exemption will fix the problem. The proposed new exemption will bypass the semantics and proceed directly to the real issue: citizen A's right to access or citizen B's right to privacy. The courts will not have to grope for rationale that is not available. The agencies and courts can better assess the issue in the open applying a known and quantifiable balancing test. This will lead to a measure of consistency and a better body of case law. Courts will make better and more predictable law based on the proposed balancing exemption finally reflecting the true public policy behind the Privacy Act—the protection of privacy.