



UNITED STATES DEPARTMENT OF JUSTICE OVERVIEW OF THE PRIVACY ACT OF 1974

2020 Edition

Preface

The “Overview of the Privacy Act of 1974,” prepared by the Department of Justice’s Office of Privacy and Civil Liberties (OPCL), constitutes a discussion of various provisions of the Privacy Act, as addressed by court decisions in cases involving the Act’s disclosure prohibition, its access and amendment provisions, and its agency recordkeeping requirements. Tracking the provisions of the Act itself, the Overview provides reference to and legal analysis of court decisions interpreting the Act. It is a comprehensive -- but not exhaustive -- resource that describes the current state of the law.

The Overview is not intended to provide policy guidance or create policy, as that role statutorily rests with the Office of Management and Budget (OMB), and where OMB has issued policy guidance on particular provisions of the Act, citation to such guidance is provided in the Overview. The 2020 edition of the Overview includes cases through April of 2020. It was published electronically in October 2020 and sent for print publication in November 2020. The online version will be a living document, and updated by OPCL in its discretion as appropriate.

OPCL is very pleased to provide this updated revision of the Overview, and could not have done so without the commitment of OPCL’s dedicated staff and the interagency Overview Working Group, who are recognized individually on the accompanying masthead. The organization and development of legal materials are the work product of OPCL, which is responsible for the Overview’s content.

Peter A. Winn
Acting Chief Privacy and Civil Liberties Officer
United States Department of Justice

The contents of this publication are not copyrighted and may be freely reprinted. The citation is as follows: U.S. Dep't of Justice, *Overview of the Privacy Act of 1974*, [page number] (2020). The Overview is available to the public in electronic form on OPCL's website: <https://www.justice.gov/opcl/overview-privacy-act-1974-2020-edition>.

UNITED STATES DEPARTMENT OF JUSTICE
THE OVERVIEW OF THE PRIVACY ACT OF 1974

2020 Edition

2015 – 2020
OPCL Directors

Peter A. Winn

*Katherine M. Harman-Stokes**

*Kristi Lane Scott**

Special Advisor & Senior Editor

Margaret O'Herron

OPCL Attorneys

Hannah J. Mayer

Andrew A. Proia

Michelle Ramsden

Brian Young

OPCL Privacy Analysts & Specialists

Jamie Huang

Kiran Natarajan

Andria Robinson-Smith

Michael Terry

2020 Edition Working Group

Michael J. Bujold

Christopher K. Dearing

Victoria M. Garcia

Dorothy Fountain

Samuel L. Haack

David M. Hudson

Sarah Oldfield

Alexander C. Tang

Carrie Weinfeld

Alexander Wood

2020 Edition Contributors

LaBlanche Adopo

Carla Andrews

Khaliah N. Barnes

Beau Braswell

Renee Gewercman

Jennifer Harp

Pamela A. Moye

Jonathan Piggott

Kathleen Wiederman

Nailah Williams

Beth Zelman

2020 Edition OPCL Legal Interns

Akua Abu

Stephanie Benjamini

Jeffrey Brown

Gabrielle Conti

Alexander DeGrado

Kayvan Farchad

Christopher Frascella

Laura Ashley Harris

Wail Jihadi

Kaitlyn Krall

Samuel Mott

Ryan Morrison

Christa Nicols

John O'Gorman

Charity Ogbeide

Eric Pait

Halie Peacher

Danielle Prongay

Ashley Pusey

Rebecca Rechtszaid

Shayan Said

Henry Sales

Daniel Shin

Zachary Silver

Matthew Smith

* Served in acting capacity

UNITED STATES DEPARTMENT OF JUSTICE OVERVIEW OF THE PRIVACY ACT OF 1974

2020 Edition

INTRODUCTION.....	1
A. Legislative History	4
B. Privacy Protection Study Commission	4
C. Office of Management and Budget Guidance.....	4
D. Computer Matching and Privacy Protection Act	7
JUDICIAL REDRESS ACT.....	8
A. Extension of Privacy Act Remedies to Citizens of Designated Countries.....	8
B. Attorney General Designations Related to the U.S.-EU Data Protection and Privacy Agreement	11
1. Covered Countries under the DPPA	12
2. Designated Federal Agency or Component under the DPPA.....	13
DEFINITIONS.....	15
A. 5 U.S.C. § 552a(a)(1) - Agency	15
B. 5 U.S.C. § 552a(a)(2) - Individual.....	22
C. 5 U.S.C. § 552a(a)(3) - Maintain.....	26
D. 5 U.S.C. § 552a(a)(4) - Record	27
1. Broad Definition - Any Record Linked to Individual’s Identifying Information	28
2. Narrow Definition - Record Must Reflect Individual Quality or Characteristic.....	30
3. Middle Ground - Record Must be “About” Individual, But Need Not Reflect Quality or Characteristic	30
E. 5 U.S.C. § 552a(a)(5) - System of Records	37
1. Systems of Records and Disclosures under Subsection (b).....	45
2. Systems of Records and Access and Amendment under Subsections (d)(1) and (d)(2)	57
3. Protections for Records Not Within a System of Records.....	60
CONDITIONS OF DISCLOSURE TO THIRD PARTIES	64
A. The “No Disclosure without Consent” Rule	64
B. Twelve Exceptions to the “No Disclosure without Consent” Rule	80
1. 5 U.S.C. § 552a(b)(1) - Need to Know within Agency.....	80
2. 5 U.S.C. § 552a(b)(2) - Required FOIA Disclosure.....	89
3. 5 U.S.C. § 552a(b)(3) - Routine Uses.....	94
4. 5 U.S.C. § 552a(b)(4) - Bureau of the Census.....	113
5. 5 U.S.C. § 552a(b)(5) - Statistical Research	113
6. 5 U.S.C. § 552a(b)(6) - National Archives.....	114

OVERVIEW OF THE PRIVACY ACT

7. 5 U.S.C. § 552a(b)(7) - Law Enforcement Request	114
8. 5 U.S.C. § 552a(b)(8) - Health or Safety of an Individual	116
9. 5 U.S.C. § 552a(b)(9) - Congress.....	117
10.5 U.S.C. § 552a(b)(10) - Government Accountability Office.....	118
11.5 U.S.C. § 552a(b)(11) - Court Order	118
12.5 U.S.C. § 552a(b)(12) - Debt Collection Act.....	133
ACCOUNTING OF CERTAIN DISCLOSURES	134
INDIVIDUAL’S RIGHT OF ACCESS.....	138
A. The Privacy Act and the FOIA	138
B. FOIA/Privacy Act Interface Examples: Access	141
1. If No Privacy Act Exemption Applies	141
2. If a Privacy Act Exemption Applies.....	142
3. If No Privacy Act Exemption and No FOIA Exemption Apply	142
4. If Both Privacy Act and FOIA Exemptions Apply	143
C. Records Requests and Searches	143
D. Third Party Interests.....	147
INDIVIDUAL’S RIGHT OF AMENDMENT	153
AGENCY REQUIREMENTS.....	155
A. 5 U.S.C. § 552a(e)(1) - Maintain Only Relevant and Necessary Information.....	155
B. 5 U.S.C. § 552a(e)(2) - Collect Information, to the Greatest Extent Practicable, Directly from the Individual	156
C. 5 U.S.C. § 552a(e)(3) - Inform Individuals when Asking to Collect Information.....	162
D. 5 U.S.C. § 552a(e)(4) - Publish System of Records Notice	166
E. 5 U.S.C. § 552a(e)(5) - Maintain Accurate, Relevant, Timely, and Complete Records.....	168
F. 5 U.S.C. § 552a(e)(6) - Review Records Prior to Dissemination	183
G. 5 U.S.C. § 552a(e)(7) - Record Describing the Exercise of Rights Guaranteed by the First Amendment.....	185
H. 5 U.S.C. § 552a(e)(8) - Notice of Court Disclosure	195
I. 5 U.S.C. § 552a(e)(9) - Rules of Conduct	195
J. 5 U.S.C. § 552a(e)(10) - Establish Safeguards	197
K. 5 U.S.C. § 552a(e)(11) - Publish New or Intended Use.....	200
AGENCY RULES.....	201
A. 5 U.S.C. § 552a(f)(1) - Establish Notification Procedures.....	201

OVERVIEW OF THE PRIVACY ACT

B. 5 U.S.C. § 552a(f)(2) - Define Time, Place, and Requirements for Identifying Individuals	201
C. 5 U.S.C. § 552a(f)(3) - Establish Procedures for Disclosure of Records to Individuals	202
D. 5 U.S.C. § 552a(f)(4) - Establish Procedures for Requests and Appeals	204
E. 5 U.S.C. § 552a(f)(5) - Establish Copying Fees.....	205
CIVIL REMEDIES.....	206
A. 5 U.S.C. § 552a(g)(1)(A) - Amendment Lawsuits.....	206
1. Exhaustion of Administrative Remedies.....	206
2. Standard and Scope of Review	210
3. Remedies	220
B. 5 U.S.C. § 552a(g)(1)(B) - Access Lawsuits.....	221
1. Exhaustion of Administrative Remedies.....	222
2. Standard and Scope of Review	227
3. Remedies	230
C. 5 U.S.C. § 552a(g)(1)(C) - Damages Lawsuits for Failure to Assure Fairness in Agency Determination	231
1. Exhaustion of Administrative Remedies.....	232
2. Elements of a Damages Claim	234
3. Standard and Scope of Review	242
D. 5 U.S.C. § 552a(g)(1)(D) - Damages Lawsuits for Failure to Comply with Other Privacy Act Provisions	253
1. Exhaustion of Administrative Remedy	253
2. Elements of a Subsection (g)(1)(D) Claim	254
3. Standard and Scope of Review	262
E. Principles Applicable to Damages Lawsuits	266
1. Intentional or Willful Standard	267
2. Actual Damages	280
3. Limits on Injunctive Relief for Damages Claims.....	286
4. Additional Considerations for Damages Claims	288
F. Principles Applicable to All Privacy Act Civil Actions	289
1. Attorney Fees and Costs.....	299
2. Jurisdiction and Venue	306
3. Statute of Limitations.....	310
4. Jury Trial.....	333
CRIMINAL PENALTIES	335
TEN EXEMPTIONS.....	338
A. 5 U.S.C. § 552a(d)(5) - Special Exemption for Information Compiled for Civil Action.....	338

B. 5 U.S.C. § 552a(j) - Two General Exemptions for Central Intelligence	
Agency and Criminal Law Enforcement	341
1. Law Enforcement Components	342
2. Compiled for Certain Law Enforcement Purposes	344
3. Additional Issues Relating to the Criminal Law Enforcement Exemption	349
C. 5 U.S.C. § 552a(k) - Seven Specific Exemption Rules Agencies May Promulgate	354
1. 5 U.S.C. § 552a(k)(1) - FOIA Exemption 1, Classified Information	355
2. 5 U.S.C. § 552a(k)(2) - Investigative Law Enforcement Materials	356
3. 5 U.S.C. § 552a(k)(3) - Secret Service Records	364
4. 5 U.S.C. § 552a(k)(4) - Statistical Records	366
5. 5 U.S.C. § 552a(k)(5) - Source-Identifying Investigatory Material Compiled for Determining Suitability, Eligibility, or Other Qualification	366
6. 5 U.S.C. § 552a(k)(6) - Testing or Examination Materials	370
7. 5 U.S.C. § 552a(k)(7) - Source-Identifying Armed Services Promotion Material	371
DISCLOSURE OF SOCIAL SECURITY NUMBER	373
A. Exception for Disclosures Required by Federal Statute	374
B. Exception for Laws and Regulations in Effect before January 1, 1975	376
C. Federal, State, and Local Government Notice Requirements	376
D. Causes of Action	378
GOVERNMENT CONTRACTORS	382
MAILING LISTS	384
ARCHIVAL RECORDS AND NEW SYSTEMS AND MATCHING PROVISIONS	385
TEXT OF THE PRIVACY ACT OF 1974, AS AMENDED	386

INTRODUCTION

The Privacy Act of 1974, Pub Law No. 93-579, 88 Stat 1896 (Dec. 31, 1974), codified at 5 U.S.C. § 552a (2018), went into effect on September 27, 1975, when it became the principal law governing the handling of personal information in the federal government. Enacted in the wake of the Watergate and the Counterintelligence Program (COINTELPRO) scandals involving illegal surveillance on opposition political parties and individuals deemed to be “subversive,” the Privacy Act sought to restore trust in government and to address what at the time was seen as an existential threat to American democracy. In the words of the bill’s principal sponsor, Judiciary Chairman Senator Sam Ervin, “[i]f we have learned anything in this last year of Watergate, it is that there must be limits upon what the Government can know about each of its citizens.” See S. Comm. on Gov’t. Operations & H.R. Comm. on Gov’t. Operations, 94th Cong., Legislative History of the Privacy Act of 1974 S. 3418 (Public Law 93-579): Source Book on Privacy at 4 (Comm. Print 1976) [hereinafter Source Book], https://www.justice.gov/opcl/paoverview_sourcebook.

In drafting the Privacy Act, Congress relied on a recently published and widely read report from an advisory committee of what was then the Department of Health, Education & Welfare (HEW). Records, Computers, and the Rights of Citizens: Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, DHEW Publication No. (OS) 73-94 (July 1973) (hereinafter HEW Report), <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>. The HEW Report represented the first comprehensive study of the risks to privacy presented by the increasingly widespread use of electronic information technologies by organizations, replacing traditional paper-based systems of creation, storage, and retrieval of information. To address these risks, the HEW Report developed what it called a “code of fair information practices,” now more commonly called the Fair Information Practice Principles, or FIPPs.

As implemented in the Privacy Act, the FIPPs: allow individuals to determine what records pertaining to them are collected, maintained, used, or disseminated by an agency; require agencies to procure consent before records pertaining to an individual collected for one purpose could be used for other incompatible purposes; afford individuals a right of access to records pertaining to them and to have them corrected if inaccurate; and require agencies to collect such records only for lawful and authorized purposes and safeguard them appropriately. Exceptions from some of these principles are permitted only for important reasons of public policy. Judicial redress is afforded to individuals when an agency fails to comply with access and amendment rights, but only after an internal appeals process fails to correct the problem. Otherwise, liability for damages is afforded in the event of a willful or intentional violation of these rights.

The FIPPs are not only central to the framework of the Privacy Act, they have been the basis of almost every other privacy law and treaty in the world today. See, e.g.,

Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of Natural Persons with Regard to the Processing of Personal Data and on the Free Movement of Such Data (known as the General Data Protection Regulation (“GDPR”)); The Gramm-Leach-Bliley Act, 15 U.S.C. § 6801; The Health Insurance Portability and Accountability Act (“HIPAA”) of 1996, 42 U.S.C. § 320d-2; HIPAA Privacy Rule, 45 CFR Part 160 and Subparts A and E of Part 164; Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 (repealed and replaced by the GDPR); Org. for Econ. Coop. & Dev., Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (rev. 2013). It is therefore helpful to understand something about their origins.

The FIPPs were the brainchild of three people, the HEW Secretary’s Advisory Committee Chairman Willis Ware, Executive Director David B. H. Martin, and Associate Director Carole Parsons. Chairman Ware was a legendary computer scientist and pioneer in the field of information security who had worked with John Von Neumann and Claude Shannon building the first modern computer at the Institute for Advanced Study at Princeton. Chairman Ware later diagnosed fundamental vulnerabilities in what was then called the ARPANET (now renamed INTERNET), and is recognized as the founder of the field of information security. Executive Director Martin was the principal architect of the Cape Cod National Seashore, a multi-stakeholder collaborative governance structure, which became the model for the National Environmental Policy Act of 1970. Executive Director Martin would go on to devise other innovative collaborative governance frameworks like government-backed student loans. Associate Director Parsons was a National Research Council expert on government administrative and scientific uses of recorded personal information. She later served in the White House overseeing the legislative process leading to the enactment of the Privacy Act, and as Executive Director of the Privacy Protection Study Commission.

As explained by the authors of the HEW Report, underlying the FIPPs was an understanding of the nature of electronic data as reflecting and mediating relationships in which both individuals and organizations have an interest, made for purposes that are shared by organizations and individuals. The concept of privacy had, at that point in time, been understood as a narrow, property-based concept of individual control. Unlike paper-based information systems, individuals cannot exercise the same level of physical control of information in electronic computer systems controlled by organizations. Accordingly, the authors of the HEW Report argued that the concept of privacy needed to be reimagined to recognize the mutual interests that institutions and individuals shared in the fair and appropriate management of personal information. This meant that instead of a property-based concept of individual control, what was needed was a governance framework designed to ensure the trust of the stakeholders in the information. These included

the individuals about whom the information pertained and the agency with a public need to use the information, as well as others. As such, the model of the FIPPs developed in the HEW Report bears close similarities to the framework for management of shared common environmental resources, such as the Cape Cod National Seashore, which Executive Director Martin had helped design.

As implemented in the Privacy Act, the multi-stakeholder governance idea underlying the FIPPs can be seen in the fact that each of the individual rights that Congress created also serves the interests of any reasonable agency, and is consistent with the need for other legitimate secondary users, such as public health authorities, financial oversight agencies, law enforcement and national security agencies—indeed any stakeholder with a legitimate need to use the information in the public interest—to access and appropriately use the information. Just as loss of trust in the governance framework would harm the interests of all, so proper and appropriate use of personal information within a secure governance framework would maintain trust and benefit the interests of all.

The Ninety-Third United States Congress, facing a crisis of public trust, found the information governance model of the FIPPs, as presented in the HEW Report, to be an attractive approach. Following the breakdown of trust in the government after the Watergate and COINTELPRO scandals, Congress recognized that agency implementation of the FIPPs could help restore the most critical relationship of trust of all, that between the people and their government.

In the more than 45 years since the Privacy Act was enacted, information technologies have expanded in ways that the drafters of the HEW Report could never have imagined, and the risks associated with the collection and use of personal data have grown accordingly. But the basic principles of fair information practices as implemented in the Act have continued to do their work maintaining the relationship of trust between the people and their government. The Privacy Act was later modified by the Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, 102 Stat. 2507, extending the Privacy Act's FIPPs-based protections to computer-matching activities by agencies, with requirements for certain additional internal agency procedures. The Privacy Act also has been supplemented by other structures of information governance, such as the E-Government Act of 2002, Pub. Law No. 107-347, 116 Stat. 2899, and the Federal Information Security Modernization Act of 2014, Pub. Law No. 113-283, 128 Stat. 3073. However, the original language of the Privacy Act, as drafted in 1974, has shown itself sufficiently flexible to adapt to those changes. More than any other law in the field, the Privacy Act has, to a remarkable extent, withstood the test of time.

A. Legislative History

Although the HEW Report provides key historical context for the Privacy Act, the formal legislative history of the Privacy Act is contained in a convenient, one-volume compilation. See Source Book, https://www.justice.gov/opcl/paoverview_sourcebook. The Act was passed in great haste during the final week of the Ninety-Third United States Congress. No conference committee was convened to reconcile differences in the bills passed by the House and Senate. Instead, staffs of the respective committees – led by Senators Ervin and Percy, and Representatives Moorhead and Erlenborn – prepared a final version of the bill that was ultimately enacted. The original reports are thus of limited utility in interpreting the final statute; the more reliable legislative history consists of a brief analysis of the compromise amendments – entitled “Analysis of House and Senate Compromise Amendments to the Federal Privacy Act” – prepared by the staffs of the counterpart Senate and House committees and submitted in both the House and Senate in lieu of a conference report. See 120 Cong. Rec. at 40, 405-09, 40,881-83, (1974), reprinted in Source Book, at 858-68, 987-94, https://www.justice.gov/opcl/paoverview_sourcebook.

B. Privacy Protection Study Commission

Section 5 of the original Privacy Act established the “Privacy Protection Study Commission” to evaluate the statute and to issue a report containing recommendations for its improvement. See U.S. Priv. Prot. Study Comm’n, Personal Privacy in an Information Society (1977) [hereinafter Privacy Commission Report], https://www.justice.gov/paoverview_ppsc. Although the Commission generated many ideas and discussions and issued its final report in 1977, it ceased operation that year and its recommendations did not result in further legislation. See generally Doe v. Chao, 540 U.S. 615, 622-23 (2004) (considering mandate and recommendation of Privacy Protection Study Commission as well as legislative history to interpret Privacy Act damages provision).

C. Office of Management and Budget Guidance

“The Director of the Office of Management and Budget shall—

(1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and

(2) provide continuing assistance to and oversight of the implementation of this section by agencies.” 5 U.S.C. § 552a(v).

Comment:

The vast majority of Privacy Act guidelines and regulations are published in the Executive Office of the President’s Office of Management and Budget (“OMB”) 1975 memorandum. Off. of Mgmt. & Budget, Exec. Off. of the President, Privacy Act Implementation: Guidelines and Responsibilities, 40 Fed. Reg. 28,948, 949 (July 9, 1975) [hereinafter OMB 1975 Guidelines], <https://www.justice.gov/paoverview omb-75>. OMB has since supplemented and expanded upon the 1975 Privacy Act Guidelines in particular subject areas over the years. *See, e.g.*, Off. of Mgmt. & Budget, Exec. Off. of the President, Implementation of the Privacy Act of 1974 Supplementary Guidance, 40 Fed. Reg. 56,741 (Dec. 4, 1975) [hereinafter OMB Supplementary Guidance], <https://www.justice.gov/paoverview omb-75-supp> (supplementing certain sections of the 1975 Privacy Act Guidelines, including the “system of records” definition, routine use and intra-agency disclosures, consent and Congressional inquiries, accounting of disclosures, amendment appeals, rights of parents and legal guardians, relationship to Freedom of Information Act (FOIA)); Off. of Mgmt. & Budget, Exec. Off. of the President, Guidelines on the Relationship of the Debt Collection Act of 1982 to the Privacy Act of 1974, 48 Fed. Reg. 1,556 (April 11, 1983) [hereinafter OMB Debt Collection Act Guidance], <https://www.justice.gov/paoverview omb-83-dca>; Off. of Mgmt. & Budget, Exec. Off. of the President, Guidance on the Privacy Act Implication of “Call Detail” Programs to Manage Employees’ Use of the Government’s Telecommunications Systems, 52 Fed. Reg. 12,990 (April 20, 1987) [hereinafter OMB Call Detail Guidance], <https://www.justice.gov/paoverview omb-87-cd>; Off. of Mgmt. & Budget, Exec. Off. of the President, Final Guidance Interpreting the Provisions of Public Law 100-503, the Computer Matching and Privacy Protection Act of 1988, 54 Fed. Reg. 25,818 (June 19, 1989) [hereinafter OMB 1989 Guidelines], <https://www.justice.gov/paoverview omb-89-cma>; Off. of Mgmt. & Budget, Exec. Off. of the President, The Computer Matching and Privacy Protection Amendments of 1990 and The Privacy Act of 1974, 56 Fed. Reg. 18,599 (Apr. 23, 1991) [hereinafter OMB CMPPA Guidelines], <https://www.justice.gov/paoverview omb-91-cma>; *see also* Off. of Mgmt. & Budget, Exec. Off. of the President, OMB Circular No. A-130, Managing Information as a Strategic Resource (July 28, 2016) (notice of availability published at 81 Fed. Reg. 49,689) [hereinafter OMB Circular A-130], <https://www.justice.gov/paoverview omb-a-130> (establishing agency responsibilities for managing personally identifiable information); Off. of Mgmt. & Budget, Exec. Off. of the President, OMB Circular No. A-108, Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act

(Dec. 23, 2016) (notice of availability published at 81 Fed. Reg. 94,424) [hereinafter OMB Circular A-108], https://www.justice.gov/paoverview_omb-a-108 (establishes general reporting requirements for the Privacy Act).

Most courts give the OMB guidelines and regulations the same deference they give interpretations of an agency that has been charged with the administration of a statute. See Sussman v. Marshals Serv., 494 F.3d 1106, 1120 (D.C. Cir. 2007). In Sussman, the Court of Appeals for the District of Columbia Circuit discussed this standard: “Congress explicitly tasked the OMB with promulgating guidelines for implementing the Privacy Act, and we therefore give the OMB Guidelines ‘the deference usually accorded interpretation of a statute by the agency charged with its administration.’” Id. (citation omitted) (citing Albright v. United States, 631 F.2d 915, 920 n.5 (D.C. Cir. 1980)). With regard to the OMB 1975 Guidelines, the court stated: “The OMB apparently invited no public comment prior to publishing its guidelines, and after we decided Albright, Congress pointedly replaced its original grant of authority to the OMB with one that expressly required the OMB to respect such procedural niceties before its guidelines could be binding. But Congress made clear the change was not meant to disturb existing guidelines. Hence, the old OMB Guidelines still deserve the same level of deference they enjoyed prior to the 1998 amendment.” Sussman, 494 F.3d at 1120 n.8 (citations omitted). Numerous cases have applied this standard of deference. See, e.g., Maydak v. United States, 363 F.3d 512, 518 (D.C. Cir. 2004); Henke v. Commerce, 83 F.3d 1453, 1460 n.12 (D.C. Cir. 1996); Quinn v. Stone, 978 F.2d 126, 133 (3d Cir. 1992); Baker v. Navy, 814 F.2d 1381, 1383 (9th Cir. 1987); Perry v. FBI, 759 F.2d 1271, 1276 n.7 (7th Cir. 1985), rev’d en banc on other grounds, 781 F.2d 1294 (7th Cir. 1986); Bartel v. FAA, 725 F.2d 1403, 1408 n.9 (D.C. Cir. 1984); Smiertka v. Treasury, 604 F.2d 698, 703 n.12 (D.C. Cir. 1979); Whitaker v. CIA, 31 F. Supp. 3d 23, 47-48 (D.D.C. 2014); Rogers v. Labor, 607 F. Supp. 697, 700 n.2 (N.D. Cal. 1985); Sanchez v. United States, 3 Gov’t Disclosure Serv. (P-H) ¶ 83,116, at 83,709 (S.D. Tex. Sept. 10, 1982); Golliher v. USPS, 3 Gov’t Disclosure Serv. (P-H) ¶ 83,114, at 83,703 (N.D. Ohio June 10, 1982); Greene v. VA, No. C-76-461-S, slip op. at 6-7 (M.D.N.C. July 3, 1978); Daniels v. FCC, No. 77-5011, slip op. at 8-9 (D.S.D. Mar. 15, 1978); see also Martin v. Office of Special Counsel, 819 F.2d 1181, 1188 (D.C. Cir. 1987) (OMB interpretation is “worthy of our attention and solicitude.”).

The United States Supreme Court has not gone that far, however. See Doe v. Chao, 540 U.S. at 620 n.11 (disagreeing with dissent’s reliance on OMB interpretation of damages provision and stating that Court does “not find its unelaborated conclusion persuasive”). In addition, a few courts have rejected particular aspects of the OMB guidelines and regulations as inconsistent with the statute. See Wrocklage v. DHS, 769 F.3d 1363, 1368-69 (Fed. Cir. 2014)

(interpreting when records are “disclosed”); Scarborough v. Harvey, 493 F. Supp. 2d 1, 13-14 n.28 (D.D.C. 2007) (personal/entrepreneurial distinction); Henke v. Commerce, No. 94-0189, 1996 WL 692020, at *2-3 (D.D.C. Aug. 19, 1994) (same), aff’d on other grounds, 83 F.3d 1445 (D.C. Cir. 1996); Kassel v. VA, No. 87-217-S, slip op. at 24-25 (D.N.H. Mar. 30, 1992) (subsection (e)(3)); Saunders v. Schweiker, 508 F. Supp. 305, 309 (W.D.N.Y. 1981) (same); Metadure Corp. v. United States, 490 F. Supp. 1368, 1373-74 (S.D.N.Y. 1980) (subsection (a)(2)); Fla. Med. Ass’n v. HEW, 479 F. Supp. 1291, 1307-11 (M.D. Fla. 1979) (same); Zeller v. United States, 467 F. Supp. 487, 497-99 (E.D.N.Y. 1979) (same).

D. Computer Matching and Privacy Protection Act

The Computer Matching and Privacy Protection Act of 1988 amended the Privacy Act to add several new provisions. See 5 U.S.C. § 552a(a)(8)-(13), (e)(12), (o), (p), (q), (r), (u) (2018). These provisions add procedural requirements for agencies to follow when engaging in computer-matching activities, provide matching subjects with opportunities to receive notice and to refute adverse information before having a benefit denied or terminated, and require that agencies engaged in matching activities to establish Data Protection Boards to oversee those activities. These provisions became effective on December 31, 1989. OMB’s guidelines on computer matching should be consulted in this area. See, e.g., OMB 1989 Guidelines, 54 Fed. Reg. at 25,818-29, https://www.justice.gov/paoverview_omb-89-cma. Subsequently, Congress enacted the Computer Matching and Privacy Protection Amendments of 1990, Pub. L. No. 101-508 §7201, 104 Stat. 1388, 1388-334, which further clarified the due process provisions found in subsection (p). See also OMB CMPPA Guidelines, 56 Fed. Reg. at 18,599, https://www.justice.gov/paoverview_omb-91-cma. Although there has not been significant litigation on this provision to date, in one recent case, the court considered the requirements of the computer matching amendments and concluded that the agency had not met them. See Calvillo Manriquez v. DeVos, 345 F. Supp. 3d 1077, 1098 (N.D. Cal. 2018) (concluding that because sharing of data between the SSA and the Dep’t of Educ. was “a matching program as defined by the Privacy Act, the agencies must comply with the requirements. . . [and] [i]t is undisputed that the [agency and SSA] did not comply with the requirements above and thus violated the Privacy Act”).

The highly complex and specialized provisions of the Computer Matching and Privacy Protection Act of 1988 and the Computer Matching and Privacy Protection Amendments of 1990 are not further addressed herein. Additional guidance on these provisions can be found in the OMB 1989 Guidelines and OMB CMPPA Guidelines, cited above.

JUDICIAL REDRESS ACT

In 2016, the Congress enacted and the President signed the Judicial Redress Act of 2015. 5 U.S.C. § 552a note (2018). Section 2 of the Judicial Redress Act extends the right to pursue certain civil remedies under the Privacy Act to citizens of designated foreign countries or regional economic organizations. It provides in pertinent part:

(a) CIVIL ACTION; CIVIL REMEDIES. – With respect to covered records, a covered person may bring a civil action against an agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to records under –

(1) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and

(2) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.

(b) EXCLUSIVE REMEDIES. – The remedies set forth in subsection (a) are the exclusive remedies available to a covered person under this section.

(c) APPLICATION OF THE PRIVACY ACT WITH RESPECT TO A COVERED PERSON. – For purposes of a civil action described in subsection (a), a covered person shall have the same rights, and be subject to the same limitations, including exemptions and exceptions, as an individual has and is subject to under section 552a of title 5, United States Code, when pursuing the civil remedies described in paragraphs (1) and (2) of subsection (a).” Section 2 of the Judicial Redress Act of 2015, 5 U.S.C. § 552a note (2018).

A. Extension of Privacy Act Remedies to Citizens of Designated Countries

Comment:

The Judicial Redress Act extends the right to pursue certain civil remedies under the Privacy Act to citizens of designated foreign countries or regional economic organizations.

The Judicial Redress Act extends certain rights of judicial redress established under the Privacy Act to citizens of designated foreign countries or regional

economic organizations, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to: (1) intentional or willful unlawful disclosures of a covered record under subsection (g)(1)(D); and (2) improper refusal by a designated Federal agency or component to grant a covered person access to or amendment of a covered record under subsection (g)(1)(A) & (B). For more information on judicial redress rights under the Privacy Act, see “Civil Remedies” subsections below: “5 U.S.C. § 552a(g)(1)(A) - Amendment Lawsuits,” “5 U.S.C. § 552a(g)(1)(B) - Access Lawsuits,” “5 U.S.C. § 552a(g)(1)(C) - Damages Lawsuits for Failure to Assure Fairness in Agency Determination,” “5 U.S.C. § 552a(g)(1)(D) - Damages Lawsuits for Failure to Comply with Other Privacy Act Provisions.”

As described in the House Committee Report on the Judicial Redress Act, the Act was primarily enacted to complement an anticipated agreement between the United States and the European Union (“EU”) harmonizing legal protections of personal information shared between the United States and EU member states for the prevention, investigation, detection, and prosecution of criminal offenses:

For many years, the European Union and many of its member states have complained to U.S. officials about the fact that the Privacy Act of 1974 only applies to U.S. citizens and lawful permanent residents, and not to foreign citizens. Although other U.S. laws provide any person with judicial remedies for specified types of privacy violations, the absence of a broader right of action with respect to privacy violations by the Federal Government has remained a point of friction with the European Union. Complaints have accelerated as it has become possible, due to digitalization of the economy, and indeed necessary for public security reasons, for U.S. and EU law enforcement agencies to exchange increasing quantities of information. In contrast to the Privacy Act, U.S. citizens have rights under EU and member state data protection laws to challenge adverse decisions by European government agencies in court.

...

[T]he United States has been in the process of negotiating a Data Protection and Privacy Agreement (DPPA, often referred to as the “umbrella agreement”) with the European Union, in order to address the EU desire for clear standards governing the privacy of personal information exchanged for law enforcement purposes. The United States entered into these negotiations in order to ensure that robust information sharing with Europe for law enforcement purposes will continue. During the course of the negotiations, the

European Commission and Parliament have both made it clear that there will be no agreement without the enactment of a U.S. law that enables EU citizens to sue the U.S. government for major privacy violations.

H.R. Rep. No. 114-294, at 2-3 (2015) (Judicial Redress Act).

The District Court for the District of Columbia has exclusive jurisdiction over claims arising under the Judicial Redress Act.

Unlike the Privacy Act's jurisdictional provisions for its civil remedies, the United States District Court for the District of Columbia has exclusive jurisdiction over any claim arising under the Judicial Redress Act. § 2(g). Currently, the D.C. District Court has not substantively interpreted the provisions in the Judicial Redress Act. As a result, the text of the Act, its legislative history, and the Attorney General's designations serve as the best source material for interpreting the Judicial Redress Act.

The Judicial Redress Act applies to citizens of "covered countries," so designated by the Attorney General.

The Judicial Redress Act affords "covered persons" – defined as natural persons (other than an "individual" as defined under the Privacy Act) who are citizens of a covered country – with civil remedies as provided for in the Act. § 2(h)(3). A "covered country" is a country or regional economic integration organization, or member country of such organization, that has been designated by the Attorney General, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, to have met certain protections outlined in Section 2(d)(1) of the Judicial Redress Act. Id. § 2(h)(5).

Civil remedies under the Judicial Redress Act are limited to claims involving "covered records."

The Judicial Redress Act's civil remedies are limited to a "covered record," id. § 2(a), which, for a covered person, has the same meaning as a "record" under the Privacy Act (see subsection for "5 U.S.C. 552a(a)(4) - Record" in "Definitions" below), once the covered record is transferred – (A) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and (B) to "a designated Federal agency or component" for purposes of preventing, investigating, detecting, or prosecuting criminal offenses. Id. § 2(h)(4). A covered person's right to access or amend a covered

record is limited to only those covered records maintained by a designated Federal agency or component. See id. § 2(a).

The Attorney General is responsible for designating Federal agencies and components for purposes of the Judicial Redress Act.

The Attorney General determines that an agency or component of an agency is a “designated Federal agency or component” if: (1) the information exchanged by such agency, or component thereof, with a covered country is within the scope of an agreement with the United States that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses; or (2) designating such agency, or component thereof, is in the law enforcement interests of the United States. Id. § 2(e), (h)(5).

B. Attorney General Designations Related to the U.S.-EU Data Protection and Privacy Agreement

Comment:

The Data Protection and Privacy Agreement between the United States and the European Union and its Member States, provides privacy protections for information shared to prevent, investigate, detect, or prosecute criminal offenses.

As referenced in the House Committee Report, the U.S. Government’s efforts to enact the Judicial Redress Act were, in part, a response to negotiations of an Executive Agreement between the United States and the EU relating to privacy protections for personal information transferred between the U.S., the EU, and the EU Member States for the prevention, detection, investigation, or prosecution of criminal offenses – commonly known as the “Data Protection and Privacy Agreement” (“DPPA”) or the “Umbrella Agreement.” See Agreement on the Protection of Personal Information Relating to the Prevention, Investigation, Detection, and Prosecution of Criminal Offenses, U.S.-EU, June 2, 2016, 17 U.S.T. 201, https://www.justice.gov/us-eu_dppa.

The DPPA went into force on February 1, 2017, and established a set of protections that the United States and the EU must apply to personal information exchanged for the purpose of preventing, detecting, investigating, or prosecuting criminal offenses. The DPPA establishes an obligation for the United States and the EU to provide, in their respective domestic laws, specific judicial redress rights to each other’s citizens. Id. at Art. 19. The Judicial Redress Act is implementing legislation for Article 19 of the DPPA.

1. Covered Countries under the DPPA

Following the approval of the DPPA, the Attorney General designated 26 countries and one regional economic integration organization as “covered countries.”

On January 17, 2017, the Attorney General designated 26 countries and one regional economic integration organization as “covered countries” to be effective on February 1, 2017 – the date of entry into force of the DPPA. See Attorney General Order No. 3824-2017, “Judicial Redress Act of 2015; Attorney General Designations,” 82 Fed. Reg. 7860 (Jan. 23, 2017). On February 12, 2019, following notification from the European Commission, the Attorney General designated the United Kingdom as a “covered country,” effective April 1, 2018. See Attorney General Order No. 4381-2019, “Judicial Redress Act of 2015; Attorney General Designations,” 84 Fed. Reg. 3493 (Feb. 12, 2019). Overall, the Attorney General has designated the following regional economic integration organization and countries as “covered counties” for purposes of the DPPA:

- European Union;
- Austria;
- Belgium;
- Bulgaria;
- Croatia;
- Republic of Cyprus;
- Czech Republic;
- Estonia;
- Finland;
- France;
- Germany;
- Greece;
- Hungary;
- Ireland;
- Italy;
- Latvia;
- Lithuania;
- Luxembourg;
- Malta;
- Netherlands;
- Poland;
- Portugal;
- Romania;
- Slovakia;

- Slovenia;
- Spain;
- Sweden;
- United Kingdom.

2. Designated Federal Agency or Component under the DPPA

Following the approval of the DPPA, the Attorney General identified “designated Federal agencies or components.”

On January 17, 2017, the Attorney General designated four Federal agencies and nine Federal agency components as “designated Federal agencies or components,” to be effective on February 1, 2017. See Attorney General Order No. 3824-2017, “Judicial Redress Act of 2015; Attorney General Designations,” 82 Fed. Reg. 7860 (Jan. 23, 2017). The following Federal agencies and all of their respective components are “designated federal agencies”:

- United States Department of Justice;
- United States Department of Homeland Security;
- United States Securities and Exchange Commission;
- United States Commodity Futures Trading Commission.

In addition, the Attorney General designated the following agency components as “designated Federal . . . components”:

- Bureau of Diplomatic Security, United States Department of State;
- Office of the Inspector General, United States Department of State;
- Alcohol and Tobacco Tax and Trade Bureau, United States Department of the Treasury;
- Financial Crimes Enforcement Network, United States Department of the Treasury;
- Internal Revenue Service, Division of Criminal Investigation, United States Department of the Treasury;
- Office of Foreign Assets Control, United States Department of the Treasury;
- Office of the Inspector General, United States Department of the Treasury;
- Office of the Treasury Inspector General for Tax Administration, United States Department of the Treasury;
- Special Inspector General for the Troubled Asset Relief Program, United States Department of the Treasury.

Tracking the provisions of the Privacy Act itself, the Overview analyzes each section of the Act in turn, and provides reference to and legal analysis of court decisions interpreting the Act's provisions.

DEFINITIONS

A. 5 U.S.C. § 552a(a)(1) - Agency

“[T]he term ‘agency’ means any Executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the [federal] Government (including the Executive Office of the President), or any independent regulatory agency.” 5 U.S.C. § 552a(a)(1) (incorporating 5 U.S.C. § 552(f)(1) (2018), which in turn incorporates 5 U.S.C. § 551(1) (2018)).

Comment:

Executive branch agencies, their components, and government-controlled entities are “agencies.”

The Privacy Act – like the Freedom of Information Act (FOIA), 5 U.S.C. § 552 – applies only to a federal Executive Branch “agency,” and it incorporates the FOIA’s definition of “agency.” See OMB 1975 Guidelines, 40 Fed. Reg. 28,950-51, https://www.justice.gov/paoverview_omb-75; 120 Cong. Rec. at 40,408, reprinted in Source Book at 866, https://www.justice.gov/opcl/paoverview_sourcebook (discussing scope of the Act’s “agency” definition and its application to components of agencies, i.e., agencies within agencies). The Privacy Act “is intended to give ‘agency’ its broadest statutory meaning” so records can be transferred between the various offices and components that comprise an agency on a “need-for-the-record basis.” 120 Cong. Rec. at 36,967, reprinted in Source Book at 958, https://www.justice.gov/opcl/paoverview_sourcebook (providing DOJ as example of an “agency” and recognizing propriety of subsection (b)(1) “need to know” disclosures between its various components, e.g., FBI, DEA, and ATF). See also Cloonan v. Holder, 768 F. Supp. 2d 154, 162 (D.D.C. 2011) (“[N]aming components as defendants under the Privacy Act is appropriate since the statute’s plain language is clear that ‘an agency need not be a cabinet-level agency such as the DOJ to be liable.’” (quoting Lair v. Treasury, No. 03 Civ. 827, 2005 WL 645228 (D.D.C. Mar. 21, 2005)); but see Iqbal v. FBI, No. 3:11-cv-369, 2012 WL 2366634, at *4 (M.D. Fla. June 21, 2012) (declining to dismiss “just because the Plaintiff brought his claims against the FBI instead of the Department of Justice”).

The Privacy Act applies to government corporations and government-controlled corporations, and it is intended to apply to establishments like the Postal Service and the Postal Regulatory Commission. See 5 U.S.C. § 552a(a)(1); 120 Cong. Rec. at 40,408, reprinted in Source Book at 866, <https://www.justice.gov/opcl>

[/paoverview_sourcebook](#) (indicating congressional intent for Privacy Act to apply to Postal Service and Postal Rate Commission (later renamed the Postal Regulatory Commission)); NLRB v. USPS, 841 F.2d 141, 144 n.3 (6th Cir. 1988) (Postal Service is an “agency” because it is an “independent establishment of the executive branch”).

Courts may look at the characteristics of establishments to determine whether they are “agencies” under the Privacy Act. See, e.g., Thompson v. State, 400 F. Supp. 2d 1, 21-22 (D.D.C. 2005) (finding Foreign Service Grievance Board to be an “agency” because it “consists of members appointed exclusively by an executive department, administers federal statutes, promulgates regulations, and adjudicates the rights of individuals”). Courts may consider non-federal entities to be “agencies” under the Privacy Act when the non-federal entities operate establishments that are under the supervision and control of federal Executive Branch agencies pursuant to contracts in which the non-federal entities agree to comply with the Act. See Shannon v. Gen. Elec. Co., 812 F. Supp. 308, 313, 315 n.5 (N.D.N.Y. 1993) (“no dispute” that GE falls within definition of “agency” subject to requirements of Privacy Act where, pursuant to contract, it operated Department of Energy-owned lab under supervision, control, and oversight of Department and where by terms of contract GE agreed to comply with Privacy Act).

The White House, federal courts, and entities merely linked to the government are not “agencies.”

With regard to the White House, courts have held that those components of the Executive Office of the President whose sole function is to advise and assist the President are not “agencies” for purposes of the Privacy Act. See, e.g., Alexander v. FBI, 456 F. App’x 1, 2 (D.C. Cir. 2011) (per curiam), aff’d 691 F. Supp. 2d 182 (D.D.C. 2010) (determining case’s prior contrary interpretation, 971 F. Supp. 603, 606-07 (D.D.C. 1997), was “no longer the correct one”); Falwell v. Exec. Office of the President, 113 F. Supp. 2d 967, 968-70 (W.D. Va. 2000). In fact, the Court of Appeals for the District of Columbia Circuit observed that “Congress did not inadvertently omit the Offices of the President and Vice President from the Privacy Act’s disclosure requirements.” Wilson v. Libby, 535 F.3d 697, 708 (D.C. Cir. 2008).

Federal entities outside of the executive branch are not subject to the Act. See, e.g., Hankerson v. U.S. Dep’t of Prob. & Parole, No. 5:13-CV-78, 2014 WL 533495, at *1 (M.D. Ga. Feb. 7, 2014) (federal courts); Goddard v. Whitmer, No. 09-CV-404, 2010 WL 116744, at *2 (E.D. Ky. Jan. 6, 2010) (federal courts); Cobell v. Norton, 157 F. Supp. 2d 82, 86 & n.6 (D.D.C. 2001) (federal district court);

Standley v. DOJ, 835 F.2d 216, 218 (9th Cir. 1987) (grand jury); Hankerson v. United States, 594 F. App'x 608, 609 (11th Cir. 2015) (per curiam) (probation office); Kates v. King, 487 F. App'x 704, 706 (3d Cir. 2012) (per curiam) (probation office); Fuller-Avent v. Prob. Office, 226 F. App'x 1, 2 (D.C. Cir. 2006) (probation office); Schwartz v. DOJ, No. 95-6423, 1996 WL 335757, at *1 (2d Cir. June 6, 1996) (probation office); Morris v. Prob. Servs., 723 F. Supp. 2d 225, 227 (D.D.C. 2010) (probation office); Jackson v. DOJ, No. 09-0846, 2009 WL 5205421, at *4 (D. Minn. Dec. 23, 2009) (probation office); Kyles v. Kaufman, No. 08-4169, 2008 WL 4906141, at *1 (D.S.D. Nov. 14, 2008) (probation office); Harrell v. BOP, No. 99-1619, slip op. at 6 (W.D. Okla. Mar. 5, 2001), aff'd on other grounds sub nom. Harrell v. Fleming, 285 F.3d 1292 (10th Cir. 2002) (probation office); Callwood v. Dep't of Prob. of the V.I., 982 F. Supp. 341, 343 (D.V.I. 1997) (probation office); In re Adair, 212 B.R. 171, 173 (Bankr. N.D. Ga. 1997) (federal bankruptcy court).

Similarly, the Smithsonian Institution, although having many “links” with the federal government, “is not an agency for Privacy Act purposes.” Dong v. Smithsonian Inst., 125 F.3d 877, 879-80 (D.C. Cir. 1997); see also Dodge v. Trs. of Nat'l Gallery of Art, 326 F. Supp. 2d 1, 10-11 (D.D.C. 2004) (finding that “the National Gallery is a Smithsonian Museum” and explaining that “Smithsonian Museums . . . are not subjected to the limitations of the Privacy Act because they do not fall within the definition of an ‘agency’”). Amtrak is another entity with links to the federal government that the courts have held is not an “agency” under the Privacy Act. See United States v. Jackson, 381 F.3d 984, 989-90 (10th Cir. 2004) (citing Ehm, infra and holding that Amtrak is not an “agency”); Ehm v. Nat'l R.R. Passenger Corp., 732 F.2d 1250, 1252-55 (5th Cir. 1984) (Amtrak held not to constitute a “Government-controlled corporation”).

State and local government agencies are not “agencies” under the Privacy Act.

State and local government agencies are not covered by the Privacy Act. See, e.g., Clancy v. Fla. Dep't of Corr., 782 F. App'x 779, 781 (11th Cir. 2019) (finding Interstate Commission for Adult Offender Supervision to be an agency of compacting states that is not subject to Privacy Act); Hatfield v. Berube, 714 F. App'x 99, 105-06 (3rd Cir. 2017); N'Jai v. Pittsburgh Bd. of Public Educ., 487 F. App'x 735, 737 (3d Cir. 2012) (per curiam); Spurlock v. Ashley Cnty., 281 F. App'x 628, 629 (8th Cir. 2008); Schmitt v. City of Detroit, 395 F.3d 327, 331 (6th Cir. 2005); Perez-Santos v. Malave, 23 F. App'x 11, 12 (1st Cir. 2001) (per curiam); Dittman v. California, 191 F.3d 1020, 1026, 1029 (9th Cir. 1999); Nguyen v. Pennsylvania, No. 19-CV-2551, 2019 WL 3423651, at *3 (E.D. Pa. Sept. 28, 2019); Brown v. Kelly, No. 93-5222, 1994 WL 36144, at *1 (D.C. Cir. Jan. 27, 1994) (per curiam); Williams v. City of New York, No. 12 Civ. 8518, 2014 WL 1383661, at *13 (S.D.N.Y. Mar. 26, 2014); Linder v. Friedman, No. 1:12-cv-3051, 2012 WL 6633905,

at *1 (D.S.C. Dec. 20, 2012); Warnock v. City of Canton, S.D., No. 11-4023, 2012 WL 2050734, at *7 (D.S.D. June 7, 2012); Oliver v. Garfield Cnty. Det. Facility, No. CIV-10-1281, 2012 WL 668802, at *3 (W.D. Okla. Feb. 8, 2012); Roggio v. City of Gardner, No. 10-40076, 2011 WL 1303141, at *7 (D. Mass. Mar. 30, 2011); Willis v. DOJ, 581 F. Supp. 2d 57, 67-68 (D.D.C. 2008); Barickman v. Bumgardner, No. 1:07CV134, 2008 WL 2872712, at *3 (N.D. W. Va. July 22, 2008); Fetzer v. Cambria Cnty. Human Servs., 384 F. Supp. 2d 813, 816 (W.D. Pa. 2005); Daniel v. Safir, 175 F. Supp. 2d 474, 481 (E.D.N.Y. 2001) (although characterizing claims as under FOIA, dismissing Privacy Act claims against local agency), aff'd, 42 F. App'x 528 (2d Cir. 2002); Atamian v. Ellis, No. 00-797, 2001 WL 699016, at *3 (D. Del. June 19, 2001), aff'd, 35 F. App'x 356 (3d Cir. 2002) (unpublished table decision); McClain v. DOJ, No. 97 C 0385, 1999 WL 759505, at *2 (N.D. Ill. Sept. 1, 1999), aff'd, 17 F. App'x 471 (7th Cir. 2001); Ferguson v. Ala. Criminal Justice Info. Ctr., 962 F. Supp. 1446, 1446-47 (M.D. Ala. 1997); Connolly v. Beckett, 863 F. Supp. 1379, 1383-84 (D. Colo. 1994); MR by RR v. Lincolnwood Bd. of Educ., Dist. 74, 843 F. Supp. 1236, 1239-40 (N.D. Ill. 1994), aff'd sub nom. Rheinstrom v. Lincolnwood Bd. of Educ., Dist. 74, No. 94-1357, 1995 U.S. App. LEXIS 10781 (7th Cir. May 10, 1995).

Additionally, neither federal funding nor regulation converts state and local entities into covered agencies. See St. Michaels Convalescent Hosp. v. California, 643 F.2d 1369, 1373 (9th Cir. 1981); Logan v. Matveevskii, 57 F. Supp. 3d 234, 275-76 (S.D.N.Y. 2014) (finding federally subsidized housing authorities are not agencies under Privacy Act); Adelman v. Discover Card Servs., 915 F. Supp. 1163, 1166 (D. Utah 1996).

Likewise, the Privacy Act does not apply to tribal entities, the governments of territories or possessions of the United States, or the District of Columbia's government. See 5 U.S.C. § 551(1) (specifically excluding governments of territories or possessions of U.S. and government of D.C. from statutory definition of "agency" incorporated into Privacy Act); Neptune v. Nicholas, No. 1:17-cv-88-GZS, 2017 WL 1102716, at *2 (D. Me. Mar. 24, 2017) (unpublished table decision) (citing Stevens v. Skenandore, 234 F.3d 1274 (7th Cir. 2000)) (finding no right of action against tribal officials under Privacy Act); Williams v. District of Columbia, No. 95CV0936, 1996 WL 422328, at *2-3 (D.D.C. July 19, 1996) (acknowledging Privacy Act does not apply to D.C.). However, the D.C. Circuit has held that National Guard units are within the Privacy Act's definition of "agency" at all times – not just when they are on active federal duty. See In re Sealed Case, 551 F.3d 1047, 1049-50 (D.C. Cir. 2009) (concluding that "Privacy Act's definition of agency includes federally recognized National Guard units at all times" and not solely when unit is on active federal duty). But see Reno v. United States, No. 4-94CIV243, 1995 U.S. Dist. LEXIS 12834, at *6 (W.D.N.C. Aug.

14, 1995) (holding national guard to be state entity in case decided prior to In re Sealed Case).

An exception to the rule that state and local entities are not “agencies” under the Privacy Act, however, is the social security number usage restrictions contained in section 7 of the Privacy Act, which do apply to federal, state, and local government agencies. Pub. L. No. 93-579, § 7, 88 Stat. 1896, 1909 (codified at 5 U.S.C. § 552a note, “Disclosure of Social Security Number”). This special provision is discussed below under “Disclosure of Social Security Number.”

Private entities are not “agencies.”

Private entities are not subject to the Act. See Probert v. Kalamarides, 528 F. App'x 741, 742 (9th Cir. 2013); Johnson v. Mel Foster Co. Ins., 475 F. App'x 640, 640 (8th Cir. 2012) (per curiam); Chimarev v. TD Waterhouse Investor Servs., 99 F. App'x 259, 261-62 (2d Cir. 2004); Sharwell v. Best Buy, No. 00-3206, 2000 WL 1478341, at *2 (6th Cir. Sept. 26, 2000); Sutton v. Providence St. Joseph Med. Ctr., 192 F.3d 826, 844 (9th Cir. 1999); Mitchell v. G.E. Am. Spacenet, No. 96-2624, 1997 WL 226369, at *1 (4th Cir. May 7, 1997); Gilbreath v. Guadalupe Hosp. Found., 5 F.3d 785, 791 (5th Cir. 1993) (per curiam); Gourdine v. Synchrony Bank/Fraud Unit, No. 19-CV-17158, 2019 WL 5558832, at *2 (D.N.J. Oct. 28, 2019); Smith v. Citimortgage, Inc., No. 1:13-cv-2177, 2014 WL 279728, at *7 (N.D. Ga. Jan. 24, 2014); Curran v. Mark Zinamosca & Assoc., No. 1:12-cv-750, 2014 WL 271634, at *10 (M.D. Pa. Jan. 23, 2014); Metro. Life Ins. Co. v. Blyther, 964 F. Supp. 2d 61, 71 (D.D.C. 2013); Barnes v. Med. Dep't, No. 13-cv-00285, 2013 U.S. Dist. LEXIS 51298, at *3 (S.D. Ill. Apr. 10, 2013); Sethunya v. Monson, No. 2:12-CV-454, 2013 WL 65471, at *3 (D. Utah Jan. 4, 2013); Abdelfattah v. DHS, 893 F. Supp. 2d 75, 81 n.4 (D.D.C. 2012), aff'd, 787 F.3d 524, 533 n. 4 (affirming District Court's dismissal of claims against private entities as Privacy Act does not apply to them); Cintron-Garcia v. Supermercados Econo, Inc., 818 F. Supp. 2d 500, 510 (D.P.R. 2011); Chapman v. Wright Transp., No. CA 11-0097, 2011 U.S. Dist. LEXIS 96913, at *6 n.4 (S.D. Ala. Aug. 10, 2011); Brooks v. AAA Cooper Transp., 781 F. Supp. 2d 472, 487-88 (S.D. Tex. 2011); Nouri v. TCF Bank, No. 10-12436, 2011 WL 836764, at *4 (E.D. Mich. Mar. 9, 2011); DeConcini Family Trust v. Home Fed. Bank, No. 2:10-CV-258, 2011 WL 635257, at *1 (D. Utah Feb. 11, 2011); Wilkerson v. H & S Lee, Inc., No. CV609-033, 2010 WL 2942635, at *2 (S.D. Ga. June 22, 2010), aff'd per curiam, 438 F. App'x 769 (11th Cir. 2011); Fox v. Cal. Franchise Tax Bd., No. 08-cv-01047, 2010 WL 56094, at *6 (D. Colo. Jan. 5, 2010); Tyree v. Hope Village, Inc., 677 F. Supp. 2d 109, 110 (D.D.C. 2009); Lengerich v. Columbia Coll., 633 F. Supp. 2d 599, 607-08 (N.D. Ill. 2009); Piper v. R.J. Corman R.R. Group, No. 05-CV-104, 2005 WL 1523566, at *8 (E.D. Ky. June 28, 2005); Locke v. MedLab/Gen. Chem., No. 99-2137, 2000 WL 127111 (E.D. Pa. Feb. 3,

2000); Payne v. EEOC, No. 99-270, slip op. at 2-3 (D.N.M. July 7, 1999), aff'd, No. 00-2021, 2000 WL 1862659, at *2 (10th Cir. Dec. 20, 2000); Davis v. Boston Edison Co., No. 83-1114-2, 1985 U.S. Dist. LEXIS 23275 (D. Mass. Jan. 21, 1985).

Neither federal funding nor regulation renders private entities subject to the Act. See Burch v. Pioneer Credit Recovery, Inc., 551 F.3d 122, 125 (2d Cir. 2008); Unt v. Aerospace Corp., 765 F.2d 1440, 1448 (9th Cir. 1985); United States v. Miller, 643 F.2d 713, 715 n.1 (10th Cir. 1981) (finding that definition of “agency” does not encompass national banks); United States v. Haynes, 620 F. Supp. 474, 478-79 (M.D. Tenn. 1985); Dennie v. Univ. of Pittsburgh Sch. of Med., 589 F. Supp. 348, 351-52 (D.V.I. 1984), aff'd, 770 F.2d 1068 (3d Cir. 1985) (unpublished table decision).

Individual agency officials generally are not considered “agencies.”

A civil action under the Privacy Act is properly filed against an “agency” only, not against an individual, a government official, an employee, or the United States. See, e.g., Palmieri v. United States, 896 F.3d 579, 586 (D.C. Cir. 2018) (“[u]nder the Privacy Act, an individual person is not an ‘agency’”); Kates v. King, 487 F. App’x 704, 706 (3d Cir. 2012) (per curiam); Flores v. Fox, 394 F. App’x 170, 172 (5th Cir. 2010) (per curiam); Jones v. Luis, 372 F. App’x 967, 969 (11th Cir. 2010) (per curiam); Weinberger v. Grimes, No. 07-6461, 2009 WL 331632, at *8 (6th Cir. Feb. 10, 2009); Pennyfeather v. Tessler, 431 F.3d 54, 55 (2d Cir. 2005); Connelly v. Comptroller of the Currency, 876 F.2d 1209, 1215 (5th Cir. 1989); Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1340 (9th Cir. 1987); Unt v. Aerospace Corp., 765 F.2d at 1447; Brown-Bey v. United States, 720 F.2d 467, 469 (7th Cir. 1983); Windsor v. The Tennessean, 719 F.2d 155, 159-60 (6th Cir. 1983); Bruce v. United States, 621 F.2d 914, 916 n.2 (8th Cir. 1980); Parks v. IRS, 618 F.2d 677, 684 (10th Cir. 1980); Osborne v. United States, No. 3:14-cv-25, 2014 WL 309468, at *7 (W.D.N.C. Jan. 28, 2014); Padilla-Ruiz v. United States, 893 F. Supp. 2d 301, 309 (D.P.R. 2012); Lim v. United States, No. 10-2574, 2011 WL 2650889, at *8 (D. Md. July 5, 2011); Blanton v. Warden, No. 7:10-cv-00552, 2011 WL 1226010, at *3 (W.D. Va. Mar. 30, 2011); Hollins v. Cross, No. 1:09cv75, 2010 WL 1439430, at *3 (N.D. W. Va. Mar. 17, 2010); Truesdale v. DOJ, 657 F. Supp. 2d 219, 227 (D.D.C. 2009); Walker v. Gambrell, 647 F. Supp. 2d 529, 536 (D. Md. 2009); Fetzer, 384 F. Supp. 2d at 816; Burns v. Potter, 334 F. Supp. 2d 13, 20-21 (D. Mass. 2004); Stokes v. Barnhart, 257 F. Supp. 2d 288, 299 (D. Me. 2003); Mumme v. Labor, 150 F. Supp. 2d 162, 169 (D. Me. 2001) (“[A] claimant bringing a Privacy Act claim must bring suit against a particular agency, not the entire United States.”), aff'd, No. 01-2256 (1st Cir. June 12, 2002); Dennie, 589 F. Supp. at 351-53.

Furthermore, “courts have consistently declined to imply a Bivens-style right of action against individual officers for conduct that would be actionable under the Privacy Act.” Gordon v. Gutierrez, No. 1:06cv861, 2006 WL 3760134, at *3 (E.D. Va. Dec. 14, 2006). One court also noted, though, that while a Privacy Act action “must be maintained against an agency,” it is “unaware of any authority which requires the Plaintiffs to specifically name, either as an individual defendant or within the body of a complaint, each and every agency employee who may have contributed to an alleged Privacy Act violation.” Buckles v. Indian Health Serv., 305 F. Supp. 2d 1108, 1112 (D.N.D. 2004).

The District Court for the District of Columbia has explained that “[i]n order for an agency to be liable for a Privacy Act violation allegedly committed by one of its employees, the responsible agency employee must have been acting within the scope of his or her employment.” Convertino v. DOJ, 769 F. Supp. 2d 139, 147 (D.D.C. 2011) (“Therefore, even if [plaintiff] could prove that the leak must have come from a DOJ employee – which he cannot – his claim would fail because no reasonable fact-finder could conclude that any such DOJ employee was acting within the scope of his or her employment at the time of the leak.”), rev’d and remanded on other grounds, 684 F.3d 93 (D.C. Cir. 2012).

Some courts have held that the head of an agency, if sued in his or her official capacity, can be a proper party defendant under the Privacy Act. See Hampton v. FBI, No. 93-0816, slip op. at 8, 10-11 (D.D.C. June 30, 1995); Jarrell v. Tisch, 656 F. Supp. 237, 238 (D.D.C. 1987); Diamond v. FBI, 532 F. Supp. 216, 219-20 (S.D.N.Y. 1981), aff’d, 707 F.2d 75 (2d Cir. 1983); Nemetz v. Treasury, 446 F. Supp. 102, 106 (N.D. Ill. 1978); Rowe v. Tennessee, 431 F. Supp. 1257, 1264 (M.D. Tenn. 1977), vacated on other grounds, 609 F.2d 259 (6th Cir. 1979); cf. Cloonan, 768 F. Supp. 2d at 162 (“find[ing] that plaintiff’s error in naming only individual defendants was harmless” because “[o]n its face, the Complaint makes clear that in naming former attorney general Michael Mukasey, plaintiff was naming the Department of Justice as a defendant” and because complaint named Attorney General only in his official capacity). But see Williams v. Fanning, 63 F. Supp. 3d 88, 90 n.2 (D.D.C. 2014) (dismissing Secretary of Air Force and Commanding Officer of Headquarters Air Force Personnel Center as improper parties under Privacy Act and proceeding with Air Force as only proper defendant under Privacy Act).

Suits against agency heads by pro se plaintiffs may be more likely to be construed as suits against the respective agencies because pro se pleadings are construed liberally. See Walker, 647 F. Supp. 2d at 536. Further, leave to amend a complaint to substitute a proper party defendant ordinarily is freely granted where the agency is on notice of the claim. See, e.g., Reyes v. Supervisor of DEA,

834 F.2d 1093, 1097 (1st Cir. 1987); Petrus, 833 F.2d at 583. But cf. Doe v. Rubin, No. 95-CV-75874, 1998 U.S. Dist. LEXIS 14755, at *9 (E.D. Mich. Aug. 10, 1998) (granting summary judgment for defendant where plaintiff had named Secretary of Treasury as sole defendant and had filed no motion to amend). In addition, at least one court has held that while the head of an agency is not a proper defendant under the Privacy Act, an agency can waive any objections to the naming of an improper party if it received proper notice of the action and did not dispute its designation as a defendant. See Bavidó v. Apfel, 215 F.3d 743, 747 (7th Cir. 2000) (finding SSA Commissioner was not proper party defendant, but SSA had waived any objection as to naming of proper party agency defendant).

Note that a prosecution enforcing the Privacy Act's criminal penalties provision, 5 U.S.C. § 552a(i) (see "Criminal Penalties" discussion, below), would properly be filed against an individual. See Stone v. Def. Investigative Serv., 816 F. Supp. 782, 785 (D.D.C. 1993) ("Under the Privacy Act, this Court has jurisdiction over individually named defendants only for unauthorized disclosure in violation of 5 U.S.C. § 552a(i)."); see also Hampton, No. 93-0816, slip op. at 8, 10-11 (citing Stone).

B. 5 U.S.C. § 552a(a)(2) - Individual

"[T]he term 'individual' means a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2).

Comment:

The Privacy Act's definition of "individual" is much narrower than the FOIA's definition of "person," which draws from the Administrative Procedures Act. See 5 U.S.C. § 551(2) (2018) (defining person as "an individual, partnership, corporation, association, or public or private organization other than an agency."); see also, e.g., Raven, 583 F.2d at 170-71 (comparing "use of the word 'individual' in the Privacy Act, as opposed to the word 'person,' as more broadly used in the FOIA"); Cudzich v. INS, 886 F. Supp. 101, 105 (D.D.C. 1995) (A plaintiff whose permanent resident status had been revoked "is not an 'individual' for the purposes of the Privacy Act. . . . Plaintiff's only potential access to the requested information is therefore under the Freedom of Information Act.").

The Privacy Act generally covers citizens and lawful permanent residents, but others have some protections.

Generally, individuals under the Privacy Act are US citizens and lawful permanent residents. See S. Rep. No. 93-1183, at 79, reprinted in Source Book at 232, https://www.justice.gov/opcl/paoverview_sourcebook; OMB 1975 Guidelines, 40 Fed. Reg. at 28,951, https://www.justice.gov/paoverview_omb-75. The Privacy Act as initially enacted did not generally protect non-resident foreign nationals. See, e.g., Raven v. Panama Canal Co., 583 F.2d 169, 170-71 (5th Cir. 1978) (referencing legislative history that “reflects the congressional intent to exclude nonresident aliens from Privacy Act coverage”); Soto v. State, 244 F. Supp. 3d 207, 208-09 (D.D.C. 2017) (per curiam) (unpublished table decision) (citing Fares v. INS, 50 F.3d 6 (4th Cir. 1995)) (“[Privacy] Act only protects citizens of the United States or aliens lawfully admitted for permanent residence.”).

The Judicial Redress Act of 2015, however, enables citizens of certain foreign countries to bring suit under certain provisions of the Privacy Act in the same manner as U.S. citizens and lawful permanent residents. See 5 U.S.C. § 552a note. The Judicial Redress Act is discussed further under “Judicial Redress Act” above.

In addition, the OMB 1975 Guidelines provide that while the Act does not apply to records pertaining solely to non-resident foreign nationals, “[w]here a system of records covers both citizens and nonresident aliens, only that portion which relates to citizens or resident aliens is subject to the Act but agencies are encouraged to treat such systems as if they were, in their entirety, subject to the Act.” OMB 1975 Guidelines, 40 Fed. Reg. at 28,951, https://www.justice.gov/paoverview_omb-75. Other OMB guidelines establish protections for personally identifiable information, regardless of citizenship or other legal status of the individuals whose information is involved. See, e.g., OMB Circular A-130, at 33, https://www.justice.gov/paoverview_omb-a-130; see also Nat’l Inst. of Standards & Tech., Spec. Pub. 800-53, Rev. 5, Security and Privacy Controls for Federal Information Systems and Organizations, at 483 (2020), <https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/final> (defining “personally identifiable information” without regard to citizenship or other legal status).

“Individuals” do not include the deceased, corporations, organizations, derivatives, or, in some courts, sole proprietors.

Deceased individuals do not have any Privacy Act rights, nor do executors or next-of-kin. See generally OMB 1975 Guidelines, 40 Fed Reg. at 28, 951,

https://www.justice.gov/paoverview_omb-75 (stating “the thrust of the Act was to provide certain statutory rights to living as opposed to deceased individuals” and “the Act did not contemplate permitting relatives and other interested parties to exercise rights granted by the Privacy Act to individuals after the demise of those individuals”); see also Warren v. Colvin, 744 F.3d 841, 843-44 (2d Cir. 2014) (“deceased individuals generally do not enjoy rights under the Privacy Act”); Whitaker v. CIA, 31 F. Supp. 3d 23, 48 (D.D.C. 2014) (deferring to agency’s interpretation of OMB’s guidance and concluding that “Privacy Act does not speak to the access rights of relatives of deceased individuals”); Crumpton v. United States, 843 F. Supp. 751, 756 (D.D.C. 1994), aff’d on other grounds sub nom. Crumpton v. Stone, 59 F.3d 1400 (D.C. Cir. 1995); cf. Flores v. Fox, 394 F. App’x 170, 171-72 (5th Cir. 2010) (per curiam) (“[Plaintiff’s] claim for injunctive relief to correct his prison records . . . is mooted by his death.”).

Privacy Act rights are personal to the individual who is the subject of the record and cannot be asserted derivatively by others. See, e.g., Warren v. Colvin, 744 F.3d 841, 843-44 (2d Cir. 2014) (“Privacy Act does not provide an individual with a right to demand materials pertaining to him but contained only in another individual’s records.”); Parks v. IRS, 618 F.2d 677, 684-85 (10th Cir. 1980) (concluding union lacked standing to sue for damages to its members); Word v. United States, 604 F.2d 1127, 1129 (8th Cir. 1979) (finding criminal defendant lacked standing to allege Privacy Act violations regarding use at trial of medical records concerning third party); Dresser Indus., 596 F.2d at 1238 (finding company lacked standing to litigate employees’ Privacy Act claims); Whitaker, 31 F. Supp. 3d at 48 (rejecting plaintiff’s argument that agency was “required to process his requests for his father’s records under the Privacy Act as well as FOIA”); Pub. Emps. for Env’tl. Responsibility, 926 F. Supp. 2d at 54-55 (finding third-party organization did not have standing to sue even though given written consent by subject individual allowing EPA to disclose records pertaining to him); Lorenzo v. United States, 719 F. Supp. 2d 1208, 1215-16 (S.D. Cal. 2010) (holding plaintiff lacks standing to pursue claim for recovery for adverse effects she suffered based on disclosure of her husband’s record); Research Air, Inc. v. Kempthorne, 589 F. Supp. 2d 1, 11 (D.D.C. 2008) (asserting that individual’s attorney has no Privacy Act rights to request documents relating to client absent client’s written consent); Sirmans v. Caldera, 27 F. Supp. 2d 248, 250 (D.D.C. 1998) (“[Plaintiffs] may not object to the Army’s failure to correct the records of other officers.”); Abramsky v. U.S. Consumer Prod. Safety Comm’n, 478 F. Supp. 1040, 1041-42 (S.D.N.Y. 1979) (stating that union president cannot compel release of records pertaining to employee’s termination). But see Nat’l Fed’n of Fed. Emps. v. Greenberg, 789 F. Supp. 430, 433 (D.D.C. 1992) (finding union had associational standing because members whose interests union sought to

represent would themselves have standing), vacated & remanded on other grounds, 983 F.2d 286 (D.C. Cir. 1993).

Corporations and organizations also do not have any Privacy Act rights. See, e.g., Hurry v. FINRA, 782 F. App'x 600, 602 (9th Cir. 2019) ("The Act applies to records of natural persons only, and only natural persons may sue under the Act."); Corey v. USPS, 485 F. App'x 228, 229 (9th Cir. 2012) (holding USPS is not an "individual" under the Privacy Act); St. Michael's Convalescent Hosp. v. California, 643 F.2d 1369, 1373 (9th Cir. 1981); Dresser Indus. v. United States, 596 F.2d 1231, 1237-38 (5th Cir. 1980); Cell Assocs. v. NIH, 579 F.2d 1155, 1157 (9th Cir. 1978); Stone v. Exp.-Imp. Bank of the United States, 552 F.2d 132, 137 n.7 (5th Cir. 1977); Arruda & Beaudoin v. Astrue, No. 11-10254, 2013 WL 1309249, at *10 (D. Mass. Mar. 27, 2013); Pub. Emps. for Envtl. Responsibility v. EPA, 926 F. Supp. 2d 48, 55 (D.D.C. 2013); Falwell v. Exec. Office of the President, 158 F. Supp. 2d 734, 736, 739 n.3 (W.D. Va. 2001); Comm. in Solidarity v. Sessions, 738 F. Supp. 544, 547 (D.D.C. 1990) ("Privacy Act does not confer standing upon organizations on their own or purporting to sue on behalf of their members."), aff'd on other grounds, 929 F.2d 742 (D.C. Cir. 1991); United States v. Haynes, 620 F. Supp. 474, 478-79 (M.D. Tenn. 1985); see also OMB 1975 Guidelines, https://www.justice.gov/paoverview_omb-75. But cf. Recticel Foam Corp. v. DOJ, No. 98-2523, slip op. at 11-15 (D.D.C. Jan. 31, 2002) (finding corporation had standing to bring action under Administrative Procedure Act to enjoin agency from disclosing investigative information about company; "[T]he fact that Congress did not create a cause of action for corporations under the Privacy Act does not necessarily mean that Recticel's interests do not fall within the 'zone of interests' contemplated by that Act. It is sufficient for a standing analysis that Plaintiffs' interests 'arguably' fall within the zone of interests contemplated by the statute."), appeal dismissed, No. 02-5118 (D.C. Cir. Apr. 25, 2002).

Additionally, the OMB 1975 Guidelines suggest individuals have no standing under the Privacy Act to challenge agency handling of records that pertain to them solely in their "entrepreneurial" capacities. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,951, https://www.justice.gov/paoverview_omb-75 (quoting legislative history and stating it "suggests that a distinction can be made between individuals acting in a personal capacity and individuals acting in an entrepreneurial capacity (e.g., as sole proprietors) and that th[e] definition [of 'individual'] (and, therefore, the Act) was intended to embrace only the former"); see also St. Michaels Convalescent Hosp., 643 F.2d at 1373 (stating that "sole proprietorships[] are not 'individuals' and thus lack standing to raise a claim under the Privacy Act").

However, not all courts have adopted OMB's personal/entrepreneurial

distinction. Compare Shermco Indus. v. Sec’y of the Air Force, 452 F. Supp. 306, 314-15 (N.D. Tex. 1978) (accepting distinction), rev’d & remanded on other grounds, 613 F.2d 1314 (5th Cir. 1980), and Daniels v. FCC, No. 77-5011, slip op. at 8-9 (D.S.D. Mar. 15, 1978) (same), with Rice v. United States, 245 F.R.D. 3, 5-6 (D.D.C. 2007) (rejecting distinction without referencing OMB 1975 Guidelines and observing that “line between personal and business information is blurred for farmers, ranchers, and other family-owned businesses”); Scarborough v. Harvey, 493 F. Supp. 2d 1, 13 n.28 (D.D.C. 2007) (rejecting distinction); Metadure Corp. v. United States, 490 F. Supp. 1368, 1373-74 (S.D.N.Y. 1980) (same); Fla. Med. Ass’n v. HEW, 479 F. Supp. 1291, 1307-11 (M.D. Fla. 1979) (same); and Zeller v. United States, 467 F. Supp. 487, 496-99 (E.D.N.Y. 1979) (same).

Parents or legal guardians may, however, act on behalf of certain individuals.

The parent of a minor or the legal guardian of an incompetent may act, however, on behalf of that individual. See 5 U.S.C. § 552a(h); Gula v. Meese, 699 F. Supp. 956, 961 (D.D.C. 1988); cf. Maldonado Guzman v. Massanari, No. 00-2410, slip op. at 6-7 (D.P.R. Aug. 10, 2001) (holding plaintiff had no avenue of relief for obtaining information about his emancipated daughter under Privacy Act because he did not provide documentation required by agency regulations to verify he was her legal guardian), subsequent related opinion sub nom. Maldonado Guzman v. SSA, 182 F. Supp. 2d 216 (D.P.R. 2002). The OMB 1975 Guidelines note that subsection (h) is “discretionary and that individuals who are minors are authorized to exercise the rights given to them by the Privacy Act or, in the alternative, their parents or those acting in loco parentis may exercise them in their behalf.” 40 Fed. Reg. at 28,970, <https://www.justice.gov/paoverview omb-75>; but see OMB Supplementary Guidance, 40 Fed. Reg. at 56,742, <https://www.justice.gov/paoverview omb-75-suppl> (noting that “[t]here is no absolute right of a parent to have access to a record about a child absent a court order or consent”).

C. 5 U.S.C. § 552a(a)(3) - Maintain

“[T]he term ‘maintain’ includes maintain, collect, use or disseminate.” 5 U.S.C. § 552a(a)(3).

Comment:

The definition of “maintain” embraces various activities with respect to records and has a meaning much broader than the common usage of the term. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,951, <https://www.justice.gov/paoverview omb-75>. The United States Court of Appeals for the Ninth Circuit recently

considered the meaning of “maintain” in the context of records describing First Amendment activity. Garris v. FBI, 937 F.3d 1284, 1300 (9th Cir. 2019). The Ninth Circuit presumed that because Congress defined “maintain” to include “maintain” and “collect,” Congress intended the provision to apply to distinct activities. Id. at 1295. For an agency to “maintain” a record describing how an individual exercises rights guaranteed by the First Amendment “pertinent to and within the scope of an authorized law enforcement activity,” the Ninth Circuit found that, “to give each of these verbs its meaning,” the most reasonable reading of the statute as a whole is that the record must be pertinent to an authorized law enforcement activity both “at the time of gathering, i.e., collecting, [and] at the time of keeping, i.e., maintaining.” Id. at 1295 (quoting L. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 607 (D.C. Cir. 1996) (Tatel, J., concurring in part and dissenting in part)). See also, e.g., Albright v. United States, 631 F.2d 915, 918-20 (D.C. Cir. 1980) (analyzing scope of term “maintain” in context of subsection (e)(7) challenge to record describing First Amendment-protected activity and stating that “the Act clearly prohibits even the mere collection of such a record, independent of the agency’s maintenance, use or dissemination of it thereafter”).

D. 5 U.S.C. § 552a(a)(4) - Record

“[T]he term ‘record’ means any 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.” 5 U.S.C. § 552a(a)(4).

Comment:

A Privacy Act “record” must identify an individual.

To qualify as a Privacy Act “record,” the information must identify an individual. See, e.g., Reuber v. United States, 829 F.2d 133, 142 (D.C. Cir. 1987) (concluding that letter reprimanding individual sent to and disclosed by agency was “record” because it clearly identified individual by name and address); Albright, 631 F.2d 915 at 920 (citing subsection (e)(7) case holding that videotape of meeting constituted “record” because “[a]s long as the tape contains a means of identifying an individual by picture or voice, it falls within the definition of a ‘record’ under the Privacy Act”); Fleming v. U.S. R.R. Ret. Bd., No. 01 C 6289, 2002 WL 252459, at *2 (N.D. Ill. Feb. 21, 2002) (citing Robinson, 1988 WL 5083, at *1) (holding that summary of investigation of plaintiff disclosed in semi-annual

report to Congress did not identify plaintiff and thus did not constitute a “record” because disclosure “would have identified plaintiff only to an individual who had other information that would have caused that individual to infer from the report that plaintiff was the subject of the investigation”); cf. Speaker v. HHS Ctrs. for Disease Control & Prevention, 623 F.3d 1371, 1383-87 n.12 (11th Cir. 2010) (reversing district court’s dismissal of complaint, finding that complaint sufficiently alleged that CDC disclosed plaintiff’s identity); Cacho v. Chertoff, No. 06-00292, 2006 WL 3422548, at *6 n.3 (D.D.C. Nov. 28, 2006) (declining to decide “the novel issue of whether a disclosure of the absence of information from a system of records can constitute the disclosure of a record”; given that plaintiff deliberately did not report his health problems, “accepting plaintiff’s characterization of his failure to report them as itself constituting a record that is afforded protection by the Privacy Act would stretch the meaning of the statute beyond its intended purpose”).

The OMB 1975 Guidelines state that the term “record” means “any item of information about an individual that includes an individual identifier,” and “can include as little as one descriptive item about an individual.” 40 Fed. Reg. at 28,951-52, https://www.justice.gov/paoverview_omb-75 (quoting legislative history appearing at 120 Cong. Rec. 40,408, 40,883 (1974), reprinted in Source Book at 866, 993, https://www.justice.gov/opcl/paoverview_sourcebook).

The courts of appeals have established differing tests for identifying a “record” under the Act.

Several courts of appeals have articulated tests for determining whether an item qualifies as a “record” under the Privacy Act, resulting in different tests for determining whether information meets the “record” definition:

1. Broad Definition - Any Record Linked to Individual’s Identifying Information

Consistent with the OMB 1975 Guidelines, the Courts of Appeals for the Second, Third, and Fourth Circuits have broadly interpreted the term “record” to include any record that is linked to an individual through identifying information. See Bechhoefer v. DEA, 209 F.3d 57 (2d Cir. 2000); Williams v. VA, 104 F.3d 670, 673-74 (4th Cir. 1997); Quinn v. Stone, 978 F.2d 126 (3d Cir. 1992). 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 “limited to information which taken alone directly reflects a characteristic or quality.” Quinn, 978 F.2d at 133 (holding that out-of-date home address on roster and

time card information are records covered by the Privacy Act). The Second Circuit, after analyzing the tests established by the other courts of appeals, adopted a test “much like the Third Circuit’s test.” Bechhoefer, 209 F.3d at 60. The Second Circuit did so for three reasons. First, it found the Third Circuit’s test to be “most consistent with the ‘broad terms’ . . . of the statutory definition.” Id. Second, it found the Third Circuit’s test to be the only one consistent with the Supreme Court’s decision in DOD v. FLRA, 510 U.S. 487, 494 (1994), which held that federal civil service employees’ home addresses qualified for protection under the Privacy Act. Bechhoefer, 209 F.3d at 61. Finally, it found the Third Circuit’s test to be supported by the legislative history of the Privacy Act and OMB guidelines and regulations. Id. at 61-62. The Second Circuit held that the term “record” “has ‘a broad meaning encompassing,’ at the very least, any personal information ‘about an individual that is linked to that individual through an identifying particular.’” Id. at 62 (quoting Quinn and holding that letter containing plaintiff’s name and “several pieces of ‘personal information’ about him, including his address, his voice/fax telephone number, his employment, and his membership in [an association],” were “records” covered by Privacy Act).

The Court of Appeals for the Fourth Circuit has also construed the term “record” broadly, holding that “the legislative history of the Act makes it clear that a ‘record’ was meant to ‘include as little as one descriptive item about an individual,’” and finding that “draft” materials qualified as “records” because they “substantially pertain to Appellant,” “contain ‘information about’ [him], as well as his ‘name’ or ‘identifying number,’” and “do more than merely apply to him”). Williams, 104 F.3d at 673-74 (quoting Source Book at 866, https://www.justice.gov/opcl/paoverview_sourcebook).

Several district courts also have applied a broad interpretation of the term “record.” See, e.g., Akmal v. United States, No. C12-1499, 2014 WL 906231, at *2 (W.D. Wash. Mar. 7, 2014) (finding that “[a]gency employee names, addresses, phone numbers, and dates of birth are ‘records’ covered by the Privacy Act”); Walia v. Napolitano, 986 F. Supp. 2d 169, 186 (E.D.N.Y. 2013) (finding that documents maintained by DHS in Plaintiff’s employment and personnel files, including plaintiff’s EEO activity, “may qualify as ‘records’ [in the broadest sense] because they identify the Plaintiff by name and contain information about a prospective investigation premised on the Plaintiff’s alleged misconduct”); Arruda & Beaudoin v. Astrue, No. 11-10254, 2013 WL 1309249, at *10 (D. Mass. Mar. 27, 2013) (quoting Bechhoefer and finding “queries satisfy these criteria” as “record” under the Privacy

Act); Sullivan v. USPS, 944 F. Supp. 191, 196 (W.D.N.Y. 1996) (finding that disclosing to plaintiff's employer that applicant had applied for employment with Postal Service constituted disclosure of "record" under Privacy Act; mere fact of record's existence was sufficient to constitute record because applicant's name was part of information contained in application and Postal Service disclosed that particular applicant by that name had applied for employment).

2. **Narrow Definition - Record Must Reflect Individual Quality or Characteristic**

The Courts of Appeals for the Ninth and Eleventh Circuits have limited Privacy Act coverage by adopting a narrow construction of the term "record" and requiring that the information "must reflect some quality or characteristic of the individual involved." Boyd v. Sec'y of the Navy, 709 F.2d 684, 686 (11th Cir. 1983) (per curiam) (although stating narrow test, finding that memorandum reflecting "Boyd's failure to follow the chain of command and his relationship with management" qualified as Privacy Act record); accord Unt v. Aerospace Corp., 765 F.2d 1440, 1448-49 (9th Cir. 1985) (finding letter written by employee – containing allegations of mismanagement against corporation that led to his dismissal – held not his "record" because it was "about" corporation and reflected "only indirectly on any quality or characteristic" of employee); but see Unt, 765 F.2d at 1449-50 (Ferguson, J., dissenting) (opining that majority's narrow interpretation of term "record" "is illogical, contrary to the legislative intent, and defies the case laws' consistent concern with the actual effect of a record on a person's employment when assessing that record's nature or subject").

3. **Middle Ground - Record Must be "About" Individual, But Need Not Reflect Quality or Characteristic**

The Courts of Appeals for the District of Columbia and Fifth Circuits have staked out the middle ground. See Pierce v. Air Force, 512 F.3d 184, 188 (5th Cir. 2007); Tobey v. NLRB, 40 F.3d 469, 471 (D.C. Cir. 1994). The D.C. Circuit held that to qualify as a "record," the information "must both be 'about' an individual and include his name or other identifying particular." Tobey, 40 F.3d at 471. The D.C. Circuit rejected the Third Circuit's determination in Quinn that information could qualify as a record "if that piece of information were linked with an identifying particular (or was itself an identifying particular)," because "[it] fails to require that information both be 'about' an individual and be linked to that individual by an identifying particular." Id. (discussing Quinn, 978 F.2d at 133).

On the other hand, the D.C. Circuit found the Ninth and Eleventh Circuits' definitions in Unt and Boyd too narrow, stating that: "So long as the information is 'about' an individual, nothing in the Act requires that it additionally be about a 'quality or characteristic' of the individual." Tobey, 40 F.3d at 472. Ultimately, the D.C. Circuit concluded that an NLRB computer system for tracking and monitoring cases did not constitute a system of records because its files contained no information "about" individuals, despite the fact that the information contained the initials or identifying number of the field examiner assigned to the case. Id. at 471-73. Although the court recognized that the case information could be, and apparently was, used in connection with other information to draw inferences about a field examiner's job performance, it stated that that "does not transform the [computer system] files into records about field examiners." Id. at 472-73. See also Sussman v. Marshals Serv., 494 F.3d 1106, 1121 (D.C. Cir. 2007) ("[the record] must actually describe him in some way"); Houghton v. State, 875 F. Supp. 2d 22, 34-36 (D.D.C. 2012) (following standard set out in Tobey and determining transcripts at issue were not "about" plaintiff but rather "about a Memorandum of Understanding [between governments]" and "[e]ven the parts of the transcripts that mention [plaintiff] are about a letter he wrote that was published . . . not about him . . . The mere fact that the transcripts contain reference to or quote from plaintiff's written work is not sufficient to make it a 'record.'"); Aguirre v. SEC, 671 F. Supp. 2d 113, 121-22 (D.D.C. 2009) (following Sussman and concluding that where plaintiff sought "records of an investigation of his allegation that the SEC "fired [him] for questioning" the decision to give "preferential treatment to one of Wall Street's elite," plaintiff had "alleged that the records describe the reasons for his termination" and, therefore it was, "at the very least, plausible that these records . . . describe him in some way"); Hatfill v. Gonzalez, 505 F. Supp. 2d 33, 35-39 (D.D.C. 2007) (concluding that information in news articles and reports concerning plaintiff's suspected involvement in criminal activity that were leaked to reporters by government officials were "records"); Scarborough v. Harvey, 493 F. Supp. 2d 1, 15-16 (D.D.C. 2007) (asserting documents naming individual plaintiffs and describing their involvement in allegedly criminal activities were "about" plaintiffs and therefore were not excluded from definition of "records," even if these activities were undertaken in connection with plaintiffs' businesses); Leighton v. CIA, 412 F. Supp. 2d 30, 38-39 (D.D.C. 2006) (finding information included in magazine column, which did not name plaintiff contractor or contain identifier but stated that "the CIA is looking at contractors and suspended two in June for talking to the press," was not "record" "about" plaintiff); Roberts v. DOJ, 366 F. Supp. 2d 13, 26 (D.D.C. 2005) (finding that FBI director's public response to OIG

report investigating plaintiff's allegations of FBI wrongdoing was not "about" plaintiff; rather, it was an examination of the "validity of public allegations of misconduct lodged against [the FBI]"; Tripp v. DOD, 193 F. Supp. 2d 229, 236 (D.D.C. 2002) (citing Tobey and finding salary information for position plaintiff applied for "is not 'about' plaintiff – the fact that she could receive that salary had she been chosen for the position does not convert this into information 'about' plaintiff"); Voinche v. CIA, No. 98-1883, 2000 U.S. Dist. LEXIS 14291, at *8, 11-12 (D.D.C. Sept. 27, 2000) (citing Tobey and Fisher, *infra*, and finding that records regarding plaintiff's administrative appeal concerning prior access request and case files of plaintiff's prior Freedom of Information Act litigation, "while identifying plaintiff by name, are not 'about' the plaintiff, but rather are 'about' the administrative appeal and prior litigation under the FOIA"); Fisher v. NIH, 934 F. Supp. 464, 466-67, 469-72 (D.D.C. 1996) (following Tobey and finding that bibliographic information published in scientific journals including title of article and publication, name and address of author, summary of article and annotation ["scientific misconduct – data to be reanalyzed"], provides "information 'about' the article described in each file, not 'about' [the author]," even though information "could be used to draw inferences or conclusions about [the author]"; "The fact that it is possible for a reasonable person to interpret information as describing an individual does not mean the information is about that individual for purposes of the Privacy Act."), summary affirmance granted, No. 96-5252 (D.C. Cir. Nov. 27, 1996); Henke v. Commerce, No. 94-0189, 1996 WL 692020, at *3 (D.D.C. Aug. 19, 1994) (holding that names of four reviewers who evaluated grant applicant's proposal are applicant's "records" under Privacy Act), aff'd on other grounds, 83 F.3d 1445 (D.C. Cir. 1996), abrogated on other grounds, Mobley v. CIA, 924 F. Supp. 2d 24, 57 (D.D.C. 2013) (finding Henke holding that "information contained in one individual's record is exempt from the disclosure requirements of the Privacy Act simply because the same information is also contained in another individual's records" did not survive Sussman) Doe v. DOJ, 790 F. Supp. 17, 22 (D.D.C. 1992) (applying Nolan, *infra*, and alternatively holding that "names of agents involved in the investigation are properly protected from disclosure"); Topuridze v. FBI, No. 86-3120, 1989 WL 11709, at *2 (D.D.C. Feb. 6, 1989) (citing Unt with approval and holding that letter written about requester, authored by third party, cannot be regarded as third party's record; it "does not follow that a document reveals some quality or characteristic of an individual simply by virtue of the individual having authored the document"), reconsideration denied sub nom. Topuridze v. USIA, 772 F. Supp. 662, 664-65 (D.D.C. 1991) (reaffirming that "[i]n order to be about an individual a record must 'reflect some quality or characteristic of the individual involved,'" stating that

document “may well be ‘about’ the author,” after in camera review, as it discussed author’s family status, employment, and fear of physical retaliation if letter were disclosed to plaintiff, and ultimately ruling that it need not reach issue of whether or not letter was “about” author and denying reconsideration on ground that letter was without dispute about subject/plaintiff); and Shewchun v. U.S. Customs Serv., No. 87-2967, 1989 WL 7351, at *1 (D.D.C. Jan. 11, 1989) (finding that letter concerning agency’s disposition of plaintiff’s merchandise “lacks a sufficient informational nexus with [plaintiff] (himself, as opposed to his property) to bring it within the definition of ‘record’”).

Agreeing with Tobey, the Fifth Circuit concluded that information must be both “about” an individual and contain an identifying particular assigned to that individual to qualify as a “record.” See Pierce, 512 F.3d at 188. In Pierce, the Fifth Circuit explained that “[a]lthough the Privacy Act protects more than just documents that contain a person’s name, it does not protect documents that do not include identifying particulars.” Id. at 187. In determining whether a “final response letter” and “summary report of investigation” containing only “duty titles” constituted “records,” the court concluded that, because duty titles did “not pertain to one and only one individual,” they did not qualify as “identifying particulars” and thus, did not qualify as records under Privacy Act. Id. at 187-88. However, the court also recognized that “where duty titles pertain to one and only one individual . . . duty titles may indeed be ‘identifying particulars’ as that term is used in the definition of ‘record’ in the Privacy Act.” Id.

Additional courts have adopted different, narrow, and, at times, conflicting interpretations of the term “record.”

Several other courts have limited Privacy Act coverage by applying narrow constructions of the term “record” without explicitly adopting the Ninth and Eleventh Circuits’ requirement that information must reflect some characteristic of the individual involved. See, e.g., Minshev v. Donley, 911 F. Supp. 2d 1043, 1071 (D. Nev. 2012) (finding that emails revealing information about plaintiff were “the method of disclosure, not the source of the Privacy Act protected material” and, thus, the emails themselves were not “records”); Counce v. Nicholson, No. 3:06cv00171, 2007 WL 1191013, at *15 (M.D. Tenn. Apr. 18, 2007) (concluding that “email contain[ing] information regarding a potential presentation on bullying that [plaintiff’s] supervisors directed her to submit for their review” was not “record”); Lapka v. Chertoff, No. 05-C-668, 2006 WL 3095668, at *6-7 (N.D. Ill. Oct. 30, 2006) (citing Unt and explaining that “[u]nder the Privacy Act, records that

are generated in response to a complaint are not records about the complainant but rather are considered records about the accused"); Nolan v. DOJ, No. 89-A-2035, 1991 WL 36547, at *10 (D. Colo. Mar. 18, 1991) (holding names of FBI special agents and other personnel are not requester's "record" and therefore "outside the scope of the [Privacy Act]"), aff'd, 973 F.2d 843 (10th Cir. 1992); Blair v. U.S. Forest Serv., No. A85-039, slip op. at 4-5 (D. Alaska Sept. 24, 1985) (holding "Plan of Operation" form completed by plaintiff is not his "record" as it "reveals nothing about his personal affairs"), appeal dismissed, No. 85-4220 (9th Cir. Apr. 1, 1986); Windsor v. A Fed. Exec. Agency, 614 F. Supp. 1255, 1260-61 (M.D. Tenn. 1983) (noting that "record" includes only sensitive information about individual's private affairs), aff'd, 767 F.2d 923 (6th Cir. 1985) (unpublished table decision) Cohen v. Labor, 3 Gov't Disclosure Serv. (P-H) ¶ 83,157, at 83,791 (D. Mass. Mar. 21, 1983) (record includes only "personal" information); AFGE v. NASA, 482 F. Supp. 281, 282-83 (S.D. Tex. 1980) (determining that sign-in/sign-out sheet was not "record" because, it was not "in and of itself, reflective of some quality or characteristic of an individual").

For a further illustration of conflicting views concerning the meaning of the term "record" in the context of individuals' right to access their records under subsection (d)(1), compare Voelker v. IRS, 646 F.2d 332, 334 (8th Cir. 1981) (requiring agency to provide individual with access to his entire record, even though some information in that record "pertained" to a third party), with Sussman, 494 F.3d at 1121 n.9 (interpreting subsection (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"; "[f]or an assemblage of data to qualify as one of [plaintiff's] records, it must not only contain his name or other identifying particulars but also be about him"). See also Aguirre v. SEC, 671 F. Supp. 2d 113, 121 (D.D.C. 2009), Nolan v. DOJ, No. 89-A-2035, 1991 WL 36547, at *3 (D. Colo. Mar. 18, 1991), aff'd, 973 F.2d 843 (10th Cir. 1992), and DePlanche v. Califano, 549 F. Supp. 685, 693-98 (W.D. Mich. 1982). These important cases are discussed further below under "Individual's Right of Access."

One district court, in a case concerning the Privacy Act's subsection (b)(3) routine use exception, held that a plaintiff may choose which particular "item of information," i.e., one document, contained within a "collection or grouping of information" to designate as a "record" and challenge as wrongfully disclosed. Covert v. Harrington, 667 F. Supp. 730, 736-37 (E.D. Wash. 1987), aff'd on other grounds, 876 F.2d 751 (9th Cir. 1989). Purporting to construe the term "record" narrowly, the district court in Covert ruled that the Department of Energy's routine use permitting disclosure of

relevant records where “a record” indicates a potential violation of law did not permit its Inspector General to disclose personnel security questionnaires to the Justice Department for prosecution because the questionnaires themselves did not reveal a potential violation of law on their face. 667 F. Supp. at 736-37. Covert is discussed further below under “Conditions of Disclosure to Third Parties,” “Agency Requirements,” and “Civil Remedies.”

Private notes are not “records,” but may become them once used to make a determination about an individual.

Purely private notes – such as personal memory refreshers – generally are found not to be subject to the Privacy Act because they are not “agency records.” Bowyer v. Air Force, 804 F.2d 428, 431 (7th Cir. 1986); see also Johnston v. Horne, 875 F.2d 1415, 1423 (9th Cir. 1989); Boyd, 709 F.2d at 686; Harmer v. Perry, No. 95-4197, 1998 WL 229637, at *3 (E.D. Pa. Apr. 28, 1998), *aff’d*, No. 98-1532 (3d Cir. Jan. 29, 1999); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,952, https://www.justice.gov/paoverview_omb-75 (“Uncirculated personal notes, papers and records which are retained or discarded at the author’s discretion and over which the agency exercises no control or dominion (e.g., personal telephone lists) are not considered to be agency records within the meaning of the Privacy Act.”); *cf.* System of Records Notice, Employee Performance File System Records (OPM/GOVT-2), 71 Fed. Reg. 35347, 35348 (June 19, 2006) (“[W]hen supervisors/managers retain personal ‘supervisory’ notes, i.e., information on employees that the agency exercises no control [over] and does not require or specifically describe in its performance system, which remain solely for the personal use of the author and are not provided to any other person, and which are retained or discarded at the author’s sole discretion, such notes are not subject to the Privacy Act and are, therefore, not considered part of this system.”); Department of Justice Guide to the Freedom of Information Act 10 [hereinafter FOIA Guide] (analyzing concepts of agency records and personal records under FOIA), <https://www.justice.gov/oip/page/file/1199421/download#page=10>.

However, in Chapman v. NASA, 682 F.2d 526, 528-29 (5th Cir. 1982), the Court of Appeals for the Fifth Circuit, relying on the fair recordkeeping duties imposed by subsection (e)(5), ruled that private notes may “evanesce” into records subject to the Act when they are used to make a decision on the individual’s employment status well after the evaluation period for which they were compiled. See also Thompson v. Coast Guard, 547 F. Supp. 274, 283-84 (S.D. Fla. 1982) (holding timeliness requirement of

subsection (e)(5) met where private notes upon which disciplinary action is based are placed in system of records “contemporaneously with or within a reasonable time after an adverse disciplinary action is proposed”); cf. Risch v. Henderson, 128 F. Supp. 2d 437, 441 (E.D. Mich. 1999) (stating that “another person’s witnessing of a personal note converts it to a Level 2 – Supervisor’s Personnel Record, and therefore it is properly maintained under the Privacy Act” in a system of records in accordance with the agency manual).

Publicly available information can be a “record.”

Publicly available information, such as newspaper clippings or press releases, can constitute a “record.” See Clarkson v. IRS, 678 F.2d 1368, 1372-73 (11th Cir. 1982) (permitting subsection (e)(7) First Amendment challenge to agency’s maintenance of newsletters and press releases); Krieger v. DOJ, 529 F. Supp. 2d 29, 51 (D.D.C. 2008) (permitting subsection (e)(7) challenge to agency’s maintenance of copies of plaintiff’s speech announcements and publicly filed court complaint); see also OMB Supplementary Guidance, 40 Fed. Reg. at 56,742, https://www.justice.gov/paoverview_omb-75-suppl (“Collections of newspaper clippings or other published matter about an individual maintained other than in a conventional reference library would normally be a system of records.”); cf. Gerlich v. DOJ, 659 F. Supp. 2d 1, 12-16 (D.D.C. 2009) (concluding without discussing that “printouts” of “[i]nternet searches regarding [job] candidates’ political and ideological affiliations” constituted “records”), aff’d in part, rev’d in part & remanded, on other grounds, 711 F.3d 161 (D.C. Cir. 2013); Fisher, 934 F. Supp. at 469 (discussing difference between definition of “record” for purposes of FOIA and statutory definition under Privacy Act and rejecting argument, based on FOIA case law, that “library reference materials” are not covered by Privacy Act), 934 F. Supp. at 469 (discussing difference between definition of “record” for purposes of FOIA and statutory definition under Privacy Act and rejecting argument, based on FOIA case law, that “library reference materials” are not covered by Privacy Act).

One court has held that grand jury materials are not “records.”

One court has relied on non-Privacy Act case law concerning grand jury records to hold that a grand jury transcript, “though in possession of the U.S. Attorney, is not a record of the Justice Department within the meaning of the Privacy Act.” Kotmair v. DOJ, No. S 94-721, slip op. at 1 (D. Md. July 12, 1994) (citing United States v. Penrod, 609 F.2d 1092, 1097 (4th Cir. 1979), for above proposition, but then confusingly not applying same theory to

analysis of FOIA accessibility), aff'd, 42 F.3d 1386 (4th Cir. 1994) (unpublished table decision).

Agencies are not required to create "records."

The Privacy Act – like the FOIA – does not require agencies to create records that do not exist. See DeBold v. Stimson, 735 F.2d 1037, 1041 (7th Cir. 1984); see also, e.g., Villanueva v. DOJ, 782 F.2d 528, 532 (5th Cir. 1986) (rejecting argument that the FBI was required to “find a way to provide a brief but intelligible explanation for its decision . . . without [revealing exempt information]”). But see May v. Air Force, 777 F.2d 1012, 1015-17 (5th Cir. 1985) (singularly ruling that “reasonable segregation requirement” obligates agency to create and release typewritten version of handwritten evaluation forms so as not to reveal identity of evaluator under exemption (k)(7)). For further analysis of this principle, see the “Individual’s Right of Access” section below.

E. 5 U.S.C. § 552a(a)(5) - System of Records

“[T]he term ‘system of records’ means 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.” 5 U.S.C. § 552a(a)(5).

Comment:

To be a “system of records,” documents must be retrievable by, and agencies must actually retrieve them by, a personal identifier.

The statutory definition of a “system of records” requires that: (1) “there is an indexing or retrieval capability using identifying particulars built into the system”; and (2) the agency “does, in fact, retrieve records about individuals by reference to some personal identifier.” OMB 1975 Guidelines, 40 Fed. Reg. 28,948, 28,952 (July 9, 1975), https://www.justice.gov/paoverview_omb-75. The OMB 1975 Guidelines state that the “is retrieved by” criterion “implies that the grouping of records under the control of an agency is accessed by the agency by use of a personal identifier; not merely that a capability or potential for retrieval exists.” Id. (emphasis added).

By its very terms, the statute includes, as personal identifiers, items beyond the most commonly used name and social security number. As the Court of Appeals for the District of Columbia Circuit pointed out when considering a “photo file”:

Recall that a system of records is “a group of any records . . . 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.” 5 U.S.C. § 552a(a)(5) (emphasis added). The term “record” includes “any item . . . about an individual . . . 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.” Id. § 552a(a)(4) (emphasis added). Under the Act’s plain language, then, a “system of records” may be a group of any records retrieved by an identifying particular such as a photograph. In other words, the personal identifier may be the photograph itself.

Maydak v. United States, 363 F.3d 512, 519-20 (D.C. Cir. 2004) (remanding case to district court to determine whether prisons’ compilation of photographs constitutes system of records), on remand No. 1:97-cv-02199, slip op. at 2-4 (D.D.C. Mar. 30, 2006) (“Searching through a box or collection of unidentified photos with the hope of recognizing an inmate does not fit the definition because the photos are not ‘retrieved’ by any ‘assigned’ personal identifier.”), aff’d in part on other grounds, vacated in nonpertinent part, 630 F.3d 166, 179 (D.C. Cir. 2010) (electing to “simply assume, without deciding, that BOP’s review and retention of the duplicate photos constituted a ‘system of records’” and to “focus on whether Government officials acted intentionally or willfully to violate appellants’ rights under the Act”); see also Aguiar v. Recktenwald, No. 3:13-CV-2616, 2015 WL 4066703, at *2 (M.D. Pa. July 2, 2015) (finding Facebook account is not record under Privacy Act and that disclosure of account’s existence is information that is not maintained by BOP in its systems of records); 10 Ring Precision v. Jones, 722 F.3d 711, 725 (5th Cir. 2013) (finding that ATF’s “Firearms Tracing System is not a ‘system of records,’ because traces are conducted by entering an identifying characteristic of the firearm, not the individual, into ATF’s database”); Chambers vs. Interior, No. 05-0380, 2006 WL 8433911, at *4-5 (D.D.C. September 26, 2008) (finding performance evaluation at issue was retrievable by name which is linked directly to plaintiff but that genuine issue of fact existed whether supervisor’s hard copy “hot topics” file, electronic hard drive, or floppy disk was system of records, where defendant’s own witnesses provided conflicting evidence); but see Ingerman v. IRS, No. 89-5396, slip op. at 6 (D.N.J. Apr. 3, 1991) (“An individual’s social security number does not contain his name, identifying number, or other identifying particular. . . . [A] social security number is the individual’s identifying number, and therefore, it cannot qualify as a record under . . . the Privacy Act.”), aff’d, 953 F.2d 1380 (3d Cir. 1992) (unpublished table decision).

The Court of Appeals for the District of Columbia Circuit also concluded that to be a “system of records,” “it is not sufficient that an agency has the capability to retrieve information indexed under a person’s name, but the agency must in fact retrieve records in this way in order for a system of records to exist.” Henke v. Commerce, 83 F.3d 1453, 1460 n.12 (D.C. Cir. 1996); see also Elec. Privacy Info. Ctr. v. DHS, 653 F.3d 1, 8 (D.C. Cir. 2011) (“Even if . . . the [agency] has the ability to combine various sources of information and then to link names to the images produced using [advanced imaging technology], [the petitioners’] Privacy Act claim still fails because they offer no reason to believe the [agency] has in fact done that.” (citing Henke)); Chang v. Navy, 314 F. Supp. 2d 35, 41 (D.D.C. 2004) (“[A]n agency’s failure to acknowledge that it maintains a system of records will not protect the agency from statutory consequences if there is evidence that the agency in practice retrieves information about individuals by their names or personal identifiers. . . . [H]owever, mere retrievability – that is, the capability to retrieve – is not enough.”).

Generally, the “system of records” definition makes the method of retrieval of a record more important than the content of the record.

The highly technical “system of records” definition is perhaps the single most important Privacy Act concept, because (with some exceptions discussed below) it makes coverage under the Act dependent upon the method of retrieval of a record rather than its substantive content. See Baker v. Navy, 814 F.2d 1381, 1384 (9th Cir. 1987) (noting the “overwhelming support for using a record’s method of retrievability to determine the scope of accessibility”); see also Burton v. Wolf, 803 F. App’x 120, 122 (9th Cir. 2020) (concluding that records were not in a system of records under the Privacy Act because they were “retrievable only with the identifying information of his estranged wife in her A-File, not his own”); Kearns v. FAA, 312 F. Supp. 3d 97, 108 (D.D.C. 2018) (concluding that requested documents were not retrieved from system of records because they were not retrieved by plaintiff’s name or identifier but by the case number); Mulvey v. Hugler, No. 3:14-CV-01835, 2017 WL 1737851, at *7 (M.D. Tenn. May 4, 2017) (granting summary judgment because plaintiff failed to allege that email was retrieved from system of records and not simply reply which was copied to third person and because office email is not system of records); Lambert v. U.S., No. 3:15-CV-147, 2016 WL 632461, at *5 (E.D. Tenn. Feb. 17, 2016) (dismissing claim where no allegation was made that either ethics legal opinion or investigation files were actually retrieved by personal identifier); Barouch v. DOJ, No. 14-0552, 2015 WL 5544424, at *4-5 (D.D.C. Sept. 18, 2015) (finding audio recording located only in personal files of Special Agent was not contained in system of records); Corr v. Bureau of the Pub. Debt, 987 F. Supp. 2d 711, 720 (S.D.W. Va. 2013) (finding that “Administrative Inquiry File was retrievable only

by the names of [p]laintiff’s supervisors” and not contained in system of records retrievable by plaintiff’s name); Mata v. McHugh, No. 10-CV-838, 2012 WL 2376285, at *6 (W.D. Tex. June 22, 2012) (finding that “[p]laintiff’s resume was retrieved by his job description, not his name, and is thus not a record in a system of records”); Krieger v. DOJ, 529 F. Supp. 2d 29, 44-46 (D.D.C. 2008) (“That several of the documents do not fit th[e] description [of label used to retrieve them] does not mean that [agency employee] has intentionally evaded the provisions of the Privacy Act,” because “agency finding that employee seeking to find records relating to [plaintiff] would have to individually review each document” is not “an ‘actual practice of retrieval by name’” and “[b]ecause the agency’s press releases are actually retrieved by date and not by individual identifier, they cannot be characterized as included within a system of records.” (quoting McCready v. Nicholson, *infra*)); Lee v. Geren, 480 F. Supp. 2d 198, 207 (D.D.C. Mar. 29, 2007) (citing Henke and finding that record was not maintained in system of records because record was retrieved by log number that was “unrelated to specific individuals”); Lee v. DOJ, No. 04-1013, 2007 WL 2852538, at *9-10 (W.D. Pa. Sept. 27, 2007) (concluding that plaintiff’s wrongful disclosure claim must fail because record at issue was “retrieved by the name of the fugitive,” not by plaintiff’s name); Artz v. United States, No. 3:05-CV-51, 2007 WL 1175512, at *5 (D.N.D. Apr. 20, 2007) (maintaining that although the report named plaintiffs, it was not contained in a “system of records” because it was retrieved by date, not by plaintiffs’ names); Smith v. Henderson, No. C-99-4665, 1999 WL 1029862, at *5 (N.D. Cal. Oct. 29, 1999) (applying Henke and finding that “locked drawer containing a file folder in which [were] kept . . . notes or various other pieces of paper relating to special circumstances hires” did not constitute system of records because agency “did not utilize the drawer to systematically file and retrieve information about individuals indexed by their names”), *aff’d sub nom.* Smith v. Potter, 17 F. App’x 731 (9th Cir. 2001); Crumpton v. United States, 843 F. Supp. 751, 755-56 (D.D.C. 1994) (maintaining that although records disclosed to press under FOIA contained information about plaintiff, they were not retrieved by her name and therefore Privacy Act did not apply), *aff’d on other grounds sub nom.* Crumpton v. Stone, 59 F.3d 1400 (D.C. Cir. 1995); Shannon v. Gen. Elec. Co., 812 F. Supp. 308, 321 (N.D.N.Y. 1993) (determining method of retrieval rather than substantive content controls determination of whether record is in system of records).

Indeed, a major criticism of the Privacy Act is that it can easily be circumvented by not filing records in name-retrieved formats. See Privacy Commission Report, at 503-04 n.7, https://www.justice.gov/paoverview_ppsc. Recognizing this potential for abuse, some courts have relaxed the “actual retrieval” standard in particular cases (examples in cases cited below). Moreover, certain subsections of the Privacy Act have been construed to apply even to records not

incorporated into a “system of records.” See “Definition” of “5 U.S.C. § 552a(a)(5) - System of Records” analysis below.

The agency, rather than those outside the agency, must be in the practice of retrieving records by an identifying particular to meet the “system of records” definition.

Note also that the “practice of retrieval by name or other personal identifier must be an agency practice to create a system of records and not a ‘practice’ by those outside the agency.” McCready v. Nicholson, 465 F.3d 1, 13 (D.C. Cir. 2006) (holding that agency’s public website, which was not used by agency personnel to retrieve information by personal identifier, did not constitute a “system of records”). See also Yonemoto v. VA, No. 06-00378, 2007 WL 1310165, at *5-6 (D. Haw. May 2, 2007) (“[I]t was not the agency, but the public who caused [information contained in e-mails] to be retrieved. Just because an agency is capable of retrieving the information, and just because it does so to comply with a FOIA request, does not mean that the information is maintained in a Privacy Act ‘system of records.’”), appeal dismissed as moot, 305 F. App’x 333 (9th Cir. 2008); Freeman v. EPA, No. 02-0387, 2004 WL 2451409, at *11-12 (D.D.C. Oct. 25, 2004) (internal quotation marks omitted) (explaining that because agency’s search for records pursuant to FOIA request “will normally trigger a search beyond the narrow confines of a Privacy Act system of records,” it is not conclusive as to whether any responsive records would be “retrieved by [plaintiff’s] name or some other identifying particular assigned to the individual”).

Retrievability, alone, is not enough to be part of a “system of records.”

Courts have held that retrievability alone is insufficient to satisfy the system of records “retrieved by” requirement; the records must also be organized by personally identifying information. See In re 2122 21st Rd. N. Arlington, No. 1:17–CR–00236, 2018 WL 534161, at *4 (E.D. Va. Jan. 23, 2018) (reasoning that plaintiff failed to show that evidence seized during search conducted in criminal investigation constituted records “contained in a system of records” under Privacy Act); Lewis v. SSA, No. 9:14-CV-31, 2015 WL 9664967, at *5 (E.D. Tex. Dec. 7, 2015) (magistrate’s recommendation) (allowing case to proceed because pleadings did not rule out possibility that SSA had retrieved information by plaintiff’s name or by some identifying number, symbol, or other identifying particular), adopted, 2016 WL 81577 (E.D. Tex. Jan 06, 2016); Walia v. Holder, 59 F. Supp. 3d 492, 501-02 (E.D.N.Y. 2014) (finding disclosing agent acquired personal knowledge through contemporaneous conversations with plaintiff such that information did fall within exception from actual retrieval rule where personal knowledge of disclosed information was gained from investigation

disclosing party initiated); Mobley v. CIA, 924 F. Supp. 2d 24, 56 (D.D.C. 2013) (“Since the WISE database is essentially a database of e-mail messages, some of which are messages containing ‘open source media articles,’ . . . it is logical that such messages would not be organized by the name or personal identifying information of individuals discussed in such articles, and [plaintiff] has offered no evidence to contradict this explanation”); York v. McHugh, 850 F. Supp. 2d 305, 306, 314-315 (D.D.C. 2012) (holding where agency stored electronic documents containing plaintiff’s medical information in “shared network drive” accessible to other employees, shared drive did not constitute system of records even though this method of storage “allowed [plaintiff] to discover the files by searching the shared . . . drive for [her name]”; “The fact that some documents were labeled with [plaintiff’s] name does not convert the shared . . . drive into a system of records, particularly where there is no evidence that the agency used the shared drive to retrieve the personal information by personal identifiers and the drive was not created for employees to do so.”); Krieger, 529 F. Supp. 2d at 42-44, 45-46 (finding that plaintiff “offers no facts suggesting that [emails] would have been indexed by name, or that an electronic folder existed that grouped emails related to him by name or other identifier” and noting that “a search function does not [make it] a system of records”); Chang, 314 F. Supp. 2d at 41 (applying Henke and stating that “[p]laintiff’s assertion that it is ‘technically possible’ to retrieve the [document] by searching for [plaintiff’s] name is insufficient to meet the requirement that the data was retrieved in such a manner”); Fisher v. NIH, 934 F. Supp. 464, 472-73 (D.D.C. 1996) (applying Henke and stating: “[T]he primary practice and policy of the agency [during the time of the alleged disclosures] was to index and retrieve the investigatory files by the name of the institution in which the alleged misconduct occurred, rather than by the name of the individual scientist accused of committing the misconduct. The fact that it was possible to use the plaintiff’s name to identify a file containing information about the plaintiff is irrelevant.”), summary affirmance granted, No. 96-5252, 1996 WL 734079 (D.C. Cir. Nov. 27, 1996); Bequette v. USPS, No. 88-802, slip op. at 19-22 (E.D. Va. July 3, 1989) (finding that even though the agency “could retrieve . . . records by way of an individual’s name or other personal identifier,” that fact “does not make those records a Privacy Act system of records. The relevant inquiry is whether the records or the information they contain are [in fact] retrieved by name or other personal identifier.”).

Indeed, the issue in Henke was whether or not computerized databases that contained information concerning technology grant proposals submitted by businesses constituted a “system of records” as to individuals listed as the “contact persons” for the grant applications, where the agency had acknowledged that “it could theoretically retrieve information by the name of the contact person.” Id. at 1457-58. The D.C. Circuit looked to Congress’s use of

the words “is retrieved” in the statute’s definition of a system of records and focused on whether the agency “in practice” retrieved information. Id. at 1459-61. The court held that “in determining whether an agency maintains a system of records keyed to individuals, the court should view the entirety of the situation, including the agency’s function, the purpose for which the information was gathered, and the agency’s actual retrieval practice and policies.” Id. at 1461. Regarding the purpose for which the information was gathered, the court drew a distinction between information gathered for investigatory purposes and information gathered for administrative purposes. Id. at 1461. The court stated that where information is compiled about individuals “primarily for investigatory purposes, Privacy Act concerns are at their zenith, and if there is evidence of even a few retrievals of information keyed to individuals’ names, it may well be the case that the agency is maintaining a system of records.” Id. Applying this test, the D.C. Circuit determined that the agency did “not maintain a system of records keyed to individuals listed in the contact person fields of its databases” because the agency’s “purpose in requesting the name of a technical contact [was] essentially administrative and [was] not even necessary for the conduct of the [program’s] operations,” nor was there “any evidence that the names of contact persons [were] used regularly or even frequently to obtain information about those persons.” Id. at 1456, 1461-62.

Several courts have followed Henke insofar as it calls on them to “view the entirety of the situation, including the agency’s function, the purpose for which the information was gathered, and the agency’s actual retrieval practice and policies” in determining “whether an agency maintains a system of records keyed to individuals.” Id. at 1461. See Maydak, 363 F.3d at 520 (quoting Henke, remanding case to district court to determine whether prisons’ compilation of photographs constituted system of records, and instructing district court to “take into account ‘the entirety of the situation, including the agency’s function, the purpose for which the information was gathered, and the agency’s actual retrieval practices and policies’”); Pippinger v. Rubin, 129 F.3d 519, 526-27 (10th Cir. 1997) (finding approach in Henke “instructive” and holding that under “a properly ‘narrow’ construction of 5 U.S.C. § 552a(a)(5),” an IRS database containing an “abstraction” of information from two existing Privacy Act systems did not constitute new system of records because it could be “accessed only by the same users, and only for the same purposes, as those published in the Federal Register for the original ‘system[s] of records’”); Sussman v. Marshals Serv., 657 F. Supp. 2d 25, 27-28 (D.D.C. 2009) (“Given the function of the Marshals Service, Privacy Act concerns are at their zenith . . . [T]he Marshals Service’s declarations do not establish a record that sufficiently explains the purpose for which all of the information on Sussman was gathered, or its actual retrieval practice and policies for the information maintained in various locations

on Sussman”), on remand from 494 F.3d 1106 (D.C. Cir. 2007); Koenig v. Navy, No. 05-35, 2005 WL 3560626, at *4 (S.D. Tex. Dec. 29, 2005) (“[A]lthough neither party presented any evidence regarding where or in what manner the request for medical leave was kept, common sense and experience in an office setting lead to the conclusion that the record was most likely either kept in a file with the plaintiff’s name on it, or entered into her leave record, which also would have been accessible by her name or social security number.”); Doe v. Veneman, 230 F. Supp. 2d 739, 752 (W.D. Tex. 2002) (quoting language from Henke regarding “even a few retrievals,” and determining that noninvestigatory information “[e]ll within the ambit of the Privacy Act” where information could “be retrieved by personal identifiers” and information was maintained in “single data repository from which more than 200 different types of reports [we]re generated,” all from raw data entered into system), aff’d in pertinent part, rev’d & remanded on other grounds, 380 F.3d 807 (5th Cir. 2004); Walker v. Ashcroft, No. 99-2385, slip op. at 17-18 (D.D.C. Apr. 30, 2001) (alternative holding) (applying Henke and finding no evidence that FBI “independently collected, gathered or maintained” document containing plaintiff’s prescription drug information given to FBI by state investigator, or that FBI “could, in practice, actually retrieve the record by reference to [plaintiff’s] name”), summary affirmance granted on other grounds, No. 01-5222, 2002 U.S. App. LEXIS 2485 (D.C. Cir. Jan. 25, 2002); Alexander v. FBI, 193 F.R.D. 1, 6-8 (D.D.C. 2000) (applying Henke and finding that agency maintained system of records, considering “purpose for which the information was gathered and the ordinary retrieval practices and procedures”), mandamus denied per curiam sub nom. In re: Exec. Office of the President, 215 F.3d 20 (D.C. Cir. 2000); cf. Gerlich v. DOJ, 711 F.3d 161, 168 (D.C. Cir. 2013) (holding that because “[a]ppellants’ argument regarding the ‘functional’ incorporation of the [records] into the Department’s system of records appears only in a footnote to their opening brief” and appellant failed to make this argument in district court, appellants’ “functional” argument “that the lack of physical incorporation into a system of records is not dispositive of the question whether the record at issue were ‘functionally’ and thus legally, within an appropriate personnel records system” was not properly before circuit court), aff’d in part & rev’d in part, 659 F. Supp. 2d 1 (D.D.C. 2009). But see Williams v. VA, 104 F.3d 670, 676 (4th Cir. 1997) (finding “narrow Henke rationale – that since this document was not in practice *actually* retrieved ‘by the name of the individual or by some identifying number,’ 5 U.S.C. § 552a(a)(5), it cannot be a record within a ‘system of records’ – unconvincing in these circumstances where there appears to exist already a formal system of records of which the [document] may be a part”).

1. Systems of Records and Disclosures under Subsection (b)

a. Retrieved from System of Records

A record is “disclosed” under the Privacy Act only if it is retrieved from a system of records.

Subsection 552a(b), discussed in detail below under “Conditions of Disclosure to Third Parties,” prohibits only the disclosure of records that are retrieved from a system of records. 5 U.S.C. § 552a(a)(5), (b); see also, e.g., Paige v. DEA, 665 F.3d 1355, 1359-61 (D.C. Cir. 2012) (concluding that disclosure of video excerpted from longer video did not violate Privacy Act because video was not retrievable by appellant’s name or other personal identifier at time it was created and, therefore, was not record contained in system of records; “disclosure of [excerpted video] was not prohibited simply because [it] *subsequently* became a ‘record which is contained in a system of records’); Doe v. VA, 519 F.3d 456 (8th Cir. 2008) (finding Congress intended to limit liability for disclosures to a record “contained in a system of records”); Harris v. Holder, 885 F. Supp. 2d 390, 401 (D.D.C. 2012) (finding plaintiff’s complaint failed to state how an offending record with respect to an investigation was “about” plaintiff or was retrieved by plaintiff’s name or other personal identifier); White v. Schafer, 738 F. Supp. 2d 1121, 1139-40 (D. Colo. 2010) (holding plaintiff, who claimed that agency disclosed investigatory report in violation of subsection (b), failed to present evidence that report “was maintained within and retrieved from a ‘system of records’”), aff’d, 435 F. App’x 764 (10th Cir. 2011); Bechhoefer v. DOJ, 179 F. Supp. 2d 93, 95-101 (W.D.N.Y. 2001) (finding that disclosed record “never became a part of a system of records” where DEA agent “stuck [record] in his desk drawer along with a number of [f] other miscellaneous documents, and later retrieved it from that drawer, from his own memory and personal knowledge of where he kept it”; and noting that plaintiff’s allegation that agent looked at plaintiff’s name on record to retrieve it from drawer “confuses retrieving a document with identifying the document”; “If one is looking for a letter from a particular person, one will probably look at the name on the letter in order to identify it as the letter being sought. If that letter is in a stack of unrelated, miscellaneous documents, however, it cannot be said to be contained within a group of records organized in such a fashion that information can be retrieved by an individual’s name.”), aff’d, 312 F.3d 563, 567-68 & n.1 (2d Cir. 2002) (concluding that an “assortment of papers excluded from the agency’s formal files because they are deemed not relevant to the agency’s mission and left in a desk drawer are not part of

the agency's system of records, to which the obligations of the Act apply" and accordingly, finding no need to consider agency's further argument concerning single instance of retrieval by individual's name); Barhorst v. Marsh, 765 F. Supp. 995, 999-1000 (E.D. Mo. 1991) (dismissing plaintiff's claim under subsection (b) on alternative grounds because record was retrieved by job announcement number rather than individual's name and "'mere potential for retrieval' by name or other identifier is insufficient to satisfy the 'system of records' requirement" (quoting Fagot v. FDIC, 584 F. Supp. 1168, 1175 (D.P.R. 1984), aff'd in part & rev'd in part, 760 F.2d 252 (1st Cir. 1985) (unpublished table decision)); cf. Corey v. McNamara, 265 F. App'x 555, 557 (9th Cir. 2008) (finding that appellant "offered no evidence to counter [agency's] evidence that [appellant's] documentation, the disclosure of which forms the basis of [his] federal action, is not part of the [agency's] 'system of records'"); Gadd v. United States, No. 4:08CV04229, 2010 WL 60953, at *11 (E.D. Ark. Jan. 5, 2010) (concluding that DEA did not disclose record within system of records because plaintiff, DEA employee, "was the source of the medical records in dispute" and did not allege or present evidence that DEA disclosed documents initially obtained from system of records), aff'd per curiam, 392 F. App'x 503 (8th Cir. 2010); Smith v. BOP, No. 05-1824, 2006 WL 950372, at *3 (D. Md. Apr. 11, 2006) (finding "no basis in the Privacy Act for the conclusion that the Act's elaborate record-keeping and notice requirements apply" where plaintiff's "single item of correspondence" was intercepted in conformity with BOP regulations). But see Wall v. IRS, No. 1:88-CV-1942, 1989 U.S. Dist. LEXIS 9427, at *4-7 (N.D. Ga. July 5, 1989) (explaining that because agency official retrieved applicant's folder by name from file maintained under vacancy announcement number, records were kept within "system of records" and thus subsection (b) was applicable).

Similarly, the disclosure of information "acquired from non-record sources – such as observation, office emails, discussions with co-workers and the 'rumor mill' – does not violate the Privacy Act ... even if the information disclosed is also contained in agency records." Dick v. Holder, 67 F. Supp. 3d 167, 180 (D.D.C. 2014), citing Cloonan v. Holder, 768 F. Supp. 2d 154, 164 (D.D.C. 2011) (citations omitted); see also deLeon v. Wilkie, No. CV 19-1250, 2020 WL 210089, at *9 (D.D.C. Jan. 14, 2020) (concluding that because security officer "had personal knowledge of Plaintiff's physical altercation . . . and would have known about any ensuing disciplinary action," the disclosure of information did not violate the Privacy Act). Krieger v. DOJ, 529 F. Supp. 2d 29, 47 (D.D.C. 2008) (citations omitted) (finding that disclosure of information "derived solely

from independent sources is not prohibited by the statute even though identical information may be contained in an agency system of records”).

Several courts have stated that the first element a plaintiff must prove in a wrongful disclosure suit is that the information disclosed is a record within a system of records. See Jacobs v. Nat’l Drug Intel. Ctr., 423 F.3d 512, 516 (5th Cir. 2005); Davis v. Runyon, No. 96-4400, 1998 WL 96558, at *4-5 (6th Cir. Feb. 23, 1998) (affirming district court’s dismissal of wrongful disclosure claim pursuant to the Privacy Act where appellant’s factual allegations failed to indicate whether “‘information’ was a ‘record’ contained in a ‘system of records,’” whether it was “disclos[ed] within the meaning of the Act,” whether disclosure had “adverse effect,” or whether disclosure was “willful or intentional”); Quinn v. Stone, 978 F.2d 126, 131 (3d Cir. 1992); Atkins v. Mabus, No. 12cv1390, 2013 WL 524061, at *2-3 (S.D. Cal. Feb. 11, 2013); York v. McHugh, 850 F. Supp. 2d 305, 312 (D.D.C. 2012) (concluding that files at issue were not contained in a system of records because system was “not set up for employees to retrieve records by use of personal identifiers” and plaintiff did not submit evidence to establish that “agency in practice retrieves information about individuals by their names or personal identifiers”) (internal citations omitted); Harris, 885 F. Supp. 2d at 400-01; Al-Dahir v. Hamlin, No. 10-2571, 2011 WL 1666894, at *4 (D. Kan. May 3, 2011); Cloonan v. Holder, 768 F. Supp. 2d 154, 163 (D.D.C. 2011); Feldman v. CIA, 797 F. Supp. 2d 29, 38 (D.D.C. 2011); Banks v. Butler, No. 5:08cv336, 2010 WL 4537902, at *6 (S.D. Miss. Sept. 23, 2010) (magistrate’s recommendation), adopted, 2010 WL 4537909 (S.D. Miss. Nov. 2, 2010); White v. Schafer, 738 F. Supp. 2d at 1139-40; Walker v. Gambrell, 647 F. Supp. 2d 529, 536 (D. Md. 2009); Doe v. Treasury, 706 F. Supp. 2d 1, 6 (D.D.C. 2009); Armstrong v. Geithner, 610 F. Supp. 2d 66, 70 (D.D.C. 2009), aff’d, 608 F.3d 854 (D.C. Cir. 2010); Shutte v. IRS, No. 08-CV-2013, 2008 WL 2114920, at *2 (N.D. Iowa May 19, 2008); Mittleman v. Treasury, 919 F. Supp. 461, 468 (D.D.C. 1995) (“Undisputed evidence of record reveals that only a statement of general provisions of law was made to [newspaper columnist], not disclosure of information retained in [agency’s] records on [plaintiff]” and, therefore, general disclosure provisions of Privacy Act were not implicated), aff’d in part & remanded in part, on other grounds, 104 F.3d 410 (D.C. Cir. 1997); Hass v. Air Force, 848 F. Supp. 926, 932 (D. Kan. 1994); Bernson v. ICC, 625 F. Supp. 10, 13 (D. Mass. 1984) (finding plaintiff’s complaint failed to present a proper Privacy Act claim because disclosed information came from plaintiff’s tax record, not agency record system). But cf. Doe v. USPS, 317 F.3d 339, 342-43 (D.C. Cir. 2003) (precluding summary judgement because appellant’s claim sufficiently alleged that his supervisor told co-workers

of his HIV status after learning of status from appellant's Privacy Act-protected Family and Medical Leave Act form even though "evidence of retrieval [wa]s purely circumstantial" and noting "plaintiffs can rarely produce direct evidence that the government has disclosed confidential information obtained from their private records, requiring such evidence would eviscerate the protections of the Privacy Act").

The Court of Appeals for the First Circuit has gone so far as to hold that a complaint that fails to allege a disclosure from a system of records is facially deficient, and some district courts in other jurisdictions have taken the same approach. Beaulieu v. IRS, 865 F.2d 1351, 1352 (1st Cir. 1989); see also Cross v. Potter, No. 3:09-CV-1293, 2013 WL 1149525, at *10 (N.D.N.Y. Mar. 19, 2013); Zahedi v. DOJ, No. 10-694, 2011 WL 1872206, at *4 (D. Or. May 16, 2011); Del Fuoco v. O'Neill, No. 8:09-CV-1262, 2011 WL 601645, at *9-10 & n.13 (M.D. Fla. Feb. 11, 2011) (finding plaintiff's complaint insufficient because he failed to properly allege his record was from system of records even though DOJ stamped the record as confidential which implied DOJ considered record protected by Privacy Act); Thomas v. USPS, No. 3:10-CV-1091, slip op. at 7-8 (N.D. Tex. Nov. 3, 2010); Mumme v. Labor, 150 F. Supp. 2d 162, 175 (D. Me. 2001), aff'd, No. 01-2256 (1st Cir. June 12, 2002).

However, other courts have not held pleadings in Privacy Act cases to the same strict standard. The D.C. Circuit, for example, concluded that a plaintiff need not identify the particular records that were improperly disclosed because the complaint properly put the government on notice and alleged the essential elements of his claim, by alleging that "records concerning [himself] were wrongfully disclosed." Krieger v. Fadely, 211 F.3d 134, 136-37 (D.C. Cir. 2000) ("If his lawsuit went forward, there would come a time when [plaintiff] would have to identify the particular records [defendant] unlawfully disclosed. But that point surely was not as early as the pleading stage."); see also Feldman, 797 F. Supp. 2d at 41 (explaining that circuit court case law did not require plaintiff to allege full details of disclosure at pleading stage, noting "in the typical case, a plaintiff can hardly be expected to know the full details behind an improper disclosure prior to discovery, since those details are most likely to be under the control of the defendant"); Tripp v. DOD, 193 F. Supp. 2d 229, 237 (D.D.C. 2002) (following Krieger and "the liberal pleading standard permitted by the Federal Rules of Civil Procedure"); Tripp v. DOD, 219 F. Supp. 2d 85, 89-91 (D.D.C. 2002) (considering complaint that alleged "specific defendant repeatedly released information about plaintiff to the press and public that is contained in a Privacy Act system

of records, including but not limited to the contents of plaintiff's security forms and other personnel files," and following Krieger to hold that Rule 8 of the Federal Rules of Civil Procedure "does not require plaintiff to plead facts to further elaborate which records were released, by which DOD officials, to which members of the press or public, or on which specific dates"); Johnson v. Rinaldi, No. 1:99CV170, 2001 WL 677306, at *5-6 (M.D.N.C. Apr. 13, 2001) (stating that "Federal Rules of Civil Procedure require only that the complaint put Defendants on notice" and that plaintiff "need not use the exact words 'record' or 'system of records' or state facts sufficient to show that the documents in dispute meet those legal definitions"); cf. Wade v. Donahoe, Nos. 11-3795, 11-4584, 2012 WL 3844380, at *10 (E.D. Pa. Sept. 4, 2012) (finding that plaintiffs must identify Privacy Act provision agency violated in order to meet pleading requirements of Rule 8 of Federal Rules of Civil Procedure); Sterling v. United States, 798 F. Supp. 47, 49 (D.D.C. 1992) ("[P]laintiff is not barred from stating a claim for monetary damages [under (g)(1)(D)] merely because the record did not contain 'personal information' about him and was not retrieved through a search of indices bearing his name or other identifying characteristics."), subsequent related opinion, Sterling v. United States, 826 F. Supp. 570, 571-72 (D.D.C. 1993), summary affirmance granted, No. 93-5264, 1994 WL 88894 (D.C. Cir. Mar. 11, 1994).

It is not enough, however, for a plaintiff claiming that an agency disclosed information in violation of subsection (b) to show that the information was contained in any system of records maintained by the agency. See Sussman v. Marshals Serv., 494 F.3d 1106, 1123 (D.C. Cir. 2007). Rather, the plaintiff "must show [that] the [agency] improperly disclosed materials located in records retrievable by [the plaintiff's] name as opposed to someone else's name." Id. The plaintiff in Sussman alleged that the agency disclosed information about him in violation of subsection (b). The Marshals Service did "not deny[] the materials were in a system of records" but argued that "[t]he information was not maintained in a system of records retrievable by [the plaintiff's] name, but by [another individual's] name." Id. Reasoning in part that it "must construe § 552a(g)(1)(D)'s waiver of sovereign immunity narrowly," the D.C. Circuit held that "for his action to survive, [the plaintiff] must present evidence that materials from records about him, which the [agency] retrieved by his name, were improperly disclosed." Id.

Courts have held that information taken from a record in a system of records remains protected, even if later incorporated into a record that is not maintained in a system of records.

Furthermore, information taken from a protected record in a system of records, but subsequently incorporated into a record that is not maintained in a system of records, can nonetheless itself be deemed a protected record. See e.g., Jacobs, 423 F.3d at 516-519 (ruling that disclosure of executive summary, which was not retrieved by plaintiff's name but was created from information in system of records that was so retrieved, was from system of records); see also Bartel v. FAA, 725 F.2d 1403, 1407-09 (D.C. Cir. 1984) (finding that letters that communicated sensitive information contained in report of investigation, which was "a record" maintained in "a system of records," triggered disclosure provisions of the Privacy Act even though letters were not themselves considered "records," because "an absolute policy of limiting the Act's coverage to information physically retrieved from a record would make little sense in terms of [Privacy Act's] underlying purpose"); Chang v. Navy, 314 F. Supp. 2d 35, 41 (D.D.C. 2004) (maintaining that, although it was undisputed that documents at issue – press release and "information paper" containing details of plaintiff's non-judicial punishment – were not retrieved from system of records, information from system of records had been disclosed because "underlying documents, from which the documents were compiled, were contained in a system of records").

Similarly, the First Circuit held that "the unauthorized disclosure by one agency of protected information obtained from a record in another agency's system is a prohibited disclosure under the Act, unless the disclosure falls within the statutory exceptions." Orekoya v. Mooney, 330 F.3d 1, 6-7 (1st Cir. 2003), abrogated on other grounds, Doe v. Chao, 540 U.S. 614 (2004); Doe v. Treasury, 706 F. Supp. 2d at 6 ("[T]he Privacy Act only covers disclosures of information which was either directly or indirectly retrieved from a system of records." (quoting Fisher v. NIH, 934 F. Supp. 464, 473 (D.D.C. 1996))). In Orekoya, the First Circuit, although ultimately affirming the district court on other grounds, disagreed with the district court's determination that such a disclosure was not a violation of the Privacy Act and stated that the language of the Privacy Act "does not support the view that an agency may immunize itself from liability by obtaining information from a different agency's system of records and then saying its further unauthorized disclosure is protected because its own system of records was not the original source." Id.

b. Actual Retrieval

Generally, a “disclosure” requires that the record be actually retrieved from a system of records; a disclosure made on the basis of knowledge acquired independent of actual retrieval from an agency’s system of records is not enough, even when the information happens to be in a system of records.

Although subsection (b) “does not specifically require that the information disclosed be retrieved directly from” a record contained in a system of records, “courts generally apply some type of retrieval requirement to give effect to the meaning and purpose of the Privacy Act.” Doe v. VA, 519 F.3d at 464 (Hansen, J., concurring); *see also, e.g., Armstrong v. Geithner*, 608 F.3d 854, 857 (D.C. Cir. 2010) (“To be actionable . . . a disclosure generally must be the result of someone having actually retrieved the ‘record’ from th[e] ‘system of records’; the disclosure of information is not ordinarily a violation ‘merely because the information happens to be contained in the records.’” (quoting Bartel v. FAA, 725 F.2d at 1408)); Doe v. VA, 519 F.3d at 461 (“[T]he only disclosure actionable under section 552a(b) is one resulting from a retrieval of the information initially and directly from the record contained in the system of records.” (quoting Olberding v. DOD, 709 F.2d 621, 622 (8th Cir. 1983)); Cloonan, 768 F. Supp. 2d at 164 (“[D]efinition [of ‘system of records’] – which incorporates the requirement that information ‘is retrieved’ – has given rise to the so-called ‘retrieval rule’ under the Privacy Act”). Thus, it has frequently been held that subsection (b) is not violated when a disclosure is made on the basis of knowledge acquired independent of actual retrieval from an agency’s system of records (such as a disclosure purely from memory), regardless of whether the identical information also happens to be contained in the agency’s systems of records.

The leading case articulating the “actual retrieval” and “independent knowledge” concepts is Savarese v. HEW, 479 F. Supp. 304, 308 (N.D. Ga. 1979), aff’d, 620 F.2d 298 (5th Cir. 1980) (unpublished table decision), in which the court ruled that for a disclosure to be covered by subsection (b), “there must have initially been a retrieval from the system of records which was at some point a source of the information.” 479 F. Supp. at 308. In adopting this stringent “actual retrieval” test, the court in Savarese reasoned that a more relaxed rule could result in excessive governmental liability, or an unworkable requirement that agency employees “have a pansophic recall concerning every record within every system of records within the agency.” Id.

There are numerous subsection (b) cases that follow Savarese and apply the “actual retrieval” and “independent knowledge” concepts in varying factual situations. See, e.g., Doe v. VA, 519 F.3d at 460-63; Kline v. HHS, 927 F.2d 522, 524 (10th Cir. 1991); Manuel v. VA Hosp., 857 F.2d 1112, 1119-20 (6th Cir. 1988); Boyd v. Sec’y of the Navy, 709 F.2d 684, 687 (11th Cir. 1983) (per curiam); Thomas v. Energy, 719 F.2d 342, 344-46 (10th Cir. 1983); Doyle v. Behan, 670 F.2d 535, 538-39 & n.5 (5th Cir. 1982) (per curiam); Hanley v. DOJ, 623 F.2d 1138, 1139 (6th Cir. 1980) (per curiam); Marquez v. Johnson, No. 11-cv-545, 2012 WL 6618238, at *11 (D. Colo. Dec. 19, 2012), aff’d, 545 F. App’x 735 (10th Cir. 2013); deLeon v. Wilkie, No. 19-CV-1250, 2020 WL 210089, at *9 (D.D.C. Jan. 14, 2020) (finding that agency had not improperly disclosed records where plaintiff had not established that agency employee “retrieved any record” and employee who disclosed information “had personal knowledge” of plaintiff’s actions and “disclosure of information acquired from an independent source – including personal knowledge – does not violate the Act”); Minshev v. Donley, 911 F. Supp. 2d 1043, 1070-72 (D. Nev. 2012); Doe v. Treasury, 706 F. Supp. 2d at 9-11 (D.D.C. 2009); Tarullo v. Def. Contract Audit Agency, 600 F. Supp. 2d 352, 360-61 (D. Conn. 2009); Balbinot v. United States, 872 F. Supp. 546, 549-51 (C.D. Ill. 1994); Coakley v. DOT, No. 93-1420, 1994 WL 16953072, at *1 (D.D.C. Apr. 7, 1994); Olberding v. DOD, 564 F. Supp. 907, 913 (S.D. Iowa 1982), aff’d per curiam, 709 F.2d 621 (8th Cir. 1983); Gibbs v. Brady, 773 F. Supp. 454, 458 (D.D.C. 1991); McGregor v. Greer, 748 F. Supp. 881, 885-86 (D.D.C. 1990); Krowitz v. USDA, 641 F. Supp. 1536, 1545 (W.D. Mich. 1986), aff’d, 826 F.2d 1063 (6th Cir. 1987) (unpublished table decision); Howard v. Marsh, 654 F. Supp. 853, 855 (E.D. Mo. 1986); Johnson v. Air Force, 526 F. Supp. 679, 681 (W.D. Okla. 1980), aff’d, 703 F.2d 583 (Fed. Cir. 1981) (unpublished table decision); Jackson v. VA, 503 F. Supp. 653, 655-57 (N.D. Ill. 1980); King v. Califano, 471 F. Supp. 180, 181 (D.D.C. 1979); see also Armstrong, 608 F.3d at 858-60 (affirming district court finding that plaintiff failed to establish information disclosed was retrieved from record in system of records where agency employee disclosed information regarding investigation of plaintiff from independent sources – her own “‘observations and speculation’ or ‘those of others,’ or information ‘from the rumor mill’”); Reed v. Navy, 910 F. Supp. 2d 32, 41 (D.D.C. 2012) (finding disclosures “were clearly derived from ‘records’” because defendant “did not personally witness any of the alleged incidents, nor did he disclose information gleaned from the ‘rumor mill’”; rather disclosures “were based on the report and other written documents that became part of the investigative case file”); Cloonan, 768 F. Supp. 2d at 169 (“[O]n its face, the language of the . . . letter is replete with references to ‘the record’ and

‘documentation’ from which a reasonable juror could conclude that the preparer of the document did in fact review, and is referring to, agency records.”); Finnerty v. USPS, No. 03-558, 2006 WL 54345, at *11-13 (D.N.J. Jan. 9, 2006) (“The fact that the memorandum documenting [a witness’] observations may have been simultaneously circulated to recipients and directed to a file and thereafter maintained as a ‘record’ in a ‘system of records’ does not change the fact that [the witness’] source of the information was his own observation, and not a retrieval of information from a system of records.”); Drapeau v. United States, No. Civ. 04-4091, 2006 WL 517646, at *6-7 (D.S.D. Mar. 1, 2006) (finding that disclosed information from agency employees regarding plaintiff’s dismissal for rules violation was not obtained from record in system of records but from employee who observed violation); Krieger v. Fadely, 199 F.R.D. 10, 13 (D.D.C. 2001) (ruling that discovery request seeking all communications that supervisor had with anyone, irrespective of relation between communication and Privacy Act-protected record, was overbroad, and stating that Privacy Act “does not create a monastic vow of silence which prohibits governmental employees from telling others what they saw and heard merely because what they saw or heard may also be the topic of a record in a protected file”); Fisher v. NIH, 934 F. Supp. 464, 473-74 (D.D.C. 1996) (holding that plaintiff failed to demonstrate that individuals who disclosed information learned it from investigatory file or through direct involvement in investigation), summary affirmance granted, No. 96-5252, 1996 WL 734079 (D.C. Cir. Nov. 27, 1996); Viotti v. Air Force, 902 F. Supp. 1331, 1338 (D. Colo. 1995) (“Section 552a(b) contemplates a ‘system of records’ as being the direct or indirect source of the information disclosed” and although agency employee admitted disclosure of information to press “based on personal knowledge,” plaintiff “was obligated to come forward with some evidence indicating the existence of a triable issue of fact as to the identity of the ‘indirect’ source”), aff’d, 153 F.3d 730 (10th Cir. 1998) (unpublished table decision); Mittleman, 919 F. Supp. at 469 (maintaining that although no evidence indicated that there had been disclosure of information about plaintiff, information at issue would not have been subject to restrictions of Privacy Act because “it was a belief . . . derived from conversations . . . and which was acquired independent from a system of records”); Stephens v. TVA, 754 F. Supp. 579, 582 (E.D. Tenn. 1990) (comparing Olberding and Jackson and noting “confusion in the law with respect to whether the Privacy Act bars the disclosure of personal information obtained indirectly as opposed to directly from a system of records”); cf. Rice v. United States, 166 F.3d 1088, 1092 n.4 (10th Cir. 1999) (noting that, in action for wrongful disclosure in violation of tax code, plaintiff had no

Privacy Act claim for IRS's disclosure in press releases because agency official procured disclosed information from review of indictment and attendance at plaintiff's trial and sentencing); Feldman, 797 F. Supp. 2d at 41 (Feldman v. C.I.A., 797 F. Supp. 2d 29, 41 (D.D.C. 2011) (concluding that plaintiff's motion was sufficient to survive motion to dismiss where it alleged that "person who fed the rumor mill the contents of a record that had been retrieved from a system of records may have violated the Privacy Act" (quoting Armstrong, 608 F.3d at 860)); Smith v. Henderson, No. C-96-4665, 1999 WL 1029862, at *6-7 (N.D. Cal. Oct. 29, 1999) (although finding no evidence of existence of written record retrieved from system of records, concluding that alleged disclosure was made from information "obtained independently of any system of records"), aff'd sub nom. Smith v. Potter, 17 F. App'x 731 (9th Cir. 2001).

In most courts, the "actual retrieval" requirement does not apply if the agency official disclosing the record also had a role in creating the record.

However, the Court of Appeals for the District of Columbia Circuit, in Bartel v. FAA, 725 F.2d 1403 (D.C. Cir. 1984), held that the "actual retrieval" standard is inapplicable where a disclosure is undertaken by agency personnel who had a role in creating the record that contains the released information. In other words, the "independent knowledge" defense is not available to agency personnel who were involved in creating the record. Id. at 1408-11. This particular aspect of Bartel has been noted with approval by several other courts. See Manuel, 857 F.2d at 1120 & n.1; Minshew, 911 F. Supp. 2d at 1072 (finding that "source of the disclosure was the record [that the supervisor] had a role in creating and maintaining, where there is no evidence presented that [supervisor] had independent knowledge"); Longtin v. DOJ, No. 06-1302, 2006 WL 2223999, at *3 (D.D.C. Aug. 3, 2006) (following Bartel and finding reasonable agency's argument that requested disclosure of records concerning third-party criminal case would violate the Privacy Act by disclosing what was contained in a record that [official] had a primary role in creating); Stokes v. SSA, 292 F. Supp. 2d 178, 181 (D. Me. 2003) ("[A]gency employees who . . . create or initiate records are not shielded from the Privacy Act merely because they do not have to consult or retrieve those records before disclosing the information that they contain."); Pilon v. DOJ, 796 F. Supp. 7, 12 (D.D.C. 1992) (denying agency's motion to dismiss, or alternatively, for summary judgment where information "obviously stem[med] from confidential Department documents and oral statements derived therefrom"); Kassel v. VA, 709 F. Supp. 1194, 1201 (D.N.H. 1989); cf. Walia v. Holder, 59 F. Supp. 3d 492, 503 (E.D.N.Y. 2014) (distinguishing Bartel

OVERVIEW OF THE PRIVACY ACT

where plaintiff could not “reasonably deny” that employee who disclosed information learned “from his personal experience and contemporaneous conversations with the Plaintiff and other agents” rather than from records in a system of records); Armstrong, 608 F.3d at 860 (explaining that “[t]he exception we suggested in Bartel does not extend to this case [in which employee who disclosed information] neither acquired the information . . . in any way related to a record, as an investigator might have done, nor used the record in her work for the agency”); Cloonan, 768 F. Supp. 2d at 156, 165-67 (holding that Bartel exception is “inapplicable” where plaintiff’s supervisor, who had been “involved in several interagency complaints and proceedings” with plaintiff, disclosed information critical of plaintiff’s performance because “[t]here is no evidence upon which the Court can conclude that any information [disclosed by supervisor] was learned by [supervisor] during the course of any investigation that he ordered, undertook or oversaw”); Doe v. Treasury, 706 F. Supp. 2d at 8-9 (declining to apply Bartel exception where IRS employee disclosed information about investigation, which he acquired from press release and from his own involvement in investigation, because he did not “institute” investigation, did not have a “primary role in creating and using” information, and did not acquire information from “record-related role”); Krieger v. DOJ, 529 F. Supp. 2d 29, 48 (D.D.C. 2008) (distinguishing Bartel, and finding no wrongful disclosures); Carlson v. GSA, No. 04-C-7937, 2006 WL 3409150, at *3-4 (N.D. Ill. Nov. 21, 2006) (finding that supervisor’s email detailing employee’s settlement of his wrongful termination claims was “‘communication’ of a protected ‘record’” even though supervisor, who conducted investigation that resulted in settlement, “compiled the email from his own memory”). But cf. Abernethy v. IRS, 909 F. Supp. 1562, 1570 (N.D. Ga. 1995) (holding that alleged statements made to other IRS employees that plaintiff was being investigated pertaining to allegations of EEO violations, assuming they were in fact made, did not violate Privacy Act “because the information allegedly disclosed was not actually retrieved from a system of records” even though individual alleged to have made such statements was same individual who ordered investigation), aff’d per curiam, No. 95-9489, 108 F.3d 343 (11th Cir. Feb. 13, 1997) (unpublished table decision).

The Court of Appeals for the Ninth Circuit followed the approach taken by the D.C. Circuit in Bartel, and also concluded that the “actual retrieval” standard is inapplicable where a disclosure is undertaken by agency personnel who had a role in creating the record that contains the released information. Wilborn v. HHS, 49 F.3d 597, 600-02 (9th Cir. 1995).

Specifically, the court held that an Administrative Law Judge (“ALJ”) for the Department of Health and Human Services violated the Privacy Act when he stated in an opinion that one of the parties’ attorneys had been placed on a Performance Improvement Plan (“PIP”) while he was employed at HHS – despite the fact that there was no actual retrieval by the ALJ – because, as the creator of the PIP, the ALJ had personal knowledge of the matter. The Ninth Circuit noted the similarity of the facts to those of Bartel and held that “‘independent knowledge,’ gained by the creation of records, cannot be used to sidestep the Privacy Act.” Id. at 601. Additionally, it rejected the lower court’s reasoning that not only was there no retrieval, but there was no longer a record capable of being retrieved because as the result of a grievance action, all records relating to the PIP had been required to be expunged from the agency’s records and in fact were expunged by the ALJ himself. Id. at 601-02. The Ninth Circuit found the district court’s ruling “inconsistent with the spirit of the Privacy Act,” and stated that the “fact that the agency ordered expungement of all information relating to the PIP makes the ALJ’s disclosure, if anything, more rather than less objectionable.” Id. at 602.

The Court of Appeals for the Eighth Circuit, however, has twice taken a narrow view of the “actual retrieval” standard. In a per curiam decision in Olberding v. DOD, 709 F.2d 621 (8th Cir. 1983), the court ruled that information orally disclosed by a military psychiatrist to the plaintiff’s commanding general, revealing the results of the plaintiff’s examination – which had not yet been put in writing – was not retrieved from a “record.” Id. at 621 (adopting reasoning of trial court, which found that the conversation took place before the report was written, 564 F. Supp. 907, 910 (S.D. Iowa 1982)). Subsequently, in Doe v. VA, the court ruled that there was no actual retrieval from a record where a VA physician revealed an employee’s HIV status and marijuana use to a union representative because the physician recalled the information exclusively from discussions during employee’s medical appointments, not from any subsequent review of his medical notes. 519 F.3d at 459-62. Although the court purported to distinguish Bartel and Wilborn, id. at 462-63, Judge Hanson stated in his concurring opinion that were he not bound by Olberding, he would adopt a “scrivener’s exception” in order to “justify an exception to the general retrieval rule, particularly where ‘a mechanical application of the rule would thwart, rather than advance, the purpose of the Privacy Act.’” Id. at 464-65 (quoting Wilborn, 49 F.3d at 600).

2. Systems of Records and Access and Amendment under Subsections (d)(1) and (d)(2)

One of Congress's underlying concerns in narrowly defining a "system of records" appears to have been efficiency – i.e., a concern that any broader definition would require elaborate cross-references among records and/or burdensome hand-searches for records. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,957, https://www.justice.gov/paoverview_omb-75. As the Fifth Circuit has stated, the "system of records" requirement "reflects a statutory compromise between affording individuals access to those records relating directly to them and protecting federal agencies from the burdensome task of searching through agency records for mere mention of an individual's name." Betterworth v. FDIC, 248 F.3d 386, 391 (5th Cir. 2001); see also Baker v. Navy, 814 F.2d 1381, 1385 (9th Cir. 1987); Carpenter v. IRS, 938 F. Supp. 521, 522-23 (S.D. Ind. 1996).

If a record is not retrieved by a personal identifier, it is not part of a "system of records" and the Privacy Act's access and amendment provisions generally do not apply.

Consistent with OMB's guidance, numerous courts have held that, under subsection (d)(1), an individual has no Privacy Act right of access to his record if it is not retrieved by his name or personal identifier. See Mobley v. CIA, 806 F.3d 568, 587 (D.C. Cir. 2015) (concluding plaintiff was not entitled to documents where agency official claimed that it did not organize records "by individuals who may be mentioned in those records," or "retrieve records about individuals from that database by use of an individual's name or personal identifier as a matter of practice."); Betterworth v. FDIC, 248 F.3d at 391-92; Gowan v. Air Force, 148 F.3d 1182, 1191 (10th Cir. 1998); Williams v. VA, 104 F.3d 670, 673 (4th Cir. 1997); Henke, 83 F.3d at 1458-62 (D.C. Cir. 1996); Manuel v. VA Hosp., 857 F.2d 1112, 1116-17 (6th Cir. 1988); Baker, 814 F.2d at 1383-84; Cuccaro v. Sec'y of Labor, 770 F.2d 355, 360-61 (3d Cir. 1985); Wren v. Heckler, 744 F.2d 86, 89 (10th Cir. 1984); Greenlaw v. Scalia, No. 18-CV-04932, 2020 WL 4001461, at *5 (N.D. Cal. July 15, 2020); Kearns v. FAA, 312 F. Supp. 3d 97, 108 (D.D.C. 2018); Corr v. Bureau of the Pub. Debt, 987 F. Supp. 2d 711, 720 (S.D. W.Va. 2013); Augustus v. McHugh, 825 F. Supp. 2d 245, 256-57 (D.D.C. 2011); Jackson v. Shinseki, No. 10-cv-02596, 2011 WL 3568025, at *6 (D. Colo. Aug. 9, 2011), *aff'd*, 526 F. App'x 814 (10th Cir. 2013); McCready v. Principi, 297 F. Supp. 2d 178, 188 (D.D.C. 2003), *rev'd in part on other grounds sub nom. McCready*, 465 F.3d at 1; Springmann v. State, No. 93-1238, slip op. at 9 n.2 (D.D.C. Apr. 21, 1997); Fuller v. IRS, No. 96-888, 1997 WL 191034, at *3-5 (W.D. Pa. Mar. 4, 1997);

Carpenter, 938 F. Supp. at 522-23; Quinn v. HHS, 838 F. Supp. 70, 76 (W.D.N.Y. 1993); Shewchun v. Customs Serv., No. 87-2967, 1989 WL 7351, at *2 (D.D.C. Jan. 11, 1989); Bryant v. Air Force, No. 85-4096, slip op. at 4 (D.D.C. Mar. 31, 1986); Fagot v. FDIC, 584 F. Supp. 1168, 1174-75 (D.P.R. 1984), aff'd in part & rev'd in part, 760 F.2d 252 (1st Cir. 1985) (unpublished table decision); Grachow v. Customs Serv., 504 F. Supp. 632, 634-36 (D.D.C. 1980); Smiertka v. Treasury, 447 F. Supp. 221, 228 (D.D.C. 1978), remanded on other grounds, 604 F.2d 698 (D.C. Cir. 1979); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,957 (giving examples), https://www.justice.gov/paoverview_omb-75.

Likewise, with regard to amendment under subsection (d)(2), several courts have ruled that where an individual's record is being maintained allegedly in violation of subsection (e)(1) or (e)(5), the individual has no Privacy Act right to amend his record under subsection (d)(2), if it is not retrieved by his name or personal identifier. See, e.g., Baker, 814 F.2d at 1384-85 ("the scope of accessibility and the scope of amendment are coextensive"); Clarkson v. IRS, 678 F.2d 1368, 1376-77 (11th Cir. 1982) (maintaining that although subsections (e)(1) and (e)(5) apply only to records contained in a system of records, "find[ing] it both necessary and appropriate to construe the plain meaning of the language of subsections (d)(2) and (d)(3) to authorize the amendment or expungement of all records which are maintained in violation of subsection (e)(7)"); Seldowitz v. OIG of State, No. 99-1031, slip op. at 19-23 (E.D. Va. June 21, 2002), aff'd per curiam, 95 F. App'x 465 (4th Cir. 2004); Pototsky v. Navy, 717 F. Supp. 20, 22 (D. Mass. 1989) (following Baker), aff'd per curiam, 907 F.2d 142 (1st Cir. 1990) (unpublished table decision).

The D.C. Circuit, however, has recognized that "[t]he Privacy Act also offers relief for some claims based on the government's information that is not 'within a system of records,'" including "misstatements contained in a disparaging Inspector General's report and associated agency documents" and "when an 'adverse determination is made' by the agency that maintained the flawed record or by an outside actor." Liff v. OIG for Labor, 881 F.3d 912, 923 (D.C. Cir. 2018) (quoting McCready v. Nicholson, supra); see also Gerlich v. DOJ, 711 F.3d 161, 169 (D.C. Cir. 2013) (noting that "[t]he obligations the Privacy Act established in subsection (e)(5) . . . apply even when the agency does not maintain the records at issue in its system of records"); McCready, 465 F.3d at 10-12 (holding that subsection (g)(1)(C), the civil remedy provision for violations of subsection (e)(5), "applies to any record, and not [just] any record within a system of records" (internal quotation marks omitted)), discussed, below, under "Protections for Records

not within a System of Records.”

With regards to the Privacy Act’s access and amendment provisions, courts have generally not permitted agencies to purposefully file records in an effort to evade retrieving by individual identifier.

However, with respect to access under subsection (d)(1), and amendment under subsection (d)(2), some courts have cautioned that an agency’s purposeful filing of records in a non-name-retrieved format, in order to evade those provisions, will not be permitted. *See, e.g., Pototsky v. Navy*, No. 89-1891, slip op. at 2 (1st Cir. Apr. 3, 1990) (per curiam); *Manuel*, 857 F.2d at 1120 (“The Court does not want to give a signal to federal agencies that they should evade their responsibility to place records within their ‘system of records’ in violation of the [Act].”); *Baker*, 814 F.2d at 1385; *Kalmin v. Navy*, 605 F. Supp. 1492, 1495 n.5 (D.D.C. 1985).

Several, but not all, courts have required agencies to keep adverse action records in a system of records, and therefore subject to the Privacy Act’s access and amendment provisions.

Following the rationale of the Fifth Circuit in *Chapman v. NASA*, 682 F.2d 526, 529 (5th Cir. 1982), several courts have recognized a subsection (e)(5) duty to incorporate records into a system of records – thus making them subject to access and amendment – where such records are used by the agency in taking an adverse action against the individual. *See MacDonald v. VA*, No. 87-544-CIV-T-15A, slip op. at 2-5 (M.D. Fla. Feb. 8, 1988); *Lawrence v. Dole*, No. 83-2876, slip op. at 5-6 (D.D.C. Dec. 12, 1985); *Waldrop v. Air Force*, 3 Gov’t Disclosure Serv. (P-H) ¶ 83,016, at 83,453 (S.D. Ill. Aug. 5, 1981); *Nelson v. EEOC*, No. 83-C-983, slip op. at 6-11 (E.D. Wis. Feb. 14, 1984); *cf. Manuel*, 857 F.2d at 1117-19 (asserting that there is no duty to place records within system of records where records “are not part of an official agency investigation into activities of the individual requesting the records, and where the records requested do not have an adverse effect on the individual”).

The D.C. Circuit, however, interpreted the rule differently in an unusual situation, i.e., where the agency’s regulations exempted such documents from its records. *See Horowitz v. Peace Corps*, 428 F.3d 271, 280-81 (D.C. Cir. 2005). In *Horowitz*, the court denied the plaintiff access to a draft Administrative Separation Report (“ASR”) that was not in a “system of records” where the “Peace Corps’s regulations dictate that an ASR should not be maintained in the agency’s records if a volunteer resigns prior to an

official decision to administratively separate him.” Because “the Peace Corps’s manual states that an ASR should not even be completed if a volunteer resigns before such a decision is made” and plaintiff “resigned before any final decision was made, the report was never completed and pursuant to the procedure specified by the manual was not maintained in the Peace Corps’s official files.” In addition, the court held that the plaintiff had not shown that the agency “nevertheless placed the draft ASR in a ‘system of records’” because the draft ASR was stored in Peace Corps’s Country Director’s safe and plaintiff “has not shown that files in the safe are, in practice, retrieved by individuals’ names.” See also Gowan v. Air Force, No. 90-94, slip op. at 7, 11, 13, 16, 30, 33 (D.N.M. Sept. 1, 1995) (finding access claim moot, “personal notes and legal research” in file “marked ‘Ethics’” that were originally kept in desk of Deputy Staff Judge Advocate but that was later given to Criminal Military Justice Section and used in connection with court martial hearing were not in system of records for purposes of either Privacy Act access or accuracy lawsuit for damages), aff’d, 148 F.3d 1182, 1191 (10th Cir. 1998) (concluding that “the word ‘Ethics’ was not a personal identifier” and stating that it did “not find the district court’s rulings regarding those documents to be clearly erroneous”).

3. Protections for Records Not Within a System of Records

The “system of records” threshold requirement is not a requirement for the application of all subsections of the Act. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,952, https://www.justice.gov/paoverview_omb-75 (system of records definition “limits the applicability of some of the provisions of the Act”) (emphasis added). But see Privacy Commission Report, at 503-04, https://www.justice.gov/paoverview_ppsc (assuming that definition limits entire Act); cf. Henke v. Commerce, 83 F.3d 1453, 1459 (D.C. Cir. 1996) (“[T]he determination that a system of records exists triggers virtually all of the other substantive provisions of the Privacy Act.”); McCready v. Principi, 297 F. Supp. 2d 178, 185 (D.D.C. 2003) (“For almost all circumstances, the Act extends only to those records that are in a ‘system of records’ which is a specific term of art.”), aff’d in part & rev’d in part sub nom. McCready v. Nicholson, 465 F.3d 1 (D.C. Cir. 2006), 465 F.3d 1 (D.C. Cir. 2006).

Records describing how individuals exercise First Amendment rights are protected under the Privacy Act, even if not maintained in a system of records.

Importantly, the D.C. Circuit has held that subsection (e)(7) – which restricts agencies from maintaining records describing how an individual exercises his First Amendment rights – applies even to records not incorporated into a

system of records. Albright v. United States, 631 F.2d 915, 918-20 (D.C. Cir. 1980). Albright involved a challenge on subsection (e)(7) grounds to an agency's maintenance of a videotape – kept in a file cabinet in an envelope that was not labeled by any individual's name – of a meeting between a personnel officer and agency employees affected by the officer's job reclassification decision. Id. at 918. Relying on both the broad definition of "maintain," 5 U.S.C. § 552a(a)(3), and the "special and sensitive treatment accorded First Amendment rights," the D.C. Circuit held that the mere collection of a record regarding those rights could be a violation of subsection (e)(7), regardless of whether the record was contained in a system of records retrieved by an individual's name or personal identifier. Id. at 919-20; see also Maydak v. United States, 363 F.3d 512, 516, 518-19 (D.C. Cir. 2004) (reaffirming holding in Albright).

Albright's broad construction of subsection (e)(7) has been adopted by several other courts. See MacPherson v. IRS, 803 F.2d 479, 481 (9th Cir. 1986); Boyd v. Sec'y of Navy, 709 F.2d 684, 687 (11th Cir. 1983); Clarkson v. IRS, 678 F.2d 1373, 1373-77 (11th Cir. 1982); Gerlich v. DOJ, 659 F. Supp. 2d 1, 13-15 (D.D.C. 2009), aff'd in part, rev'd in part & remanded, on other grounds, 711 F.3d 161 (D.C. Cir. 2013); Fagot v. FDIC, 584 F. Supp. 1168, 1175 (D.P.R. 1984). Further, the Court of Appeals for the Eleventh Circuit in Clarkson, held that, at least with respect to alleged violations of subsection (e)(7), the Act's amendment provision (subsection (d)(2)) also can apply to a record not incorporated into a system of records. Clarkson, 678 F.2d at 1375-77. However, Judge Tjoflat's concurring opinion in Clarkson intimated that something more than a bare allegation of a subsection (e)(7) violation would be necessary in order for an agency to be obligated to search beyond its systems of records for potentially offensive materials. Id. at 1378-79.

The D.C. Circuit also held that the "system of records" requirement does not apply in subsection (g)(1)(C) lawsuits challenging the accuracy of records.

In McCready v. Nicholson, 465 F.3d 1, 10-12 (D.C. Cir. 2006), the D.C. Circuit went even further and held that the terms of subsection (g)(1)(C) – the judicial remedy provision for subsection (e)(5) violations – "[do] not incorporate or otherwise refer to the Act's definition of a 'system of records' found in § 552a(a)(5)." The D.C. Circuit stated that the "distinction between a claim that requires a system of records and a claim under § 552a(g)(1)(C) that does not require a system of records makes perfect sense." Id. Unlike other types of Privacy Act claims, which are shielded by the system of records definition in order to avoid "costly fishing expeditions," the D.C. Circuit reasoned, subsection (g)(1)(C) claims do not implicate "[t]his

legitimate concern with preserving an agency's resources" because "an individual and an agency already have identified the record at issue, that record is therefore easily retrieved, and the only issue is the accuracy of the record." Id. See also Gerlich, 659 F. Supp. 2d at 15-16 (relying on McCready v. Nicholson to conclude that the system of records requirement did not apply to plaintiffs' claim under subsections (e)(5) and (g)(1)(C)), aff'd in part, rev'd in part & remanded, on other grounds, 711 F.3d 161 (D.C. Cir. 2013).

Courts have varied on the extent to which they would extend coverage of other Privacy Act provisions to records that are not maintained in a system of records.

Some district courts have similarly extended the coverage of other Privacy Act provisions to records that are not maintained in a system of records. See Connelly v. Comptroller of the Currency, 673 F. Supp. 1419, 1424 (S.D. Tex. 1987) (construing "any record" language contained in 5 U.S.C. § 552a(g)(1)(C) to permit a damages action arising from an allegedly inaccurate record that was not incorporated into a system of records), rev'd on other grounds, 876 F.2d 1209 (5th Cir. 1989); Reuber v. United States, No. 81-1857, slip op. at 5 (D.D.C. Oct. 27, 1982) (relying on Albright for proposition that subsections (d)(2), (e)(1)-(2), (e)(5)-(7), and (e)(10) all apply to a record not incorporated into a system of records), partial summary judgment denied (D.D.C. Aug. 15, 1983), partial summary judgment granted (D.D.C. Apr. 13, 1984), subsequent decision (D.D.C. Sept. 6, 1984), aff'd on other grounds, 829 F.2d 133 (D.C. Cir. 1987); cf. Fiorella v. HEW, 2 Gov't Disclosure Serv. (P-H) ¶ 81,363, at 81,946 n.1 (W.D. Wash. Mar. 9, 1981) (noting that subsections (e)(5) and (e)(7) "are parallel in structure and would seem to require the same statutory construction").

However, the D.C. Circuit has declined to extend the holding in Albright to certain other subsections of § 552a(e). See Maydak v. United States, 363 F.3d 512, 517-19 (D.C. Cir. 2004). In Maydak, the Court of Appeals held that in accordance with OMB guidelines and regulations, the requirements contained in subsections (e)(1), (2), (3), and (10) are "triggered only if the records are actually incorporated into a system of records." Id. The D.C. Circuit explained that it reached a different conclusion as to subsection (e)(7) in Albright because of "Congress'[s] own special concern for the protection of First Amendment rights." Id. at 518 (quoting Albright, 631 F.2d at 919). The court stated that "at least in comparison to the other subsections at issue, subsection 552a(e)(7) proves the exception rather than the rule." Id. at 519. See also Augustus v. McHugh, 825 F. Supp. 2d 245, 257-260 (D.D.C. 2011) (rejecting claims alleging violations of subsections (e)(2), (e)(4), and

(e)(10), and Army regulations implementing (e)(3), because plaintiff failed to show that records at issue were contained in system of records); Gerlich, 659 F. Supp. 2d at 16 (“[S]ubsections (e)(1), (e)(2), (e)(6), (e)(9), and (e)(10) . . . only apply to records that are contained within a ‘system of records.’”), aff’d in part, rev’d in part & remanded, on other grounds, 711 F.3d 161 (D.C. Cir. 2013); Krieger v. DOJ, 529 F. Supp. 2d 29, 50-56 (D.D.C. 2008) (finding that subsections (e)(1), (4), (6), (9), and (10) apply only to records contained in a system of records); cf. Thompson v. State, No. 03-2227, 400 F. Supp. 1, 12 (D.D.C. 2005) (following Maydak and observing that “[i]t is not at all clear that subsection (e)(2) applies where the requested information never becomes part of [the] system”), aff’d, 210 F. App’x 5 (D.C. Cir. 2006).

Other courts have also declined to follow the D.C. Circuit’s Albright decision and have limited the applicability of the Privacy Act requirements that are contained in subsections other than (e)(7) to records that are maintained in a system of records. See, e.g., Gowan v. Air Force, 148 F.3d 1182, 1192 (10th Cir. 1998) (holding that appellant “ha[d] no § 552a(e)(5) cause of action” for maintenance of report that was not maintained in system of records); Clarkson, 678 F.2d at 1377 (declining to extend Albright rationale to subsections (e)(1) and (e)(5)); Bettsworth v. FDIC, No. A-97-CA-624, slip op. at 10 (W.D. Tex. Feb. 1, 2000) (magistrate’s recommendation) (recognizing holding in Connelly, but noting that both subsections (d)(1) and (g)(1)(C) contain same “system of records” language, and stating that court is “unpersuaded that Congress intended any other meaning than what has previously been applied”), adopted, (W.D. Tex. Feb. 17, 2000), aff’d on other grounds, 248 F.3d 386 (5th Cir. 2001); Felsen v. HHS, No. CCB-95-975, slip op. at 61-62, 65 (D. Md. Sept. 30, 1998) (granting defendants summary judgment on alternative ground that subsection (e)(2) is inapplicable to records not included in system of records); Barhorst v. Marsh, 765 F. Supp. 995, 999-1000 (E.D. Mo. 1991) (dismissing, on alternative grounds, Privacy Act claims under subsections (b), (e)(1)-(3), (e)(5)-(6), and (e)(10) because of finding that information was not in system of records; information was retrieved by job announcement number, not by name or other identifying particular).

Albright and its progeny establish that the “system of records” limitation on the scope of the Privacy Act is not uniformly applicable to all of the Act’s subsections. As is apparent from the above discussion, there has been some uncertainty about which particular subsections of the statute are limited to records contained in a “system of records.”

CONDITIONS OF DISCLOSURE TO THIRD PARTIES

The general rule under the Privacy Act is that an agency cannot disclose a record contained in a system of records unless the individual to whom the record pertains gives prior written consent to the disclosure. There are twelve exceptions to this general rule.

A. The “No Disclosure without Consent” Rule

“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 [subject to 12 exceptions].” 5 U.S.C. § 552a(b).

Comment:

Under the Privacy Act’s disclosure provision, agencies generally are prohibited from disclosing records by any means of communication – written, oral, electronic, or mechanical – without the written consent of the individual, subject to twelve exceptions.

Federal officials handling personal information are “bound by the Privacy Act not to disclose any personal information and to take certain precautions to keep personal information confidential.” Big Ridge, Inc. v. Fed. Mine Safety & Health Review Comm’n, 715 F.3d 631, 650 (7th Cir. 2013); *see also, e.g., Navy, Navy Exch., Naval Training Station, Naval Hosp. v. FLRA*, 975 F.2d 348, 350 (7th Cir. 1992) (noting that “Privacy Act generally prohibits the federal government from disclosing personal information about an individual without the individual’s consent”).

A “disclosure” can be by any means of communication – written, oral, electronic, or mechanical. *See* OMB 1975 Guidelines, 40 Fed. Reg. at 28,953, https://www.justice.gov/paoverview_omb-75; Bartel v. FAA, 725 F.2d 1403, 1409 (D.C. Cir. 1984) (concluding that “an absolute policy of limiting the Act’s coverage to information physically retrieved from a record would make little sense in terms of its underlying purpose” and that Privacy Act “forbids nonconsensual disclosure of records “by any means of communication”); *see also, e.g., Speaker v. HHS Ctrs. for Disease Control & Prevention*, 623 F.3d 1371, 1382 n.11 (11th Cir. 2010) (“Numerous courts have held that the Privacy Act protects against improper oral disclosures.”); Jacobs v. Nat’l Drug Intelligence Ctr., 423 F.3d 512, 517-19 (5th Cir. 2005) (rejecting argument that “the [Privacy Act] only protects against the disclosure of a physical document that is contained in a system of

records,” and holding that “damaging information . . . taken from a protected record and inserted into a new document, which was then disclosed without the plaintiff’s consent,” violated subsection (b) because “the new document is also a protected record”); Orekoya v. Mooney, 330 F.3d 1, 6 (1st Cir. 2003) (“The Privacy Act prohibits more than dissemination of records themselves, but also ‘nonconsensual disclosure of any information that has been retrieved from a protected record’” (quoting Bartel v. FAA, 725 F.2d at 1408)); Boyd v. United States, 932 F. Supp. 2d 830, 835 (S.D. Ohio 2013) (“[w]hile the term ‘disclosure’ is not defined by the statute, it has been interpreted broadly”); Cloonan v. Holder, 768 F. Supp. 2d 154, 163 (D.D.C. 2011) (citing Bartel, 725 F.2d at 1408); Chang v. Navy, 314 F. Supp. 2d 35, 41 n.2 (D.D.C. 2004) (citing Bartel, 725 F.2d at 1408).

OMB guidelines, and some, but not all, courts have advised that disclosures can occur by either transferring a record or simply “granting access” to a record.

Further, a disclosure under the Privacy Act “may be either the transfer of a record or the granting of access to a record.” OMB 1975 Guidelines, 40 Fed. Reg. at 28953 (July 9, 1975), https://www.justice.gov/paoverview_omb-75; see also Wilkerson v. Shinseki, 606 F.3d 1256, 1268 (10th Cir. 2010) (interpreting disclosure under the Privacy Act “liberally to include not only the physical disclosure of the records, but also the accessing of private records”). Regarding actionability, however, the United States Court of Appeals for the District of Columbia Circuit has required that a record actually be retrieved. Armstrong v. Geithner, 608 F.3d 854, 857 (D.C. Cir. 2010) (quoting Bartel, 725 F.2d at 1408, and holding that, to be actionable, “a disclosure generally must be the result of someone having actually retrieved the ‘record’ from that ‘system of records’; the disclosure of information is not ordinarily a violation ‘merely because the information happens to be contained in the records’”); Lambert v. United States, No. 3:15-CV-147-PLR-HBG, 2016 WL 632461, at *4-5 (E.D. Tenn. Feb. 17, 2016). *But see* Atkins v. Mabus, No. 12CV1390-GPC, 2014 WL 2705204, at *4-8 (S.D. Cal. June 13, 2014) (holding unauthorized access not actionable under Privacy Act, even though plaintiff’s declaration provided support for conclusion that defendant’s employees individually improperly accessed plaintiff’s private medical data); Cacho v. Chertoff, No. 06-00292(ESH), 2006 WL 3422548, at *5 (D.D.C. Nov. 28, 2006) (“[A] plaintiff cannot establish a prima facie claim under the Privacy Act simply by showing that the agency official who disclosed a protected record should never have accessed the record in the first place.”); Smith v. VA, No. CIV-06-865-R, 2007 WL 9711018 (W.D. Okla. Sept. 12, 2007) (dismissing claim of improper disclosure under subsection (b) in spite of evidence suggesting agency’s employee had unauthorized access to plaintiff’s personnel file, because agency had complied with all safeguards of Privacy Act, and had not acted intentionally or willfully to disclose, defined as “to ‘open up,’

‘to expose to view,’ or ‘to make known, . . . especially to reveal in words’” (citations omitted)).

A disclosure of information from a non-record source does not violate the Privacy Act’s disclosure provision.

The disclosure of information “acquired from non-record sources – such as observation, office emails, discussions with co-workers and the ‘rumor mill’ – does not violate the Privacy Act . . . even if the information disclosed is also contained in agency records.” Lambert v. United States at *5 (quoting Cloonan, 768 F. Supp. 2d. at 164); Thompson v. BOP, No. 1:10-CV-00578-JOF, 2012 WL 13072105, at *5 (N.D. Ga. Jan. 20, 2012) (For “a disclosure to be covered by section 552a(b), there must have initially been a retrieval from the system of records which was at some point a source of the information.” (citations omitted)); Savage v. Geren, No. CV-08-S-2189-NE, 2010 WL 11519448, at *13 (N.D. Ala. Nov. 15, 2010) (“[T]he Privacy Act does not prohibit disclosure of information or knowledge obtained from other sources other than ‘records.’...In particular, it does not prevent federal employees or officials from talking – even gossiping – about anything of which they have non-record-based knowledge.” (citations omitted)).

For further discussion of the meaning of “disclosure” of records, see the “Definitions, Systems of Records and Disclosures under Subsection (b)” section above.

In one case in which a plaintiff sought relief for alleged wrongful disclosure of items seized during the execution of a search warrant, the court found, “Appellant has failed to show that evidence seized during a search conducted in a criminal investigation constitutes records that are “contained in a system of records” under the Privacy Act. Matter of Search of 2122 21st Rd. N. Arlington, Virginia, No. 1:17-CR-00236, 2018 WL 534161, at *4 (E.D. Va. Jan. 23, 2018), aff’d sub nom. U.S. v. Search of 2122 21st Rd. N. Arlington, Virginia, 735 F. App’x 66 (4th Cir. 2018). Id. at *4.

Plaintiffs maintain the burden of demonstrating that a disclosure by an agency occurred.

A plaintiff has the burden of demonstrating that a “disclosure” by the agency has occurred. See, e.g., Askew v. United States, 680 F.2d 1206, 1209-11 (8th Cir. 1982); Zerilli v. Smith, 656 F.2d 705, 715-16 (D.C. Cir. 1981); Boyd v. United States, 932 F. Supp. 2d 830, 835 (S.D. Ohio 2013); cf. Hernandez v. Johnson, 514 F. App’x 492, 500 (5th Cir. 2013) (holding that “disclosure is not actionable because it identified [plaintiff] only by his first name and neither recipient knew who

'Jaime' was"); Luster v. Vilsack, 667 F.3d 1089, 1097-98 (10th Cir. 2011) (rejecting appellant's contentions that "mere transmission of the documents to a fax machine at which unauthorized persons might have viewed the documents constitutes a prohibited disclosure" and that "the possibility that a record might be revealed to unauthorized readers by negligent or reckless transmission is sufficient to constitute a prohibited disclosure under the Act"); Whyde v. Rockwell Int'l Corp., 101 F. App'x 997, 1000 (6th Cir. 2004) ("[T]he fact that [a company] somehow came into possession of documents that might have been included in plaintiff's personnel file . . . gives rise only to a metaphysical doubt as to the existence of a genuine issue of material fact."); Brown v. Snow, 94 F. App'x 369, 372 (7th Cir. 2004) (ruling that district court grant of summary judgment was proper where no evidence was found that record was disclosed, and stating that "burden is on the plaintiff at the summary judgment stage to come forward with specific evidence"); Lennon v. Rubin, 166 F.3d 6, 10-11 (1st Cir. 1999) (where agency employee testified that, despite memorandum indicating otherwise, she had disclosed information only within agency, and where plaintiff responded that whether his file was reviewed by other individuals is question of fact he "want[ed] decided by a fact finder, 'not an affidavit,'" finding such "arguments misapprehend [plaintiff's] burden at the summary judgment stage"); Russell v. Potter, No. 3:08-CV-2272, 2011 WL 1375165, at *9 (N.D. Tex. Mar. 4, 2011) (holding that plaintiff cannot prove disclosure violation where "the only agency involved, the Postal Service, received rather than 'disclosed' the information in question"); Collins v. FBI, No. 10-cv-03470, 2011 WL 1627025, at *7 (D.N.J. Apr. 28, 2011) (dismissing claim and stating that plaintiff's "conclusory allegations" of unlawful disclosure, "without identifying or describing who acted against Plaintiff or what the person did, is insufficient"); Roggio v. FBI, No. 08-4991, 2009 WL 2460780, at *2 (D.N.J. Aug. 11, 2009) (concluding that plaintiffs "fail[ed] to allege sufficient facts supporting that the FBI, as opposed to some other law enforcement body, disclosed [one plaintiff's] rap sheet" on the Internet, where plaintiffs "base[d] their allegation on . . . the mere fact that [a particular Internet] posting contained some expunged information"), reconsideration denied, No. 08-4991, 2009 WL 2634631 (D.N.J. Aug. 26, 2009); Walia v. Chertoff, No. 06-cv-6587, 2008 WL 5246014, at *11 (E.D.N.Y. Dec. 17, 2008) (concluding that plaintiff failed to make out prima facie case under subsection (b) of Privacy Act because plaintiff alleged merely that records were accessible to other individuals in office, rather than that they were actually disclosed); Buckles v. Indian Health Serv., 310 F. Supp. 2d 1060, 1068 (D.N.D. 2004) (finding that plaintiffs failed to "prove, by a preponderance of the evidence, that IHS disclosed protected information" where plaintiffs did not "have personal knowledge that [the memorandum was disclosed]" and witnesses at trial denied disclosing or receiving memorandum); Meldrum v. USPS, No. 5:97CV1482, slip op. at 11 (N.D. Ohio Jan. 21, 1999) (finding lack of

evidence that disclosure occurred where plaintiff alleged that, among other things, file had been left in unsecured file cabinet), aff'd per curiam, No. 99-3397, 2000 WL 1477495, at *2 (6th Cir. Sept. 25, 2000). But cf. Speaker, 623 F.3d at 1386 (finding plaintiff's complaint sufficient to survive summary judgment because he "need not prove his case on the pleadings" but rather "must merely provide enough factual material to raise a reasonable inference, and thus a plausible claim, that the [Ctrs. for Disease Control & Prevention] was the source of the disclosures"); Ciralsky v. CIA, 689 F. Supp. 2d 141, 156-57 (D.D.C. 2010) (concluding that plaintiff's allegation of CIA disclosure to unidentified government officials, who were unrelated to handling of plaintiff's case, was "not unacceptably vague" and need not include identities of alleged recipients for CIA to "understand Plaintiff's charge"); Tolbert-Smith v. Chu, 714 F. Supp. 2d 37, 43 (D.D.C. 2010) (ruling that plaintiff had stated claim for relief under Privacy Act where plaintiff "pled that a member of [agency] management placed records referring and relating to her disability on a server accessible by other federal employees and members of the public").

Direct evidence that an agency disclosed a record is generally not required, but plaintiffs must produce more than mere speculation or conjecture.

Circumstantial evidence may be sufficient to prove an unauthorized disclosure occurred, although courts generally require corroborating evidence, rather than mere speculation or conjecture. Because "plaintiffs can rarely produce direct evidence that the government has disclosed confidential information obtained from their private records, requiring such evidence would eviscerate the protections of the Privacy Act." Speaker v. HHS Ctrs. for Disease Control & Prevention, No. 1:09-CV-1137-WSD, 2012 WL 13071495, at * 20 (N.D. Ga. Mar. 14, 2012) (citing Doe v. USPS, 317 F.3d 339, 343 (D.C. Cir. 2003); Drennon-Gala v. Holder, No. 1:08-CV-3210-JEC, 2011 WL 1225784 (N.D. Ga. Mar. 30, 2011).

At least one court has held that there will be an "adverse inference" against an agency that destroys evidence in order to undermine the plaintiff's ability to prove that a disclosure occurred.

One district court has concluded that when an agency destroys evidence in order to undermine the plaintiff's ability to prove that a disclosure occurred, there will be an adverse inference against the agency. See Beaven v. DOJ, No. 03-84, 2007 WL 1032301, at *17 (E.D. Ky. Mar. 30, 2007) (concluding that "whether by use of the adverse inference" or "by a preponderance of the evidence" standard, "officials who inspected the folder found evidence that an inmate had tampered with it," and finding that "disclosure" occurred in violation of Privacy Act), aff'd in part, rev'd in part & remanded, on other grounds, 622 F.3d 540 (6th Cir. 2010).

Many, but not all, courts have held that a disclosure does not occur if the disclosure is to a person who was already aware of the information.

Many, but not all, courts have held that a “disclosure” under the Privacy Act does not occur if the communication is to a person who is already aware of the information. See, e.g., Hoffman v. Rubin, 193 F.3d 959, 966 (8th Cir. 1999) (finding no Privacy Act violation where agency disclosed same information in letter to journalist that plaintiff himself had previously provided to journalist; plaintiff “waiv[ed], in effect, his protection under the Privacy Act”); Quinn v. Stone, 978 F.2d 126, 134 (3d Cir. 1992) (dictum); Kline v. HHS, 927 F.2d 522, 524 (10th Cir. 1991); Hollis v. Army, 856 F.2d 1541, 1545 (D.C. Cir. 1988); Reyes v. DEA, 834 F.2d 1093, 1096 n.1 (1st Cir. 1987); Schowengerdt v. Gen. Dynamics Corp., 823 F.2d 1328, 1341 (9th Cir. 1987); Pellerin v. VA, 790 F.2d 1553, 1556 (11th Cir. 1986); FDIC v. Dye, 642 F.2d 833, 836 (5th Cir. 1981); Ash v. United States, 608 F.2d 178, 179 (5th Cir. 1979); Mudd v. Army, No. 2:05-cv-137, 2007 WL 4358262, at *5 (M.D. Fla. Dec. 10, 2007) (finding no “disclosure” because by time agency posted statement on its web site, plaintiff had been quoted in newspaper saying he received letter of admonishment, another newspaper article had referred to letter, and plaintiff had testified before Congress regarding letter; also finding no “disclosure” of report because at time agency provided link to report on its web site, “the entire [report] had been the subject of a press release and news conference by a separate and independent agency . . . and had been released to the media by the same”); Schmidt v. VA, 218 F.R.D. 619, 630 (E.D. Wis. 2003) (“defin[ing] the term ‘disclose’ to mean the placing into the view of another information which was previously unknown”); Barry v. DOJ, 63 F. Supp. 2d 25, 26-28 (D.D.C. 1999); Sullivan v. USPS, 944 F. Supp. 191, 196 (W.D.N.Y. 1996); Loma Linda Cmty. Hosp. v. Shalala, 907 F. Supp. 1399, 1404-05 (C.D. Cal. 1995) (commenting that policy underlying Privacy Act protecting confidential information from disclosure not implicated by release of information health care provider had already received through patients’ California “Medi-Cal” cards); Viotti v. Air Force, 902 F. Supp. 1331, 1337 (D. Colo. 1995), aff’d, 153 F.3d 730 (10th Cir. 1998) (unpublished table decision); Abernethy v. IRS, 909 F. Supp. 1562, 1571 (N.D. Ga. 1995), aff’d per curiam, No. 95-9489 (11th Cir. Feb. 13, 1997); Kassel v. VA, 709 F. Supp. 1194, 1201 (D.N.H. 1989); Krowitz v. USDA, 641 F. Supp. 1536, 1545 (W.D. Mich. 1986), aff’d, 826 F.2d 1063 (6th Cir. 1987) (unpublished table decision); Owens v. MSPB, No. 3-83-0449-R, slip op. at 2-3 (N.D. Tex. Sept. 14, 1983) (mailing of agency decision affirming employee’s removal to his former attorney held not “disclosure” because “attorney was familiar with facts of [employee’s] claim” and “no new information was disclosed to him”); Golliher v. USPS, 3 Gov’t Disclosure Serv. ¶ 83,114, at 83,702 (N.D. Ohio June 10, 1982); King v. Califano, 471 F. Supp. 180, 181 (D.D.C. 1979); Harper v. United States, 423 F. Supp. 192, 197 (D.S.C. 1976); cf. Pippinger v.

Rubin, 129 F.3d 519, 532-33 (10th Cir. 1997) (finding no evidence that disclosure “could possibly have had ‘an adverse effect’” on plaintiff where recipient “had been privy to every event described in [plaintiff’s] records at the time the event occurred”); Leighton v. CIA, 412 F. Supp. 2d 30, 39 (D.D.C. 2006) (citing Hollis and expressing doubt as to whether disclosure at issue “has presented any new information to those in the intelligence community”); Jones v. Runyon, 32 F. Supp. 2d 873, 876 (N.D. W. Va. 1998) (although finding disclosure to credit reporting service valid under routine use exception, concluding information disclosed was already in possession of recipient and other courts had held that Privacy Act is not violated in such cases), aff’d, 173 F.3d 850 (4th Cir. 1999) (unpublished table decision).

However, the Court of Appeals for the District of Columbia Circuit clarified that some disseminations of protected records to individuals with prior knowledge of their existence or contents are “disclosures” under the Privacy Act. Pilon v. DOJ, 73 F.3d 1111, 1117-24 (D.C. Cir. 1996). In Pilon, the D.C. Circuit held that the Justice Department’s transmission of a Privacy Act-protected record to a former employee of the agency constituted a “disclosure” under the Privacy Act, even though the recipient had come “into contact with the [record] in the course of his duties” while an employee. Id. The court’s “review of the Privacy Act’s purposes, legislative history, and integrated structure convince[d it] that Congress intended the term ‘disclose’ to apply in virtually all instances to an agency’s unauthorized transmission of a protected record, regardless of the recipient’s prior familiarity with it.” Id. at 1124.

In an earlier case, Hollis v. Army, 856 F.2d 1541 (D.C. Cir. 1988), the D.C. Circuit had held that the release of a summary of individual child-support payments previously deducted from plaintiff’s salary and sent directly to his ex-wife, who had requested it for use in pending litigation, was not an unlawful disclosure under the Privacy Act as she already knew what had been remitted to her. Id. at 1545. In Pilon, the D.C. Circuit reconciled its opinion in Hollis by “declin[ing] to extend Hollis beyond the limited factual circumstances that gave rise to it,” 73 F.3d at 1112, 1124, and holding that:

[A]n agency’s unauthorized release of a protected record does constitute a disclosure under the Privacy Act except in those rare instances, like Hollis, where the record merely reflects information that the agency has previously, and lawfully, disseminated outside the agency to the recipient, who is fully able to reconstruct its material contents.

Id. at 1124; cf. Osborne v. USPS, No. 94-30353, slip op. at 2-4, 6-11 (N.D. Fla. May

18, 1995) (assuming without discussion that disclosure of plaintiff's injury-compensation file to retired employee who had prepared file constituted "disclosure" for purposes of Privacy Act).

Courts are split over whether a disclosure occurs if the information disclosed is publicly available or was previously published.

Courts have also split over whether the disclosure of information that is readily accessible to the public constitutes a "disclosure" under the Privacy Act. The Court of Appeals for the Fifth Circuit, along with several district courts, has concluded that there is no "disclosure" in the release of previously published or publicly available information under the Privacy Act, regardless of whether the particular persons who received the information were aware of the previous publication. FDIC v. Dye, 642 F.2d at 836; Banks v. Butler, No. 5:08cv336, 2010 WL 4537902, at *6 (S.D. Miss. Sept. 23, 2010); Drennon-Gala v. Holder, No. 1:08-CV0321G, 2011 WL 1225784, at *8 (N.D. Ga. Mar. 30, 2011); Mudd v. Army, 2007 WL 4358262, at *5 (finding no "disclosure" where, inter alia, agency had posted statement on its web site, newspapers had referred to letter, plaintiff had testified before Congress regarding letter, and the entire report had been released to the press and in a news conference by another agency); Smith v. Cont'l Assurance Co., No. 91-C-0963, 1991 WL 164348, at *5 (N.D. Ill. Aug. 22, 1991); King, 471 F. Supp. at 181; cf. Sierra Pac. Indus. v. USDA, No. 11-1250, 2012 WL 245973, at *4 (E.D. Cal. Jan. 25, 2012) (finding that Privacy Act did not require sealing documents where "substance of the information . . . [was] already in the public record in one form or another").

The Third, Ninth, Tenth, and D.C. Circuits, however, have held that the release of information that is "merely readily accessible to the public" does constitute a disclosure under subsection (b). See, e.g., Quinn v. Stone, 978 F.2d 126, 134 (3d Cir. 1992) (holding that "[t]o define disclosure so narrowly as to exclude information that is readily accessible to the public would render superfluous the detailed statutory scheme of twelve exceptions to the prohibition on disclosure"); see also Gowan v. Air Force, 148 F.3d 1182, 1193 (10th Cir. 1998) ("adopt[ing] the Third Circuit's reasoning [in Quinn] and hold[ing] that an agency may not defend a release of Privacy Act information simply by stating that the information is a matter of public record"); Scarborough v. Harvey, 493 F. Supp. 2d 1, 15-16 n.29 (D.D.C. 2007) (agreeing with Quinn and concluding that "the unqualified language of the Privacy Act," which protects individual's "criminal . . . history," does not exclude information that is readily accessible to public); cf. Wright v. FBI, 241 F. App'x 367, 369 (9th Cir. 2007) (noting that "issue of whether a Privacy Act claim can be based on a defendant's disclosure of information previously disclosed to the public is a matter of first impression," and directing

district court to stay proceedings until plaintiff “obtains from the district court . . . an order defining the scope of his claims and, potentially, stating that court’s position on whether the Privacy Act applies to information previously disclosed to the public”); Pilon v. DOJ, 796 F. Supp. 7, 11-12 (D.D.C. 1992) (rejecting argument that information was already public and therefore could not violate Privacy Act where agency had republished statement that was previously publicly disavowed as false by agency).

The D.C. Circuit’s opinions in Hollis and Pilon, both discussed above, provide some insight into its view of whether the release of information that is already available to the public constitutes a “disclosure” under the Privacy Act. In Hollis, issued in 1988, the D.C. Circuit had recognized in dictum that other courts had held that the release of previously published material did not constitute a disclosure, and suggested that it might take that approach. Hollis, 856 F.2d at 1545. The court had held that a disclosure did not violate the Privacy Act because the recipient of the information already was aware of it, but that “[o]ther courts have echoed the sentiment that when a release consists merely of information to which the general public already has access, or which the recipient of the release already knows, the Privacy Act is not violated.” However, the D.C. Circuit’s subsequent holding in 1996 in Pilon appears to foreclose such a possibility. In Pilon, the D.C. Circuit held that even under the narrow Hollis interpretation of “disclose,” the agency would not be entitled to summary judgment because it had “failed to adduce sufficient evidence that [the recipient of the record] remembered and could reconstruct the document’s material contents in detail at the time he received it.” 73 F.3d at 1124-26. Nevertheless, the D.C. Circuit in Pilon noted that “[t]his case does not present the question of whether an agency may . . . release a document that has already been fully aired in the public domain through the press or some other means” but that “the Privacy Act approves those disclosures that are ‘required’ under the [FOIA] . . . and that under various FOIA exemptions, prior publication is a factor to be considered in determining whether a document properly is to be released.” Id. at 1123 n.10; see also Barry v. DOJ, 63 F. Supp. 2d 25, 27-28 (D.D.C. 1999) (distinguishing Pilon and finding no disclosure where agency posted Inspector General report on Internet website, after report had already been fully released to media by Congress and had been discussed in public congressional hearing, even though some Internet users might encounter report for first time on website). Furthermore, though, and consistent with the D.C. Circuit’s note in Pilon, one might argue that to say that no “disclosure” occurs for previously published or public information is at least somewhat inconsistent with the Supreme Court’s decision in DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762-71 (1989), which held that a privacy interest can exist, under the FOIA, in publicly available – but “practically obscure” – information, such as a

criminal history record. Cf. Finley v. NEA, 795 F. Supp. 1457, 1468 (C.D. Cal. 1992) (alleged disclosure of publicly available information states claim for relief under Privacy Act; recognizing Reporters Comm.).

The United States Court of Appeals for the Fourth Circuit has issued contradictory unpublished decisions on the issue of whether release of publicly available information constitutes a disclosure. Compare Lee v. Dearment, 966 F.2d 1442 (4th Cir. 1992) (unpublished table case) (upholding district court's determination that "the Act does not prohibit disclosure of information which is already open to the public, or if the receiver already knew of it" (citing Hollis v. Army, 856 F.2d at 1545)), and Dye, 642 F.2d at 836, with Doe v. Herman, No. 297CV00043, 1999 WL 1000212, at *11 (W.D. Va. Oct. 29, 1999) (magistrate's recommendation) (agreeing with Quinn v. Stone, 798 F.2d at 134, in dictum and concluding that discussion of social security numbers at public hearing did not free agency to disclose those numbers), adopted in pertinent part & rev'd in other part (W.D. Va. July 24, 2000), aff'd in part, rev'd in part & remanded, on other grounds sub nom. Doe v. Chao, 306 F.3d 170 (4th Cir. 2002) (finding that plaintiff had not established "actual damages" from disclosure), aff'd, 540 U.S. 614 (2004).

The Ninth Circuit has applied the "single publication rule," in which the court limits aggregate, unauthorized disclosures to only one cause of action, where an agency disclosed records on an agency web page.

On a related point, the Ninth Circuit held in a subsection (b) case that the "single publication rule" applies to postings on an agency's web site such that "the aggregate communication can give rise to only one cause of action." See Oja v. Army Corps of Eng'rs, 440 F.3d 1122, 1130-33 (9th Cir. 2006) (affirming summary judgment for Army Corps which had posted employees' personal information on its public website). However, the court also ruled that with regard to "the same private information at a different URL address [within the same Web site] . . . that disclosure constitutes a separate and distinct publication – one not foreclosed by the single publication rule – and [the agency] might be liable for a separate violation of the Privacy Act." Id. at 1133-34.

A public filing of records with a court during the course of litigation constitutes a disclosure.

The fact that "a court is not defined as an 'agency' or as a 'person' for purposes of [the Privacy Act]," (see Definitions, infra), indicates the Act was "not designed to interfere with access to information by the courts." 120 Cong. Rec. 36,967 (1974), reprinted in Source Book at 958-59, <https://www.justice.gov/opcl/>

[paoverview_sourcebook](#). Even so, the public filing of records with a court, during the course of litigation, does constitute a subsection (b) disclosure. See Laningham v. Navy, No. 83-3238, slip op. at 2-3 (D.D.C. Sept. 25, 1984), summary judgment granted (D.D.C. Jan. 7, 1985), aff'd per curiam, 813 F.2d 1236 (D.C. Cir. 1987); Citizens Bureau of Investigation v. FBI, No. 78-60, slip op. at 2-3 (N.D. Ohio Dec. 14, 1979). Accordingly, any such public filing must be undertaken with written consent or in accordance with either the subsection (b)(3) routine use exception or the subsection (b)(11) court order exception, both discussed below. See generally Krohn v. DOJ, No. 78-1536, slip op. at 3-11 (D.D.C. Mar. 19, 1984) (finding violation of Privacy Act where agency's disclosure of records as attachments to affidavit in FOIA lawsuit "did not fall within any of the exceptions listed in Section 552a"), reconsideration granted & vacated in nonpertinent part (D.D.C. Nov. 29, 1984) (discussed below).

The Privacy Act disclosure provision does not require heightened discovery requirements.

Often during the course of litigation, an agency will be asked to produce Privacy Act-protected information pursuant to a discovery request by an opposing party. The Privacy Act "does not create a qualified discovery privilege" or "any other kind of privilege or bar that requires a party to show actual need as a prerequisite to invoking discovery," and courts generally consider whether to allow discovery under "the usual discovery standards" of the Federal Rules of Civil Procedure." Laxalt v. McClatchy, 809 F.2d 885, 888 (D.C. Cir. 1987); see also Weahkee v. Norton, 621 F.2d 1080, 1082 (10th Cir. 1980); Garraway v. Ciuffo, No. 117CV00533DADGSAPC, 2020 WL 1263562, at *8 (E.D. Cal. Mar. 16, 2020); Pennsylvania v. Navient Corp., 348 F. Supp. 3d 394, 398 (M.D. Pa. 2018); Ala. & Gulf Coast Ry. v. United States, No. CA 10-0352, 2011 WL 1838882, at *3 (S.D. Ala. May 13, 2011); Golez v. Potter, No. 09-cv-965, 2011 WL 6002612, at *1-2 (S.D. Cal. Nov. 29, 2011) ("The exceptions allowed in the Privacy Act of 1974 are not applicable here. . . . Accordingly, the Privacy Act . . . precludes the [agency] from complying with Plaintiff's discovery request."); Forrest v. United States, No. 95-3889, 1996 WL 171539, at *2 (E.D. Pa. Apr. 11, 1996); Ford Motor Co. v. United States, 825 F. Supp. 1081, 1083 (Ct. Int'l Trade 1993); Clavir v. United States, 84 F.R.D. 612, 614 (S.D.N.Y. 1979); cf. Baldrige v. Shapiro, 455 U.S. 345, 360-62 (1982) (finding that Census Act confidentiality provisions create a privilege against disclosure of raw census data in discovery because they "embody explicit congressional intent to preclude all disclosure").

Agencies may affirmatively disclose Privacy Act-protected records during litigation, so long as the disclosure is made in accordance with the Privacy Act's disclosure provision

Although courts have unanimously held that the Privacy Act does not create a privilege against discovery, an agency can disclose Privacy Act-protected records if permitted by the Act. The most appropriate method of disclosure in this situation may be pursuant to a subsection (b)(11) court order. See generally Doe v. DiGenova, 779 F.2d 74 (D.C. Cir. 1985); Doe v. Stephens, 851 F.2d 1457 (D.C. Cir. 1988) (both discussed below under subsection (b)(11)). Indeed, the courts that have rejected the Privacy Act as a discovery privilege have referenced subsection (b)(11)'s allowance for court-ordered disclosures. See Laxalt, 809 F.2d at 888-89; Weahkee, 621 F.2d at 1082; Garraway v. Ciufo, No. 117CV00533DADGSAPC, 2020 WL 1263562, at *8 (E.D. Cal. Mar. 16, 2020) (records that might otherwise be protected by the Act may still be discovered through litigation if ordered by a court); Lightsey v. Potter, No. 1:04-CV-3110-ODE, 2006 WL 8431955 (N.D. Ga. July 27, 2006); Hernandez v. United States, No. 97-3367, 1998 WL 230200, at *2-3 (E.D. La. May 6, 1998); Forrest, 1996 WL 171539, at *2; Ford Motor Co., 825 F. Supp. at 1082-83; Clavir, 84 F.R.D. at 614; cf. Alford v. Todco, No. CIV-88-731E, slip op. at 4-5 (W.D.N.Y. June 12, 1990) (ordering production of records and concluding that "[e]ven assuming the Privacy Act supplies a statutory privilege . . . the plaintiff has waived any such privilege by placing his physical condition at issue"); Tootle v. Seaboard Coast Line R.R., 468 So. 2d 237, 239 (Fla. Dist. Ct. App. 1984) (recognizing that privacy interests in that case "must give way to the function of the discovery of facts" and that subsection (b)(11) provides the mechanism for disclosure).

When an agency wishes to make an affirmative disclosure of information during litigation it may either rely on a routine use permitting such disclosure or seek a court order. Because the Privacy Act does not constitute a statutory privilege, agencies need not worry about breaching or waiving such a privilege when disclosing information pursuant to subsections (b)(3) or (b)(11). Cf. Mangino v. Army, No. 94-2067, 1994 WL 477260, at *5-6 (D. Kan. Aug. 24, 1994) (finding that disclosure to court was appropriate pursuant to agency routine use and stating that to extent Privacy Act created privilege, such privilege was waived by plaintiff when he placed his records at issue through litigation); Lemasters v. Thomson, No. 92 C 6158, 1993 U.S. Dist. LEXIS 7513, at *3-8 (N.D. Ill. June 3, 1993) (same finding as in Mangino, despite fact that "court ha[d] not located" applicable routine use). See also Vaughan v. Ky. Army Nat'l, No. 3:12-33, 2013 WL 1856418, at *4 (E.D. Ky. May 1, 2013) (finding that routine use disclosure to Department of Justice was appropriate for purposes of defending agency against claims pertaining to plaintiff's records at issue in litigation). For further discussions of disclosures during litigation, see "Conditions of Disclosure to

Third Parties,” subsections “5 U.S.C. § 552a(b)(3) - Routine Uses” and “5 U.S.C. § 552a(b)(11) - Court Order,” below.

Agencies are not prohibited from disclosing to an individual his own record in response to a “first party” access request pursuant to the Privacy Act’s access provisions.

By its own terms, subsection (b) does not prohibit an agency from releasing to an individual his own record, contained in a system of records retrieved by his name or personal identifier, in response to his “first-party” access request under subsection (d)(1). Cf. Weatherspoon v. Provincetowne Master Owners Ass’n, No. 08-cv-02754, 2010 WL 936109, at *3 (D. Colo. Mar. 15, 2010) (finding that even though records were maintained by Veterans Administration (“VA”), where plaintiff had been ordered in discovery to produce her mental health records in her emotional distress suit, there would be no improper disclosure to an ‘unauthorized party’ because “the VA will disclose Plaintiff’s mental health records to her, so that she can transmit copies of them to defense counsel”). However, as is discussed below under “Individual’s Right of Access,” the courts have split as to whether a disclosure occurs when the record is disclosed to the individual who is the subject of the record where the record is also about another individual and is “dually retrieved.”

Subsection (b) also explicitly authorizes disclosures made with the prior written consent of the individual. See, e.g., Taylor v. Potter, No. 02-1552, 2004 WL 422664, at *1-2 (D. Del. Mar. 4, 2004) (finding it to be “clear from the documents attached to Plaintiff’s complaint that she provided prior written consent . . . for her medical records to be disclosed”); Scherer v. Hill, No. 02-2043, 2002 U.S. Dist. LEXIS 17872, at *6-8 (D. Kan. Sept. 17, 2002) (finding plaintiff’s argument that agency violated his privacy by sending photographs of his skin condition to United States Attorney rather than directly to him to be “frivolous,” as “[h]e specifically asked the ‘US Attorney and the Veterans Administration’ to produce the photographs” in his motion to compel, and “Privacy Act does not prohibit the consensual disclosure of photographs or documents by an agency”); cf. Stokes v. SSA, 292 F. Supp. 2d 178, 181 (D. Me. 2003); (finding that statement directed at subject of record “did not become the kind of ‘disclosure’ for which the Privacy Act requires written consent merely because [a third party] overheard it,” especially given that individual consented to interview in third party’s presence and thereby, in accordance with the agency regulation, “affirmatively authorized [third party’s] presence during this discussion”; “The Privacy Act does not prevent an agency employee from discussing the contents of a protected record with the person to whom the record pertains.”).

Agencies cannot be held liable for disclosures that individuals make themselves.

Additionally, although it may seem self-evident, the fact pattern in one case caused a court to explicitly hold that an agency cannot be sued for disclosures that an individual makes himself. Abernethy v. IRS, 909 F. Supp. 1562, 1571 (N.D. Ga. 1995) (describing that plaintiff had informed employees that he was being removed from his position as their supervisor and disclosed reason for his removal).

While “written consent” under the Privacy Act is not defined, courts have held that “implied consent” is not sufficient.

The Act does not define the “written consent” needed to permit disclosure under the Privacy Act. Implied consent, however, is insufficient. See Taylor v. Orr, No. 83-0389, 1983 U.S. Dist. LEXIS 20334, at *6 n.6 (D.D.C. Dec. 5, 1983) (addressing alternative argument, stating that: “Implied consent is never enough” as the Act’s protections “would be seriously eroded if plaintiff’s written submission of [someone’s] name were construed as a voluntary written consent to the disclosure of her [medical] records to him”); cf. Milton v. DOJ, 783 F. Supp. 2d 55, 59 (D.D.C. 2011) (rejecting, in context of Freedom of Information Act claim, plaintiff’s argument that his privacy waiver to permit BOP to monitor his telephone calls impliedly extended to any party who accepted his calls; “[A] protected privacy interest can be waived only by the person whose interest is affected, . . . and [plaintiff] has not produced Privacy Act waivers from the individuals with whom he spoke on the telephone.”); Baitey v. VA, No. 8:CV89-706, slip op. at 5 (D. Neb. June 21, 1995) (concluding that “at a minimum, the phrase ‘written consent’ necessarily requires either (1) a medical authorization signed by [plaintiff] or (2) conduct which, coupled with the unsigned authorization, supplied the necessary written consent for the disclosure”). But cf. Pellerin v. VA, 790 F.2d 1553, 1556 (11th Cir. 1986) (applying doctrine of “equitable estoppel” to bar individual from complaining of disclosure of his record to congressmen “when he requested their assistance in gathering such information”) (distinguished in Swenson v. USPS, 890 F.2d 1075, 1077-78 (9th Cir. 1989)); Del Fuoco v. O’Neill, No. 8:09-CV-1262, 2011 WL 601645, at *10 (M.D. Fla. Feb. 11, 2011) (Where regulation mandated that DOJ furnish plaintiff’s termination letter to MSPB, noting that it was plaintiff’s appeal to MSPB that triggered the disclosure, “which did not require Plaintiff’s consent, which is implied by virtue of his appeal.”); Jones v. Army Air Force Exchange Serv. (AAFES), No. 3:00-CV-0535, 2002 WL 32359949, at *5 (N.D. Tex. Oct. 17, 2002) (referring to plaintiff’s claim that AAFES disclosed protected information to congressional offices in violation of Privacy Act, and finding plaintiff to be “estopped from asserting such a claim because AAFES released the information

pursuant to congressional office inquiries that were initiated at Plaintiff's request").

OMB guidelines suggest, and courts have generally approved of, written consent that states the general purposes for, or types of recipients to, which disclosures may be made; the scope of an agency's permitted disclosures is then defined by the terms on which the individual provided written consent.

The OMB 1975 Guidelines caution that "the consent provision was not intended to permit a blanket or open-ended consent clause, i.e., one which would permit the agency to disclose a record without limit," and that, "[a]t a minimum, the consent clause should state the general purposes for, or types of recipients [to,] which disclosure may be made." 40 Fed. Reg. at 28,954, https://www.justice.gov/paoverview_omb-75. See also Perry v. FBI, 759 F.2d 1271, 1276 (7th Cir. 1985) (upholding disclosure because release was "not so vague or general that it is questionable whether [plaintiff] knew what he was authorizing or whether the [agency] knew what documents it could lawfully release"), rev'd en banc on other grounds, 781 F.2d 1294 (7th Cir. 1986).

Courts generally have approved disclosures made with consent where the consent was broad enough to cover the disclosure. See Elnashar v. DOJ, 446 F.3d 792, 795 (8th Cir. 2006) (observing that plaintiff's signed release "authoriz[ing] representatives of [human rights organization] to obtain and examine copies of all documents and records contained by the [FBI] . . . pertaining to [plaintiff]" constituted consent for FBI to disclose "that it had records which were responsive to the request for records and that records were contained in the 'PENTBOMB' investigation"); United States v. Rogers, No. 10-00088, 2010 WL 5441935, at *1 (S.D. Ala. Dec. 28, 2010) (concluding that "if defendant is willing to make a written request to the BOP for his own records and give written consent for their release to his defense counsel, the Court sees no reason why a[] [court] order is necessary"); Roberts v. DOT, No. 02-CV-4414, 2006 WL 842401, at *8, *2 (E.D.N.Y. Mar. 28, 2006) (maintaining that plaintiff's signed SF 171, which "explicitly stated that [plaintiff] 'consent[ed] to the release of information about [his] ability and fitness for Federal employment,'" authorized disclosure of plaintiff's medical records by agency who previously employed him to employing agency to assist in "assist determining whether the employee is capable of performing the duties of the new position"); Thomas v. VA, 467 F. Supp. 458, 460 n.4 (D. Conn. 1979) (holding consent was adequate because it was both agency- and record-specific); cf. Tarullo v. Def. Contract Audit Agency, 600 F. Supp. 2d 352, 360-61 (D. Conn. 2009) (concluding that "the forms themselves put the Plaintiff on notice that they (and hence their contents) would be disclosed Yet, the Plaintiff supplied his SSN. As a result, he voluntarily

disclosed his SSN.”); Wiley v. VA, 176 F. Supp. 2d 747, 751-56 (E.D. Mich. 2001) (concluding that plaintiff’s written release for employment application that broadly authorized employer to corroborate and obtain information about plaintiff’s background constituted valid consent under Privacy Act to authorize disclosure of all 466 pages of plaintiff’s VA claims file in connection with union grievance proceeding, even though release was signed eight years prior to disclosure”).

On the other hand, courts have found consent clauses with narrower terms than the eventual disclosure to be inadequate to authorize that disclosure. See Schmidt v. Air Force, No. 06-3069, 2007 WL 2812148, at *8 (C.D. Ill. Sept. 30, 2007) (issuance of press release and posting of complete text of plaintiff’s reprimand on agency website was outside scope of plaintiff’s signed waiver, which was limited to “a press release announcing the conclusion of the case”); Fattahi v. ATE, 186 F. Supp. 2d 656, 660 (E.D. Va. 2002) (consent providing that information on application “may be disclosed to members of the public in order to verify the information on the application when such disclosure is not prohibited by law” was “a mere tautology: plaintiff consented to no more than that ATF may disclose information except in cases where that disclosure is prohibited”); Doe v. Herman, No. 297CV00043, 1999 WL 1000212, at *9 (W.D. Va. Oct. 29, 1999) (magistrate’s recommendation) (rejecting argument that when plaintiffs provided their social security numbers for purpose of determining eligibility for and amount of benefits payable, they consented to use of those numbers as identifiers on multi-captioned hearing notices sent to numerous other individuals and companies as well as to publication of numbers in compilations of opinions), adopted in pertinent part & rev’d in other part, (W.D. Va. July 24, 2000), aff’d in part, rev’d in part & remanded, on other grounds sub nom. Doe v. Chao, 306 F.3d 170 (4th Cir. 2002), aff’d, 540 U.S. 614 (2004); AFGE v. U.S. R.R. Ret. Bd., 742 F. Supp. 450, 457 (N.D. Ill. 1990) (SF-86 “release form” held overbroad and contrary to subsection (b)); and Doe v. GSA, 544 F. Supp. 530, 539-41 (D. Md. 1982) (stating that authorization, which was neither record- nor entity-specific, was insufficient under GSA’s own internal interpretation of Privacy Act); cf. Taylor, No. 83-0389, 1983 U.S. Dist. LEXIS 20334, at *6 n.6 (D.D.C. Dec. 5, 1983) (addressing alternative argument, stating: “It is not unreasonable to require that a written consent to disclosure address the issue of such disclosure and refer specifically to the records permitted to be disclosed.”).

One California district court has held that courts cannot create new disclosure exceptions based on state policy.

One district court has declined to “recognize a new exception to [subsection (b) of the Privacy Act] based on California public policy to protect persons

investigating acts of child abuse.” Stafford v. SSA, 437 F. Supp. 2d 1113, 1121 (N.D. Cal. 2006). In Stafford, a Social Security Administration (“SSA”) employee disclosed to California Child Protective Services “the precise diagnosis of mental illness on which the SSA had made its determination that [the suspected child abuser] was disabled and thus eligible for benefits.” Id. at 1116. The suspect brought a subsection (b)/(g)(1)(D) claim against the agency, and the agency argued that the court should recognize a new exception because “[t]he public interest in detecting and eradicating child abuse is so strong that under California state law, malicious acts or acts taken without probable cause by investigators such as [the Child Protective Services employee] are immunized.” Id. at 1121. The court explained that “Congress enacted the Privacy Act as a limitation on the sharing of private information among government agencies to further what it determined was an important public policy” and stated that “[t]he Court cannot create an exception to a federal statute based on state policy.” Id.

B. Twelve Exceptions to the “No Disclosure without Consent” Rule

As discussed in detail above, the general rule under the Privacy Act is that, without an individual’s written consent, records about that individual maintained in a system of records cannot be disclosed. There are, however, a number of exceptions to that general rule, or conditions under which information can be disclosed without consent. Of the twelve exceptions discussed in this section, the most significant and frequently litigated exceptions are the “need to know” exception, disclosures required under FOIA, and the “routine use” exception. The twelve exceptions are discussed here in turn.

Other than disclosures under subsection (b)(2) of the Privacy Act (see “Conditions of Disclosure to Third Parties, 5 U.S.C. § 552a(b)(2) - Required FOIA Disclosure” discussion, below), disclosures under the following exceptions are permissive, not mandatory. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,953, https://www.justice.gov/paoverview_omb-75.

1. 5 U.S.C. § 552a(b)(1) - Need to Know within Agency

“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 unless the disclosure would be –

(1) to those officers and employees of the agency which maintains the record

who have a need for the record in the performance of their duties.” 5 U.S.C. § 552a(b)(1).

Comment:

The “need to know” disclosure exception authorizes intra-agency disclosures.

The “need to know” exception authorizes the intra-agency disclosure of a record for necessary, official purposes. See OMB 1975 Guidelines, 40 Fed. Reg. 28,948, 28,950-01, 28,954 (July 9, 1975), https://www.justice.gov/pa/overview_omb-75. The Privacy Act’s legislative history indicates an intent “to give the term ‘agency’ its broadest statutory meaning,” and to permit “need to know” disclosures between components of large agencies. See 120 Cong. Rec. 36,967 (1974), reprinted in Source Book at 958, https://www.justice.gov/opcl/paoverview_sourcebook (recognizing propriety of “need to know” disclosures between DOJ components); see also Dick v. Holder, 67 F. Supp. 3d 167, 177-178 (D.D.C. 2014) (stating that “552a(b)(1) does not authorize disclosure outside the ‘agency,’ which this Court has defined broadly to include sharing between component agencies underneath the umbrella of the [Department], not just the specific agency that originally held the information, such as the FBI in this instance”); Sussman v. Marshals Serv., 808 F. Supp. 2d 192, 196-204 (D.D.C. 2011) (recognizing that “[a]lthough the [Marshals Service] and FBI may themselves be considered agencies, they are also components of DOJ, which is itself an agency,” under the statutory meaning of the term, and that disclosures between them “qualify as intra-agency disclosures”); Lora v. DOJ, No. 00-3072, slip op. at 14-15 (D.D.C. Apr. 9, 2004) (finding plaintiff’s argument that Privacy Act violation occurred when INS, then component of DOJ, released documents to DOJ prosecutor to be without merit); Walker v. Ashcroft, No. 99-2385, slip op. at 18-20 & n.6 (D.D.C. Apr. 30, 2001) (alternative holding) (finding that disclosures from FBI field office to FBI headquarters, and from FBI to DOJ prosecutors, were “proper under the ‘need to know’ exception”; “FBI employees and federal prosecutors are considered employees of the same agency, namely the Department of Justice.”), summary affirmance granted, No. 01-5222, 2002 WL 335530 (D.C. Cir. Jan. 25, 2002); cf. Lennon v. Rubin, 166 F.3d 6, 10 (1st Cir. 1999) (finding that district court correctly granted summary judgment to agency where plaintiff alleged discrimination because, despite memorandum indicating intent to distribute information to task force that included individuals from outside agency, agency employee testified that she only gave information to member who was agency employee, and recipient employee declared that she had never given information to other task force members); Freeman v. EPA, No. 02-0387,

2004 WL 2451409, at *4-5 (D.D.C. Oct. 25, 2004) (finding that disclosure of plaintiffs' drug testing schedules and results by EPA OIG to an EPA-hired DOD investigator did not violate Privacy Act because "according to the OMB 1975 Guidelines, an agency that hires a member of another agency to serve in a temporary task force or similar, cross-designated function can share otherwise protected information with that hired person and still satisfy exception (b)(1)"); OMB 1975 Guidelines, 40 Fed. Reg. at 28,954, https://www.justice.gov/paoverview_omb-75 ("Movement of records between personnel of different agencies may in some instances be viewed as intra-agency disclosures if that movement is in connection with an inter-agency support agreement").

Courts generally focus on whether the agency employee receiving the information had a need for the record in the performance of the employee's duties.

It is the employee receiving the information - not the employee making the disclosure - who must have the "need to know." So long as "the persons to whom disclosure is made are employees of the agency that maintains the records" and "those employees have a need for access," disclosure under this subsection "is not limited to the employees responsible for maintaining the records." *See, e.g., Coburn v. Potter*, 329 F. App'x 644, 646 (7th Cir. 2009); *Cacho v. Chertoff*, No. 06-00292, 2006 WL 3422548, *4-7 (D.D.C. Nov. 28, 2006) (finding plaintiff's argument alleging improper access of information irrelevant to (b)(1) analysis; "What matters then is the 'need to know' of the agency official who received the disclosure, not the authority of the agency official who made the disclosure."); *Gill v. DOD*, 92 M.S.P.R. 23, 31-32 (2002) (finding disclosure to EEO counselor of other employees' records appeared to fall within (b)(1) exception, where appellant provided records at request of EEO counselor who was investigating appellant's claim that she was disparately treated).

Some courts have found the "need to know" disclosure exception to apply to contractors who serve the function of agency employees.

Although subsection (b)(1) permits disclosure only to "those officers and employees of the agency which maintains the record," some courts have upheld disclosures to contractors who serve the function of agency employees. *See Mount v. USPS*, 79 F.3d at 532-34 (concluding disclosure of plaintiff's medical files to "a physician under contract with the USPS" who had "responsibilities for making employment and/or disciplinary decisions regarding plaintiff" had some basis in need to know exception); *Gard v. Dep't of Educ.*, 789 F. Supp. 2d 96, 110 (D.D.C. 2011) (finding permissible

intra-agency disclosure to “‘occupational medicine consultant’ under contract with” agency for purposes of evaluating employee’s risk to coworkers); Ciralsky v. CIA, 689 F. Supp. 2d 141, 155 (D.D.C. 2010) (finding permissible intra-agency disclosures to private contractors hired to investigate certain allegations, including plaintiff’s); Sutera v. TSA, 708 F. Supp. 2d 304, 318 (E.D.N.Y. 2010) (finding permissible intra-agency disclosure where medical sample was sent to outside laboratory because “[f]or testing purposes a private laboratory is necessarily treated as part of the agency”); Coakley v. DOT, No. 93-1420, 1994 WL 16953072, at *1-2 (D.D.C. Apr. 7, 1994) (holding that independent contractor serving as EEO investigator for employee’s EEO complaint “must be considered an employee of DOT for Privacy Act purposes” and that DOT’s disclosure to that contractor “in connection with an official agency investigation . . . must be considered an intra-agency communication under the Act”); Hulett v. Navy, No. TH 85-310-C, slip op. at 3-4 (S.D. Ind. Oct. 26, 1987) (discussing disclosure of medical and personnel records to contractor/psychiatrist for purpose of assisting him in performing “fitness for duty” examination), *aff’d*, 866 F.2d 432 (7th Cir. 1988) (unpublished table decision); *cf.* Gill v. DOD, 92 M.S.P.R. at 32 n.7 (noting that EEO counselor to whom disclosure was made “was employed by a contractor, rather than directly by the agency [and] . . . was performing an administrative function for which the agency was responsible,” and stating further that “[i]t is clear that, for particular purposes, the Privacy Act provides that any government contractor and any employee of such contractor shall be considered an employee of an agency” (citing 5 U.S.C. § 552a(m))). Another court, however, has held to the contrary on facts nearly identical to those in Hulett Taylor v. Orr, No. 83-0389, 1983 U.S. Dist. LEXIS 20334, at *7-10 (D.D.C. Dec. 5, 1983).

Courts generally have found intra-agency disclosures regarding personnel or employment matters as authorized disclosures under the “need to know” disclosure exception.

The cases are replete with examples of proper intra-agency “need to know” disclosures. By far the most frequent “need to know” disclosure that the courts have deemed appropriate is for the purpose of investigating alleged employee misconduct or making disciplinary determinations. *See, e.g.*, Pippinger v. Rubin, 129 F.3d 519, 529-31 (10th Cir. 1997) (discussing supervisor’s disclosure of identity of person being investigated to staff members assisting in investigation, and to agency attorney defending agency’s actions in related MSPB proceeding against another individual); Mount v. USPS, 79 F.3d 531, 533-34 (6th Cir. 1996) (discussing disclosure of

information in plaintiff's medical records to other employees "with responsibilities for making employment and/or disciplinary decisions regarding plaintiff"; "In light of the questions surrounding plaintiff's mental stability, each had at least an arguable need to access the information in plaintiff's medical records."); Covert v. Harrington, 876 F.2d 751, 753-54 (9th Cir. 1989) (discussing disclosure of security questionnaires to Inspector General for purpose of detecting fraud); Daly-Murphy v. Winston, 837 F.2d 348, 354-55 (9th Cir. 1988) (discussing disclosure of letter suspending doctor's clinical privileges to participants in peer-review proceeding); Lukos v. IRS, No. 86-1100, 1987 WL 36354, at *1-2 (6th Cir. Feb. 12, 1987) (discussing disclosure of employee's arrest record to supervisor for purpose of evaluating his conduct and to effect discipline); Howard v. Marsh, 785 F.2d 645, 647-49 (8th Cir. 1986) (discussing disclosure of employee's personnel records to agency attorney and personnel specialist for purpose of preparing response to discrimination complaint); Hernandez v. Alexander, 671 F.2d 402, 410 (10th Cir. 1982) (discussing disclosure of employee's EEO files to personnel advisors for purpose of determining whether personnel action should be taken against employee); Grogan v. IRS, 3 Gov't Disclosure Serv. (P-H) ¶ 82,385, at 82,977-78 (4th Cir. Mar. 22, 1982) (discussing disclosure of questionable income tax returns prepared by professional tax preparer while he was IRS employee to IRS examiners for purpose of alerting them to possible irregularities); Code v. Esper, 285 F. Supp. 3d 58, 70-71 (D.D.C. 2017) (concluding that Army investigative unit did not violate Privacy Act by disclosing investigative report finding plaintiff committed certain crimes to Defense Finance and Accounting Service for purposes of official debt collecting duties), rev'd and remanded on other grounds sub nom. Code v. McCarthy, 959 F.3d 406 (D.C. Cir. 2020); Lewis v. SSA, No. 9:14-CV-31, 2015 WL 9664967, at *6 (E.D. Tex. Dec. 7, 2015) (discussing disclosure of report containing allegations about plaintiff by SSA employee who had duty "to 'report threats and harassment against the agency'" to DHS), adopted by 2016 WL 81577 (E.D. Tex. Jan. 1, 2016); Drennon-Gala v. Holder, No. 1:08-CV-321G, 2011 WL 1225784, at *5 (N.D. Ga. Mar. 30, 2011) (discussing disclosure of plaintiff's workers compensation file to agency officials investigating allegations "directly related to misconduct involving [plaintiff's] worker's compensation claim"); Doe v. DOJ, 660 F. Supp. 2d 31, 45-46 (D.D.C. 2009) (discussing disclosure of plaintiff AUSA's mental state to DOJ security personnel, who "needed . . . to assess his trustworthiness and make related personnel decisions about his eligibility for security clearance," to acting U.S. Attorney and division chief, who "[a]s plaintiff's supervisors . . . were responsible for ensuring that the [office] was operating safely," and to EOUSA attorney, who was "entitled to access the records because he represented DOJ in various pending disciplinary matters against

plaintiff at the time” (internal quotation marks omitted)); Gamble v. Army, 567 F. Supp. 2d 150, 156 (D.D.C. 2008) (discussing disclosure to plaintiff’s commanding officer of past allegations of sexual misconduct by plaintiff in context of investigation of new allegations of same); Roberts v. DOJ, 366 F. Supp. 2d 13, 26-28 (D.D.C. 2005) (finding disclosure of results of investigation by OPR to FBI was “expressly permitted” because FBI referred matter to OPR for investigation and because FBI had duty to respond to plaintiff’s complaints; dismissing claim because “OPR was entitled to share information regarding the results of its investigation” with agency that was subject of its investigation); Buckles v. Indian Health Serv., 305 F. Supp. 2d 1108, 1111 (D.N.D. 2004) (finding disclosure of employees’ medical records by employer’s health facility to risk management team – due to concerns that employees were illegally receiving prescription drugs – was proper because it conformed with facility’s protocol to discuss issues of potential wrongdoing with upper management); Abernethy v. IRS, 909 F. Supp. 1562, 1570-71 (N.D. Ga. 1995) (“[Investigatory] panel’s review of Plaintiff’s performance appraisals was not a violation of the Privacy Act because the members had a need to know the contents of the appraisals.”); (finding that member of panel that recommended that plaintiff be removed from management in response to EEO informal class complaint “had a need to know the contents of the [EEO] complaint file”), aff’d per curiam, No. 95-9489, 108 F.3d 343 (11th Cir. Feb. 13, 1997) (unpublished table decision); Harry v. USPS, 867 F. Supp. 1199, 1206 (M.D. Pa. 1994) (discussing disclosure from one internal subdivision of Postal Service to another – the Inspection Service (Inspector General) – which was conducting investigation), aff’d sub nom. Harry v. USPS, 60 F.3d 815 (3d Cir. 1995) (unpublished table decision).

Similarly, where an employee has a “need to know” certain information for personnel or employment determinations, the courts have found disclosure appropriate. Tran v. Treasury, 351 F. Supp. 3d 130, 138-140 (D.D.C. 2019) (discussing disclosure of performance appraisal to managers who were considering plaintiff’s detail request), aff’d 798 F. App’x. 649, 649-650 (D.C. Cir. 2020) (“As to the need for the record, every employee who accessed Tran’s performance appraisal needed to know whether Tran had the requisite skillset for a detail, in order to perform properly his or her duty to evaluate Tran as a prospective detailee. Tran’s performance appraisal contained information relevant to that inquiry.”); Lamb v. Millennium Challenge Corp., 228 F. Supp. 3d 28, 37 (D.D.C. 2017) (noting no allegation that disclosure occurred “for any reason unrelated to the agency’s security check and suitability determination”); Sutera v. TSA, 708 F. Supp. 2d at 318 (concluding, despite plaintiff’s assertion that agency’s “statement that he

failed a drug test violated the Privacy Act,” that “[TSA Disciplinary Review Board] officials, the Medical Review Officer, and the deciding official are all agency employees responsible for making employment decisions regarding plaintiff” and “[t]heir communications are within the Privacy Act’s ‘need-to-know’ exception”); Thompson v. State, 400 F. Supp. 2d 1, 20 (D.D.C. 2005) (finding disclosure of investigative report to agency’s Office of Civil Rights to determine “whether plaintiff’s supervisor was promoting plaintiff’s career to the detriment of the office and other employees because of a romantic relationship” was “relevant to the agency’s compliance with EEO regulations”); Hanna v. Herman, 121 F. Supp. 2d 113, 123-24 (D.D.C. 2000) (finding disclosure of information about plaintiff’s demotion to supervisor in another office of agency was covered by “need to know” exception), summary affirmance granted sub nom. Hanna v. Chao, No. 00-5433 (D.C. Cir. Apr. 11, 2001); Magee v. USPS, 903 F. Supp. 1022, 1029 (W.D. La. 1995) (discussing disclosure of employee’s medical report following fitness-for-duty examination to Postmaster of Post Office where employee worked to determine whether employee could perform essential functions of job and to Postmaster’s supervisor who was to review Postmaster’s decision), aff’d per curiam, 79 F.3d 1145 (5th Cir. 1996).

Courts generally have found intra-agency disclosures of records for national security purposes to be authorized disclosures under the “need to know” disclosure exception.

The courts also have concluded that an agency employee has a “need to know” information that could affect national security. *See, e.g., Bigelow v. DOD*, 217 F.3d 875, 876-78 (D.C. Cir. 2000) (describing review of plaintiff’s personnel file by immediate supervisor in connection with supervisor’s “continuing duty to make sure that [plaintiff] was worthy of trust” because of “a need to examine the file in view of the doubts that had been raised in his mind about [plaintiff] and [plaintiff’s] access to the country’s top secrets”); Britt v. Naval Investigative Serv., 886 F.2d 544, 549 n.2 (3d Cir. 1989) (noting propriety of disclosure of investigative report to commanding officer “since the Reserves might need to reevaluate Britt’s access to sensitive information or the level of responsibility he was accorded”); Williams v. Reilly, 743 F. Supp. 168, 175 (S.D.N.Y. 1990) (discussing employee’s admission of drug use disclosed by Naval Investigative Service to plaintiff’s employer, Defense Logistics Agency, for purposes of revoking employee’s security clearance).

Courts generally have found intra-agency disclosures of records to perform administrative duties to be authorized disclosures under the “need to know” disclosure exception.

Disclosure has been deemed appropriate where an employee has a “need to know” information to perform an administrative duty. See Hudson v. Reno, 130 F.3d 1193, 1206-07 (6th Cir. 1997) (discussing disclosure of plaintiff’s performance evaluation to individual who typed it originally, for retyping), abrogated on other grounds by Pollard v. E.I. du Pont de Nemours & Co., 532 U.S. 843 (2001); Cornelius v. McHugh, No. 3:14-cv-00234, 2015 WL 4231877, at *4-6 (D.S.C. July 13, 2015) (discussing disclosure of background check information related to plaintiff’s job duties to agency employees who needed information for performance of their duties); Middlebrooks v. Mabus, No. 1:11cv46, 2011 WL 4478686, at *6-7 (E.D. Va. Sept. 23, 2011) (discussing disclosure to “small group of senior employees” who were “required ‘to perform their job of legal oversight for the agency’” and “determine proper compliance with disclosure regulations”); Shayesteh v. Raty, No. 02:05-CV-85TC, 2007 WL 2317435, at *4-5 (D. Utah Aug. 7, 2007) (finding that disclosure to law enforcement officer within agency fit within need to know exception because “record clearly shows that the purpose for the disclosures in this instance was to pursue forfeiture of funds . . . a task which is clearly within [employees’] duties as federal law enforcement officers”); Schmidt v. VA, 218 F.R.D. 619, 631 (E.D. Wis. 2003) (“VA personnel need to have access to the entire [social security number] of persons accessible through the [Computerized Patient Records System] to avoid misidentification.”).

Courts generally have found intra-agency disclosures of records to provide medical treatment or assess medical expenses as authorized disclosures under the “need to know” disclosure exception.

Courts also have allowed disclosure under the “need to know” exception where the information is needed to provide medical treatment or expenses for medical treatment. McKinley v. United States, No. 3:14-CV-01931, 2015 WL 4663206, at *8 (D. Or. Aug. 5, 2015) (“The information contained in McKinley’s treatment, counseling, and psychotherapy notes was collected in an effort to provide her medical treatment, and the records were disclosed to other VA health professionals for that same purpose.”); Marquez v. Johnson, No. 11-cv-545, 2012 WL 6618238, at *11 (D. Colo. Dec. 19, 2012) (finding that disclosure by plaintiff’s supervisor to staff that plaintiff was out on leave due to “cancer scare” was based on their need for information in performance of their duties), aff’d, 545 Fed. App’x 735, 740 (10th Cir. 2013)

("[Plaintiff] did not allege [that leave information] was revealed to the entire staff . . . Nor does [plaintiff] dispute [agency's] position that the disclosure was necessary to an investigator regarding [plaintiff's] claim for medical and therapy expenses."); Khalfani v. VA, No. 94-CV-5720, 1999 WL 138247, at *7-8 (E.D.N.Y. Mar. 10, 1999) (discussing disclosure of plaintiff's medical records within VA so that his supervisor could document his request for medical leave and determine level of work he could perform).

Courts generally have found that intra-agency disclosures to employees that do not have a need for the record in the performance of their duties are outside the scope of the "need to know" disclosure exception.

On the other hand, intra-agency disclosures to recipients who do not need the information to perform their duties are improper. *See, e.g., Parks v. IRS*, 618 F.2d 677, 680-81 & n.1 (10th Cir. 1980) (holding plaintiffs had viable claim for disclosure of names of employees who did not purchase savings bonds for solicitation purposes); Dick v. Holder, 67 F. Supp. 3d at 177-178 (finding "need to know" exception did not authorize "Be on the Lookout" alert to law enforcement officers outside DOJ or within agency "without any showing of why each employee needed to receive the information"); Carlson v. GSA, No. 04-C-7937, 2006 WL 3409150, at *3-4 (N.D. Ill. Nov. 21, 2006) (explaining that supervisor's e-mail to employees providing reasons for plaintiff's termination does not fall within need to know exception because supervisor "encouraged [employees] to share [the e-mail] without restriction" and "express[ed] his personal satisfaction with [employee's] termination"); MacDonald v. VA, No. 87-544-CIV-T-15A, slip op. at 8-9 (M.D. Fla. July 28, 1989) (holding disclosure of counseling memorandum in "callous attempt to discredit and injure" employee is improper); Koch v. United States, No. 78-273T, slip op. at 1-2 (W.D. Wash. Dec. 30, 1982) (holding letter of termination posted in agency's entrance hallway is improper); Smigelsky v. USPS, No. 79-110-RE, slip op. at 3-4 (D. Or. Oct. 1, 1982) (holding that publication of employees' reasons for taking sick leave is improper); Fitzpatrick v. IRS, 1 Gov't Disclosure Serv. (P-H) ¶ 80,232, at 80,580 (N.D. Ga. Aug. 22, 1980) (holding disclosure of fact that employee's absence was due to "mental problems" is improper; "quelling rumors and gossip [and] satisfying curiosity is not to be equated with a need to know"), aff'd in part, vacated & remanded in part, on other grounds, 665 F.2d 327 (11th Cir. 1982); *see also* Walia v. Napolitano, 986 F. Supp. 2d 169, 187 (E.D.N.Y. 2013) (finding that plaintiff "adequately allege[d] that the disclosure regarding his EEO complaint was not on a 'need to know' basis for the employees to perform their duties"); Bigelow v. DOD, 217 F.3d 875, 879 (D.C. Cir. 2000) (Tatel, J., dissenting) (interpreting DOD regulations to

find that supervisor did not have official need to review personnel security file of individual he supervised); Boyd v. Snow, 335 F. Supp. 2d 28, 38-39 (D.D.C. 2004) (denying summary judgment where there are “serious questions” as to whether plaintiff’s rebuttal statement to her performance evaluation was disclosed to certain personnel in plaintiff’s office pursuant to “need to know”); Vargas v. Reno, No. 99-2725, slip op. at 3, 12-13 (W.D. Tenn. Mar. 31, 2000) (denying summary judgment where insufficient evidence that disclosure of plaintiff’s file to Inspector General agent investigating another employee was based on agent’s “need to know”); cf. Berry v. Henderson, No. 99-283-P-C, 2000 WL 761896, at *1, 3 (D. Me. May 8, 2000) (finding that agency’s examination of personnel and medical records within its possession in connection with its defense in Title VII case did not satisfy subsection (b)(1)).

2. 5 U.S.C. § 552a(b)(2) - Required FOIA Disclosure

“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 unless the disclosure would be –

...

(2) required under section 552 of this title [the Freedom of Information Act].” 5 U.S.C. § 552a(b)(2).

Comment:

As a function of the required FOIA disclosure exception, the Privacy Act never prohibits a disclosure that the FOIA requires.

The Privacy Act never prohibits a disclosure that the Freedom of Information Act actually requires. See News-Press v. DHS, 489 F.3d 1173, 1189 (11th Cir. 2007) (“The net effect of the interaction between the two statutes is that where the FOIA requires disclosure, the Privacy Act will not stand in its way, but where the FOIA would permit withholding under an exemption, the Privacy Act makes such withholding mandatory upon the agency.”); Greentree v. U.S. Customs Serv., 674 F.2d 74, 79 (D.C. Cir. 1982) (stating subsection (b)(2) “represents a Congressional mandate that the Privacy Act not be used as a barrier to FOIA access”). See also Burwell v. EOUSA, 210 F. Supp. 3d 33, 36 (D.D.C. 2016) (“Privacy Act specifically exempts from its nondisclosure provisions documents that are otherwise required to be disclosed under the FOIA, see 5 U.S.C. §552a(b)(2), and

EOUSA processed plaintiff's request under the FOIA."); Sikes v. United States, 987 F. Supp. 2d 1355, 1372 n.14 (S.D. Ga. 2013) (finding that because FOIA required disclosure of list of names of individuals invited to ceremony at which Navy officer was sworn in as Chief of Naval Operations, Privacy Act did not bar disclosure); Woods v. DOJ, 968 F. Supp. 2d 115, 120-21 (D.D.C. 2013) (finding that "defendant properly considered plaintiff's request in light of the FOIA, [and thus] any issue arising under the Privacy Act is essentially moot"); Plunkett v. DOJ, 924 F. Supp. 2d 289, 306-07 (D.D.C. 2013) ("[T]he Privacy Act does not bar disclosure of documents that are otherwise required to be disclosed under the FOIA . . . and defendant properly reviewed and released responsive records under the FOIA.").

Thus, if an agency is in receipt of a FOIA request for information about an individual that is contained in a system of records and that is not properly withholdable under any FOIA exemption, then it follows that the agency is "required under Section 552 of this title" to disclose the information to the FOIA requester. This would be a required subsection (b)(2) disclosure. However, if a FOIA exemption – typically, Exemption 6 (personnel and medical files) or Exemption 7(C) (law enforcement information that could be an invasion of personal privacy) – applies to a Privacy Act-protected record, the Privacy Act prohibits an agency from making a "discretionary" FOIA release because that disclosure would not be "required" by the FOIA within the meaning of subsection (b)(2). See, e.g., DOD v. FLRA, 510 U.S. 487, 502 (1994); Big Ridge, Inc. v. Fed. Mine Safety and Health Review Comm'n, 715 F.3d 631, 651 (7th Cir. 2013); Navy v. FLRA, 975 F.2d 348, 354-56 (7th Cir. 1992); Andrews v. VA, 838 F.2d 418, 422-24 & n.8 (10th Cir. 1988); Roble v. DOJ, 311 F. Supp. 3d 161, 163-64 (D.D.C. 2018); Ecological Rights Found. v. FEMA, No. 16-cv-05254, slip op. at 14-16 (N.D. Cal. Nov. 30, 2017); Jett v. FBI, 139 Akmal v. United States, No. C12-1499, 2014 WL 906231, at *3 (W.D. Wash. Mar. 7, 2014); Robbins v. HHS, No. 1:95-cv-3258, slip op. at 2-9 (N.D. Ga. Aug. 13, 1996), aff'd, 120 F.3d 275 (unpublished table decision) (11th Cir. July 8, 1997); Kassel v. VA, 709 F. Supp. 1194, 1199-1200 (D.N.H. 1989); Howard v. Marsh, 654 F. Supp. 853, 855-56 (E.D. Mo. 1986), aff'd, 855 F.2d 855 (8th Cir. 1988) (unpublished table decision); Fla. Med. Ass'n v. HEW, 479 F. Supp. 1291, 1305-07 (M.D. Fla. 1979), vacated, 947 F. Supp. 2d 1325 (M.D. Fla. 2013); Providence Journal Co. v. FBI, 460 F. Supp. 762, 767 (D.R.I. 1978), rev'd on other grounds, 602 F.2d 1010 (1st Cir. 1979); Phila. Newspapers, Inc. v. DOJ, 405 F. Supp. 8, 10 (E.D. Pa. 1975); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,954, https://www.justice.gov/paover/view_omb-75.

After DOJ v. Reporters Comm. for Freedom of the Press, the FOIA is less likely to require disclosure of Privacy Act-protected records.

In DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 762-75 (1989), the Supreme Court significantly expanded the breadth of FOIA Exemptions 6 and 7(C). The Court ruled that a privacy interest may exist in publicly available information – such as the criminal history records there at issue – where the information is “practically obscure.” Id. at 764-71. Even more significantly, the Court held that the identity of the FOIA requester, and any socially useful purpose for which the request was made, are not to be considered in evaluating whether the “public interest” would be served by disclosure. Id. at 771-75. The Court determined that the magnitude of the public interest side of the balancing process can be assessed only by reference to whether disclosure of the requested records directly advances the “core purpose” of the FOIA – to shed light on the operations and activities of the government. Id. at 774-75.

In light of Reporters Comm., personal information of the sort protected by the Privacy Act is less likely to be “required” to be disclosed under the FOIA, within the meaning of subsection (b)(2). Specifically, where an agency determines that the only “public interest” that would be furthered by a disclosure is a nonqualifying one under Reporters Comm. (even where it believes that disclosure would be in furtherance of good public policy generally), it may not balance in favor of disclosure under the FOIA and therefore disclosure will be prohibited under the Privacy Act – unless authorized by another Privacy Act exception or by written consent. See, e.g., DOD v. FLRA, 510 U.S. at 497-502 (declining to “import the policy considerations that are made explicit in the Labor Statute into the FOIA Exemption 6 balancing analysis” and, following the principles of Reporters Comm., holding that home addresses of bargaining unit employees are covered by FOIA Exemption 6 and thus that Privacy Act “prohibits their release to the unions”); Schwarz v. INTERPOL, 48 F.3d 1232, at 1-2 & n.2 (10th Cir. Feb. 28, 1995) (balancing under Reporters Comm. and holding that individual clearly has protected privacy interest in avoiding disclosure of his whereabouts to third parties; disclosure of this information would not “contribute anything to the public’s understanding of the operations or activities of the government”; and thus any information was exempt from disclosure under FOIA Exemption 7(C) and does not fall within Privacy Act exception (b)(2)); FLRA v. Commerce, 962 F.2d 1055, 1059 (D.C. Cir. 1992) (asserting that Privacy Act prohibits disclosure of identities of individuals who received outstanding or commendable personnel evaluations, as such information falls within FOIA Exemption 6); Doe v. Veneman, 230 F. Supp.

2d 739, 748-52 (W.D. Tex. 2002) (finding that in reverse FOIA lawsuit where information regarding government program for protection of livestock using livestock-protection collars already had been released, no personally identifying information about particular ranchers and farmers participating in program “could shed any further light on the workings of the [program],” that information thus was protected by FOIA Exemption 6, and disclosure was prohibited by Privacy Act), aff’d in part, rev’d in part, on other grounds, 380 F.3d 807 (5th Cir. 2004); Fort Hall Landowners Alliance, Inc. v. BIA, No. CV-99-00052-E-BLW, slip op. at 7-14 (D. Idaho Mar. 17, 2000) (finding document that “contains only names and addresses . . . does not provide information shedding light on how the BIA is performing its duties,” and that “[h]aving determined that disclosure of the information is not required by FOIA . . . the Privacy Act prohibits disclosure of the information”); Burke v. DOJ, No. 96-1739, 1999 WL 1032814, at *3-5 (D.D.C. Sept. 30, 1999) (stating that “Privacy Act prohibits the FBI from disclosing information about a living third party without a written privacy waiver, unless FOIA requires disclosure,” and upholding FBI’s refusal to confirm or deny existence of investigative records related to third parties in response to FOIA request) (emphasis in original); see also FOIA Update, Vol. X, No. 2, at 3, http://www.justice.gov/oip/foia_updates/Vol_X_2/page3.html. As a result of Reporters Comm., agencies depend more on the subsection (b)(3) routine use exception to make compatible disclosures of records that are no longer required by the FOIA to be disclosed. See, e.g., USDA v. FLRA, 876 F.2d 50, 51 (8th Cir. 1989); see also FLRA v. Treasury, 884 F.2d 1446, 1450 & n.2 (D.C. Cir. 1989).

Note that President Barack Obama’s FOIA policy on openness in government, see Memorandum for the Heads of Executive Departments and Agencies, Subject: Freedom of Information Act (Jan. 21, 2009), https://www.justice.gov/paoverview_agfoia, is inapplicable to information covered by the Privacy Act that also falls under one or more of the FOIA exemptions. See U.S. Dep’t of Justice, Off. of Info. Pol’y, OIP Guidance: President Obama’s FOIA Memorandum and Attorney General Holder’s FOIA Guidelines (April 17, 2009), <https://www.justice.gov/oip/blog/foia-post-2009-creating-new-era-open-government> (“For information falling within Exemptions 6 and 7(C), if the information is also protected by the Privacy Act of 1974, it is not possible to make a discretionary release, as the Privacy Act contains a prohibition on disclosure of information not ‘required’ to be released under the FOIA.”).

The D.C. Circuit has held that the required FOIA disclosure exception cannot be invoked unless an agency actually has a FOIA request in hand; not all courts agree.

The Court of Appeals for the District of Columbia Circuit significantly limited the utility of subsection (b)(2) as a defense by holding that subsection (b)(2) cannot be invoked unless an agency actually has a FOIA request in hand. Bartel v. FAA, 725 F.2d 1403, 1411-13 (D.C. Cir. 1984); see also Chang v. Navy, 314 F. Supp. 2d 35, 41-42 (D.D.C. 2004) (citing Bartel, and noting that defendant agency conceded that it “had no FOIA request in hand”). In one case prior to Bartel, it similarly had been held that subsection (b)(2) was not available as a defense for the disclosure of information in the absence of a FOIA request. Zeller v. United States, 467 F. Supp. 487, 503 (E.D.N.Y. 1979) (finding subsection (b)(2) inapplicable to the “voluntary re-release” of a prior press release (that had been made prior to the effective date of the Privacy Act) as “nothing in the FOIA appears to require such information to be released in the absence of a request therefor”).

Other courts have not followed the rule in Bartel, however, and do not require agencies to have a FOIA request in hand to raise a (b)(2) defense. See Cochran v. United States, 770 F.2d 949, 957-58 & n.14 (11th Cir. 1985) (applying subsection (b)(2) – in absence of written FOIA request – because requested records would not be withholdable under any FOIA exemption); Jafari v. Navy, 728 F.2d 247, 249-50 (4th Cir. 1984) (same); Russo v. United States, 576 F. Supp. 2d 662, 671-72 (D.N.J. 2008) (alternative holding) (expressing reluctance to follow Bartel because subsection (b)(2)'s conditional language of “would be” rather than “is” “casts serious doubt upon Plaintiff’s argument that the exception only applies where the agency is faced with a written FOIA request”); Mudd v. Army, No. 2:05-cv-137, 2007 WL 4358262, at *6 (M.D. Fla. Dec. 10, 2007) (agreeing with agency that “under the circumstances of this case, the balance of plaintiff’s privacy against the public’s right to disclosure weighs in favor of public disclosure, and that the FOIA exception was applicable even without a formal FOIA request”).

However, because the D.C. Circuit is the jurisdiction of “universal venue” under the Privacy Act -- i.e., any Privacy Act lawsuit for wrongful disclosure could be filed within that judicial circuit -- see 5 U.S.C. § 552a(g)(5) -- its holding in Bartel is of paramount importance. See FOIA Update, Vol. V, No. 3, at 2, http://www.justice.gov/oip/foia_updates/Vol_V_3/page2.htm (discussing Bartel). Note also, though, that the Bartel decision left open the possibility that certain types of information “traditionally released by an agency to the public” might properly be disclosed even in the absence of an

actual FOIA request. 725 F.2d at 1413 (dictum). Reacting to Bartel, OMB issued guidance indicating that records that have “traditionally” been considered to be in the public domain, and those that are required to be disclosed to the public – such as names and office telephone numbers of agency employees – can be released without waiting for an actual FOIA request. Memorandum from Robert P. Bedell, Deputy Administrator, Office of Information and Regulatory Affairs, for the Senior Agency Officials for Information Resource Management, Privacy Act Guidance – Update (May 24, 1985) [hereinafter OMB Bedell Memo], https://www.justice.gov/paoverview_omb-85 (“Records which have traditionally been considered to be in the public domain and are required to be disclosed to the public, such as many of the final orders and opinions of quasi-judicial agencies, press releases, etc. may be released under this provision without waiting for a specific Freedom of Information Act request”); see also OMB Call Detail Guidance, https://www.justice.gov/paoverview_omb-87-cd (applying Bartel to “call detail” programs); OMB 1975 Guidelines, 40 Fed. Reg. at 28,954, https://www.justice.gov/paoverview_omb-75.

The District Court for the District of Columbia twice has applied this public domain aspect of Bartel. In Tripp v. DOD, 193 F. Supp. 2d 229, 236 (D.D.C. 2002), the D.C. District Court held that “the names, titles, salaries, and salary-levels of public employees are information generally in the public domain” and thus that they are not prohibited from disclosure under subsection (b)(2). In Chang v. Navy, 314 F. Supp. 2d at 42, the District Court found that the Privacy Act was not violated where the Navy disclosed information to the media about plaintiff’s nonjudicial punishment, because the information was “releasable” under the FOIA, and the Navy had asserted that it “traditionally releases information that would be releasable under the FOIA to the press without a formal FOIA request,” and was able to point to a Navy regulation to that effect. Id.; see also Russo, 576 F. Supp. 2d at 670-73 (D.N.J. 2008) (alternative holding) (concluding disclosure of active duty military status did not violate Privacy Act because “duty status is the sort of public-domain information traditionally released to the public in the absence of a FOIA request”).

For further analysis of the interplay between the FOIA and the Privacy Act, see “Individual’s Right of Access” section below, particularly the “FOIA/Privacy Act Interface Examples: Access” subsection.

3. 5 U.S.C. § 552a(b)(3) - Routine Uses

“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 unless the disclosure would be --

...

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D).” 5 U.S.C. § 552a(b)(3).

Cross-references:

Subsection (a)(7) defines the term “routine use” to mean “with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected.”

Subsection (e)(4)(D) requires Federal Register publication of “each routine use of the records contained in the system, including the categories of users and the purpose of such use.”

Comment:

The routine use disclosure exception is broad and was designed to allow disclosures other than intra-agency disclosures.

The routine use exception, because of its potential breadth, is one of the most controversial provisions in the Act. See Privacy Commission Report, at 517-18, https://www.justice.gov/paoverview_ppsc. The trend in recent cases is toward a narrower construction of the exception. The White House directed the OMB to issue additional guidance regarding the routine use exception in an executive memorandum on privacy sent to the heads of executive departments and agencies in 1998. Memorandum on Privacy and Personal Information in Federal Records, 34 Weekly Comp. Pres. Doc. 870 (May 14, 1998), https://www.justice.gov/paoverview_pmpipfr. See also U.S. Dep’t of Justice, Off. of Info. Pol’y, President Issues Privacy Act-Related Memorandum to All Federal Agencies, in FOIA Update, Vol. XIX, No. 2, at 1, <https://www.justice.gov/oip/blog/foia-update-president-issues-privacy-act-related-memorandum-all-federal-agencies> (providing summary of executive memorandum).

The routine use exception “was developed to permit other than intra-agency disclosures”; therefore “[i]t is not necessary . . . to include intra-agency transfers in the portion of the system notice covering routine uses.” OMB 1975 Guidelines, 40 Fed. Reg. at 56,742 (Dec. 4, 1975), <https://www.justice>.

[gov/paoverview_omb-75-suppl](https://www.justice.gov/paoverview_omb-75-suppl). But see *O'Donnell v. DOD*, No. 04-00101, 2006 WL 166531, at *8 n.8 (E.D. Pa. Jan. 20, 2006) (on motion to dismiss, disagreeing with plaintiff that “routine use” should be defined as “the disclosure of a record outside of [DOD]” and explaining that “the ‘routine use’ exception specifically states that disclosure is allowed ‘for a routine use as defined in subsection (a)(7) of [the Act]’”); cf. *Shayesteh v. Raty*, No. 02:05-CV-85TC, 2007 WL 2317435, at *5 (D. Utah Aug. 7, 2007) (concluding that disclosures were proper under subsection (b)(1) and explaining that purpose of disclosures was compatible with purpose of collection under subsection (b)(3)).

The routine use disclosure exception requires an agency to: (1) publish the routine use to provide constructive notice; and (2) disclose records only when compatible with the purpose for which the record was collected; some courts also have required agencies to provide actual notice in accordance with subsection (e)(3)(C).

An agency must meet two requirements for a proper routine use disclosure under this exception: (1) an agency must publish the routine use in the Federal Register to provide constructive notice; and (2) the disclosure of the record must be compatible with the purpose for which the record was collected. See, e.g., *Britt v. Naval Investigative Serv.*, 886 F.2d 544, 547-50 (3d Cir. 1989); *Brunotte v. Johnson*, 892 F. Supp. 2d 199, 207 (D.D.C. 2012); *Shannon v. Gen. Elec. Co.*, 812 F. Supp. 308, 316 (N.D.N.Y. 1993).

The Court of Appeals for the Ninth Circuit has added a third requirement for this exception, which the Court of Appeals for the District of Columbia Circuit subsequently adopted: actual notice at the time the information is collected from the individual of the purpose(s) for which the information will be used. See 5 U.S.C. § 552a(e)(3)(C); *Covert v. Harrington*, 876 F.2d 751, 754-56 (9th Cir. 1989) (discussed below); *USPS v. Nat’l Ass’n of Letter Carriers*, 9 F.3d 138, 146 (D.C. Cir. 1993).

a. Federal Register Constructive Notice

Before relying on the routine use disclosure exception, an agency must publish in the Federal Register each routine use, including the categories of users and the purpose of such use.

The notice requirement of the routine use exception “is intended to serve as a caution to agencies to think out in advance what uses [they] will make of information.” 120 Cong. Rec. 40,881 (1974), reprinted in Source Book at 987, https://www.justice.gov/opcl/paoverview_sourcebook.

Indeed, a routine use could be deemed facially invalid if it fails to satisfy subsection (e)(4)(D), and specify “the categories of users and the purpose of such use.” See Britt, 886 F.2d at 547-48 (dictum) (suggesting that routine use, 50 Fed. Reg. 22,802-03 (May 29, 1985) (permitting disclosure to “federal regulatory agencies with investigative units” is overbroad because it “does not provide adequate notice to individuals as to what information concerning them will be released and the purposes of such release); cf. Krohn v. DOJ, No. 78-1536, slip op. at 4-7 (D.D.C. Mar. 19, 1984) (“[T]o qualify as a ‘routine use,’ the agency must . . . publish in the Federal Register . . . ‘each routine use of the records contained in the system, including the categories of users and the purpose of such use.’”), reconsideration granted & vacated in non-pertinent part, (D.D.C. Nov. 29, 1984) (discussed below).

The scope of the routine use disclosure exception is limited to the published terms of the claimed routine use.

It is well settled that the “scope of [a] routine use[] is confined by the published definition.” Doe v. Naval Air Station, Pensacola, Fla., 768 F.2d 1229, 1231 (11th Cir. 1985); see also Parks v. IRS, 618 F.2d 677, 681-82 (10th Cir. 1980); Tran v. Treasury, 351 F. Supp. 3d 130, 137 (D.D.C. 2019); Local 2047, AFGE v. Def. Gen. Supply Ctr., 423 F. Supp. 481, 484-86 (E.D. Va. 1976), aff’d, 573 F.2d 184 (4th Cir. 1978). In other words, a particular disclosure is unauthorized if it does not fall within the clear terms of the routine use. See, e.g., Swenson v. USPS, 890 F.2d 1075, 1078 (9th Cir. 1989) (stating that, consistent with Federal Register notice, “[d]isclosure may be made to a congressional office from the record of an individual in response to an inquiry from the congressional office made at the request of that individual”); Tijerina v. Walters, 821 F.2d 789, 798 (D.C. Cir. 1987) (VA’s unsolicited letter notifying state board of bar examiners of possible fraud did not qualify for Privacy Act’s routine use exception because the published routine use only permitted disclosure based upon official request of state agency and no such request was made); Doe v. DiGenova, 779 F.2d 74, 86 (D.C. Cir. 1985) (holding routine use exception inapplicable to VA psychiatric report because published routine use allowed referral of records to law enforcement officials only when records themselves indicated violation of law, and record itself did not “indicate[] . . . a potential violation of law”); Tran, 351 F. Supp. 3d at 137 (holding that routine use allowing disclosure to “a Federal . . . agency . . . [of] information relevant or necessary to hiring or retaining an employee . . . or other benefit” did not permit intra-agency disclosure of plaintiff’s performance evaluation in connection with plaintiff’s detail request);

Shearson v. DHS, No. 1:06 CV 1478, 2012 WL 398444, at *3 (N.D. Ohio Feb. 6, 2012) (finding, where published routine use required agency first to be “aware of an indication of a violation or potential violation of” law and individual alleged that she had no criminal record, plaintiff “fairly alleges that defendants did not meet the ‘routine use’ exception because the disclosing agency could not have been aware of any wrongful behavior”); Cooper v. FAA, No. 3:07-cv-01383, slip op. at 14-15 (N.D. Cal. Aug. 22, 2008) (concluding that “when DOT-OIG sent the name, social security number, date of birth and gender of approximately 45,000 pilots to SSA-OIG, it was not because those records indicated a violation or potential violation of the law,” as required by language of DOT routine use), rev’d on other grounds, 596 F.3d 538 (9th Cir. 2010), rev’d on other grounds, 131 S. Ct. 3025 (2012); Bechhoefer v. DOJ, 179 F. Supp. 2d 93, 101-02 (W.D.N.Y. 2001) (finding, that where letter was collected by agency due to its initial interest in investigating plaintiff’s allegations of illegal drug activity by local law enforcement agency and was disclosed to that agency’s investigator, whose interest was in investigating possible unlawful, non-drug-related activity by plaintiff himself, such disclosure was not proper pursuant to routine use providing for disclosure to state and local law enforcement because “it is difficult to see how [the] disclosure could be said to have been compatible with the purpose for which the letter was collected”), aff’d on other grounds, 312 F.3d 563 (2002), cert. denied sub nom. Bechhoefer v. DEA, 539 U.S. 514 (2003); Kvech v. Holder, No. 10-cv-545, 2011 WL 4369452, at *3-4 (D.D.C. Sept. 19, 2011) (ruling that dismissal was not warranted where “record does not contain any evidence regarding precisely what information was disclosed . . . and the extent to which the disclosures fell inside or outside the confines of” the routine use); Pontecorvo v. FBI, No. 00-1511, slip op. at 13-15 (D.D.C. Sept. 30, 2001) (denying agency summary judgment and ordering discovery to determine whether agency “overstepped [the] explicit restrictions” contained in its routine use); Vargas v. Reno, No. 99-2725, slip op. at 3, 12-13 (W.D. Tenn. Mar. 31, 2000) (stating that routine use exception did not apply to disclosure of plaintiff’s record to DOJ Inspector General agent conducting investigation of another employee because record was “‘owned’ by the Office of Personnel Management”; “The mere existence of an investigation at a facility is not sufficient to allow an investigating agent access to the records of every employee who is employed at that facility.”); Greene v. VA, No. C-76-461-S, slip op. at 3-6 (M.D.N.C. July 3, 1978) (holding routine use exception inapplicable to VA’s disclosure of medical evaluation to state licensing bureau because routine use permitted disclosure only to facilitate VA decision); see also Covert v. Harrington, 667 F. Supp. 730, 736-39 (E.D. Wash. 1987), aff’d on other

grounds, 876 F.2d 751 (9th Cir. 1989).

When interpreting a claimed routine use, courts have generally deferred to agency interpretation.

An agency's construction of its routine use should be entitled to deference. See Air Force v. FLRA, 104 F.3d 1396, 1402 (D.C. Cir. 1997) (according great deference to OPM's interpretation of its routine use); FLRA v. Treasury, 884 F.2d 1446, 1455-56 (D.C. Cir. 1989) ("For purposes of determining the scope of OPM's routine use notice . . . an official OPM interpretation would be entitled to great deference."); Makowski v. United States, 27 F. Supp. 3d 901, 912 (N.D. Ill. 2014) (deferring to, and finding reasonable, agencies' interpretation and application of Enhanced Border Security Act because Court found statute ambiguous as to what it required FBI to do upon receiving plaintiff's fingerprints, thus finding publication requirement of FBI's routine use exception to have been met); Radack v. DOJ, 402 F. Supp. 2d 99, 106 n.7 (D.D.C. 2005) ("The court must grant 'great deference' to agency interpretations of routine uses."); cf. Stafford, 437 F. Supp. 2d at 1119 (relying on SSA regulations for proposition that "SSA generally would consider a use to be compatible if it relates to determining eligibility for needs-based income maintenance . . . or related medical benefits for low-income people" and concluding that SSA's disclosure of child abuse suspect's "precise medical diagnosis to [California Child Protective Services] . . . was not compatible with the purpose for which the information was collected"). But see NLRB v. USPS, 790 F. Supp. 31, 33 (D.D.C. 1992) (rejecting Postal Service's interpretation of its own routine use).

b. Compatibility

The term "compatible" is not defined in the Privacy Act, and agencies must assess, on a case-by-case basis, when a disclosure is compatible in accordance with the routine use disclosure exception.

The precise meaning of the term "compatible" is uncertain and must be assessed on a case-by-case basis. According to OMB, the "compatibility" concept encompasses (1) functionally equivalent uses and (2) other uses that are necessary and proper. OMB Call Detail Guidance, 52 Fed. Reg. at 12,993, https://www.justice.gov/paoverview_omb-87-cd.

In Britt, an early, leading case on "compatibility," the Court of Appeals for the Third Circuit ruled that the Naval Investigative Service's gratuitous

disclosure of records, describing a then-pending criminal investigation of a Marine Corps reservist, to that individual's civilian employer (the Immigration and Naturalization Service) was not "compatible" with the "case-specific purpose for collecting" such records. 886 F.2d at 547-50. Holding that the employment/suitability purpose for disclosure was incompatible with the criminal law enforcement purpose for collection, the Third Circuit deemed significant that "[t]here is nothing in the record suggesting that the [Immigration and Naturalization Service] was conducting its own criminal investigation of the same activity or any other activity" by the subject and that the records at issue concerned "merely a preliminary investigation with no inculpatory findings." *Id.* at 549-50. Employing especially broad language, the Third Circuit pointedly condemned the agency's equating of "compatibility" with mere "relevance" to the recipient entity, observing that "[t]here must be a more concrete relationship or similarity, some meaningful degree of convergence, between the disclosing agency's purpose in gathering the information and in its disclosure." *Id.* (citing Covert, 876 F.2d at 755 (dictum)); see also Chichakli v. Tillerson, 882 F.3d 229, 233-34 (D.C. Cir. 2018) (holding that purpose of collection of plaintiff's identifying information by State Department and Office of Foreign Assets Control was to investigate whether to designate plaintiff for economic sanctions and implement sanctions, which was "precisely aligned" with purpose of disclosure – to implement sanctions by making information public); Townsend v. United States, 236 F. Supp. 3d 280, 318 (D.C. Cir. 2017); Mazaleski v. Truesdale, 562 F.2d 701, 713 n.31 (D.C. Cir. 1977) (dictum); Ames v. DHS 153 F. Supp. 3d 342, 347 (D.D.C. 2016) (citing Britt and finding that DHS OIG had prepared report on plaintiff to determine whether plaintiff had committed misconduct in national security position, and its purpose in disclosing report to plaintiff's new agency was precisely same, to prevent misconduct by plaintiff at another national security agency), *aff'd* 861 F.3d 238 (D.C. Cir. 2017); accord Swenson, 890 F.2d at 1078; cf. Quinn v. Stone, 978 F.2d 126, 139 (3d Cir. 1992) (Nygaard, J., dissenting) (concluding that disclosure was authorized by routine use because disclosure was compatible with one of purposes for collection, even if not compatible with main purpose for collection).

The Court of Appeals for the D.C. Circuit interpreted the term "compatibility" in considering a routine use that provided for disclosure to labor organizations as part of the collective bargaining process. The court stated that "common usage" of the word would require simply that "a proposed disclosure would not actually frustrate the purposes for which the information was gathered." USPS, 9 F.3d at 144. The D.C.

Circuit recognized the “far tighter nexus” required by the Third and Ninth Circuits in Britt and Swenson, which is consistent with the legislative history, but stated:

Whatever the merit of the decisions of prior courts that have held . . . that a finding of a substantial similarity of purpose might be appropriate in the non-labor law context in order to effectuate congressional intent, the compatibility requirement imposed by section 552a(a)(7) cannot be understood to prevent an agency from disclosing to a union information as part of the collective bargaining process.

Id. at 145. In a concurring opinion, Judge Williams agreed with the disposition of the case, but noted that he did not share the “belief that the meaning of ‘compatible’ . . . may depend on the identity of the entity to which information is being disclosed.” Id. at 147 n.1 (Williams, J., concurring). Rather, seeing “no *conflict* between the purposes for which the information was collected and those for which it will be disclosed,” he found the disclosure to be compatible without further inquiry. Id. at 146-47. But cf. Pontecorvo v. FBI, No. 00-1511, slip op. at 10-11 (D.D.C. Sept. 30, 2001) (recognizing the D.C. Circuit’s holding in USPS case, but finding “the test articulated by the Third and Ninth circuits to be controlling” in the non-labor law context).

OMB guidelines, and some courts, have found that routine use disclosures to law enforcement agencies in the context of investigations or prosecutions, or when the record indicates a possible violation of law, are “compatible” disclosures under the routine use disclosure exception.

Two examples of “compatible” routine uses frequently occur in the law enforcement context. First, in the context of investigations or prosecutions, law enforcement agencies routinely may share law enforcement records with one another. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,955, https://www.justice.gov/paoverview_omb-75 (“Records in law enforcement systems may also be disclosed for law enforcement purposes when that disclosure has properly been established as a ‘routine use’; e.g., . . . transfer by a law enforcement agency of protective intelligence information to the Secret Service.”); see also, e.g., 28 U.S.C. § 534 (2018) (requiring Attorney General to exchange criminal records with “authorized officials of the Federal Government . . . , the States . . . , Indian tribes, cities, and penal and other institutions”).

Second, agencies routinely may disclose to law enforcement agencies for purposes of investigation or prosecution any records indicating a possible violation of law (regardless of the purpose for collection) if the head of the law enforcement agency specifically requests the record in writing from the agency that maintains the record. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,953, 28,955, https://www.justice.gov/paoverview_omb-75 (remarks of Congressman Moorhead); 120 Cong. Rec. 36,967, 40,884 (1974), reprinted in Source Book at 957-58, 995, https://www.justice.gov/opcl/paoverview_sourcebook; see also, e.g., 28 U.S.C. § 535(b) (2018) (requiring agencies of executive branch to report expeditiously to U.S. Attorney General “[a]ny information, allegation, matter, or complaint” relating to crimes involving government officers and employees).

These compatible use disclosures to law enforcement agencies have been criticized on the ground that they circumvent the more restrictive requirements of subsection (b)(7). See Privacy Commission Report, at 517-18, https://www.justice.gov/paoverview_ppsc; see also Britt, 886 F.2d at 548 n.1 (dictum); Covert, 667 F. Supp. at 739, 742 (dictum). They never have been challenged successfully on that basis, however. Indeed, courts routinely have upheld disclosures made pursuant to such routine uses. See, e.g., Bansal v. Pavlock, 352 F. App’x 611, 613-14 (3d Cir. 2009) (upholding disclosure of detainee’s recorded telephone conversations by Marshals Service to government case agent, who disclosed recording to interpreter, who disclosed recording to second interpreter); Weinberger v. Grimes, No. 07-6461, 2009 WL 331632, at *8 (6th Cir. Feb. 10, 2009) (stating that BOP routine use “includes disclosure to federal law enforcement agencies for ‘court-related purposes’ including ‘civil court actions’”); Shearson v. Holder, 865 F. Supp. 2d 850, 870 (N.D. Ohio 2011) (ruling that FBI “dissemination of watchlist information to CBP officers to facilitate their border security responsibilities” fell within published routine use to agencies “engaged in terrorist screening”); Ray v. DHS, No. H-07-2967, 2008 WL 3263550, at *12-13 (S.D. Tex. Aug. 7, 2008) (discussing disclosure by OIG of results of investigation concerning plaintiff’s SF 85P to U.S. Attorney’s Office was proper because it was covered by published routine use); Freeman v. EPA, No. 02-0387, 2004 WL 2451409, at *6-7 (D.D.C. Oct. 25, 2004) (concluding that “disclosure [by DOD investigator hired by EPA] of the plaintiff’s records concerning drug testing schedules and test results to AUSA . . . for the purposes of [AUSA’s] investigation of potentially criminal activity is a disclosure that is ‘compatible with the purpose for which [those records were] collected’”); Nwangoro v. Army, 952 F. Supp. 394, 398 (N.D. Tex. 1996) (finding disclosure by Military Police of financial records obtained in ongoing criminal investigation to

foreign customs officials likewise involved in investigation of possible infractions of foreign tax and customs laws was “permitted by the ‘routine use’ exception and d[id] not constitute a violation of the Privacy Act”); Little v. FBI, 793 F. Supp. 652, 655 (D. Md. 1992) (finding that disclosure did not violate Privacy Act prohibition because it was made pursuant to routine use that allows disclosure of personnel matters to other government agencies when directly related to enforcement function of recipient agency), aff’d on other grounds, 1 F.3d 255 (4th Cir. 1993).

The courts have found, however, that a disclosure does not fall within a compatible routine use if the agency is not sharing with a law enforcement agency in the context of an investigation or prosecution, there is no possible violation of law, or the law enforcement agency head has not specifically requested the record in writing. For example, a disclosure is not compatible if it is made to agencies other than the appropriate ones. See Dick v. Holder, 67 F. Supp. 3d 167, 179 (D.D.C. 2014) (holding that FBI’s disclosure of information to law enforcement agencies was not compatible with routine use because information “was not disseminated just to ‘appropriate Federal, State, or local agenc[ies]’”).

Similarly, disclosures are not compatible with a routine use if the record does not reveal a potential violation of law. In Covert, 667 F. Supp. at 736-39, the District Court for the Eastern District of Washington held that a routine use permitting the Department of Energy’s Inspector General to disclose to the DOJ relevant records when “a record” indicates a potential violation of law did not permit the disclosure of personnel security questionnaires submitted by the plaintiffs because such questionnaires, on their face, did not reveal potential violations of law. The court rejected the agency’s argument that disclosure was proper because each questionnaire was disclosed as part of a prosecutive report that (when viewed as a whole) did reveal a potential violation of law. Id. at 736-37. Further, the court found that the Inspector General’s disclosure of the questionnaires to the DOJ (for a criminal fraud prosecution) was not compatible with the purpose for which they originally were collected by the Department of Energy (for a security-clearance eligibility determination), notwithstanding the fact that the Inspector General subsequently acquired the questionnaires – on an intra-agency “need to know” basis pursuant to 5 U.S.C. § 552a(b)(1) – for the purpose of a fraud investigation. Id. at 737-39.

On cross-appeals, a divided panel of the Court of Appeals for the Ninth Circuit affirmed the district court’s judgment on other grounds. Covert,

876 F.2d at 754-56. The panel majority held that the Department of Energy's failure to provide actual notice of the routine use on the questionnaires at the time of original collection, under subsection (e)(3)(C), precluded the Department of Energy from later invoking that routine use under subsection (b)(3). Id. at 755-56; see also Puerta v. HHS, No. 99-55497, 2000 WL 863974, at *1-2 (9th Cir. June 28, 2000) (following Covert but finding that agency had provided notice of routine use on form used to collect information), aff'g No. EDCV 94-0148, slip op. at 7 (C.D. Cal. Jan. 5, 1999); USPS, 9 F.3d at 146 (citing Covert with approval and remanding case for factual determination as to whether subsection (e)(3)(C) notice was given); Stafford, 437 F. Supp. 2d at 1119-20 (adhering to Covert and finding that SSA notified plaintiff of potential uses "on three occasions when collecting her information," even though these notifications were non-specific references to the Federal Register); Pontecorvo, No. 00-1511, slip op. at 12 (D.D.C. Sept. 30, 2001) (stating that agency must comply with subsection (e)(3)(C) "in order to substantiate an exception for 'routine use'"). Prior to Covert, no other court had required actual notice. See the additional discussion under "5 U.S.C. § 552a(e)(3) - Notice Requirements," below.

Since Krohn v. DOJ, agencies have narrowed the scope of their routine use disclosures during legal proceedings, disclosing only records "arguably relevant to the litigation."

Although initially agencies published broad routine uses, they have been narrowed since the District Court for the District of Columbia issued its decision in Krohn v. DOJ, No. 78-1536, slip op. at 4-7 (D.D.C. Mar. 19, 1984). In Krohn, the court invalidated an FBI routine use allowing for "dissemination [of records] during appropriate legal proceedings," finding that such a routine use was impermissibly "vague" and was "capable of being construed so broadly as to encompass all legal proceedings." In response to Krohn, OMB issued guidance to agencies in which it suggested a model routine use – employing a "relevant and necessary to the litigation" standard – to permit the public filing of protected records with a court. OMB Bedell Memo, https://www.justice.gov/paoverview_omb-85. Many agencies, including the DOJ, have adopted "post-Krohn" routine uses designed to authorize the public filing of relevant records in court. See, e.g., 66 Fed. Reg. 36,593, 36,594 (July 12, 2001) (routine use [number 7] applicable to records in DOJ's "Civil Division Case File System"); 63 Fed. Reg. 8,666, 8,667-68 (Feb. 20, 1998) (routine uses [letters "o" and "p"] applicable to records in U.S. Attorney's Office's "Civil Case Files").

The “post-Krohn” routine uses, such as the ones cited above that employ an “arguably relevant to the litigation” standard, have withstood challenges in the courts. See, e.g., Jackson v. FBI, No. 02-C-3957, 2007 WL 2492069, at *8 (N.D. Ill. Aug. 28, 2007) (allowing U.S. Attorney’s filing in court of plaintiff’s unsuccessful application for FBI employment during pendency of plaintiff’s Title VII suit because application was “at the very heart of his civil suit”); Russell v. GSA, 935 F. Supp. 1142, 1145-46 (D. Colo. 1996) (finding disclosure in public pleadings of information regarding investigation of plaintiff was permissible under routine use providing for disclosure in proceeding before court where agency is party and records are determined “to be arguably relevant to the litigation”); Osborne v. USPS, No. 94-30353, slip op. at 6-9 (N.D. Fla. May 18, 1995) (holding on alternative ground that disclosure of plaintiff’s injury-compensation file to retired employee who had prepared file and who had been subpoenaed by plaintiff and was expecting to be deposed on matters documented in file was proper pursuant to routine use providing for disclosures “incident to litigation” and “in a proceeding before a court” because “deposition was a proceeding before [the] Court”); Sheptin v. DOJ, No. 91-2806, 1992 U.S. Dist. LEXIS 6221, at *6-7 (D.D.C. Apr. 30, 1992) (finding no wrongful disclosure where agency routine uses permit use of presentence report during course of habeas proceeding). Such challenges could arise from an argument that the routine use does not satisfy the “compatibility” requirement of subsection (a)(7) of the Act, cf. Britt, 886 F.2d at 547-50 (holding mere “relevance” to recipient entity is improper standard for “compatible” routine use disclosure).

Courts generally have held that routine use disclosures to further an investigation or enabled the receiving or disclosing agency to fulfill its mission are “compatible” disclosures under the routine use disclosure exception.

The courts generally have found that disclosing information is pursuant to a compatible routine use when the information furthered an investigation or enabled either agency to fulfill its mission. See, e.g., Taylor v. United States, 106 F.3d 833, 836-37 (8th Cir. 1997) (finding routine use exception applied to disclosure of federal taxpayer information collected for purpose of federal tax administration to state tax officials for purpose of state tax administration), aff’g Taylor v. IRS, 186 B.R. 441, 446-47, 453-54 (N.D. Iowa 1995); Alphin v. FAA, No. 89-2405, 1990 WL 52830, at *1 (4th Cir. Apr. 13, 1990) (finding routine use exception applied to disclosure of enforcement investigation final report to subject’s customers); Hastings v. Judicial Conference of the United States, 770 F.2d 1093, 1104 (D.C. Cir. 1985) (finding routine use exception applied to

disclosure of criminal investigative records to judicial committee investigating judge); United States v. Miller, 643 F.2d 713, 715 (10th Cir. 1981) (determining that records submitted by individual to parole officer became part of DOJ files and DOJ's use in criminal investigation constitutes routine use); Lugo v. DOJ, 214 F. Supp. 3d 32 (D.D.C. 2016) (finding "directly on point" routine use providing "a record relating to a person held in custody . . . after . . . conviction . . . may be disseminated" to a state parole authority"), aff'd Lugo v. DOJ, 2018 WL 1896491 (D.C. Cir. 2018); Lewis v. SSA, 2015 WL 9664967 (E.D. Tex. 2015) (finding routine use permitted disclosure to law enforcement agency out of concern for safety of SSA employees); Makowski v. United States, 27 F. Supp. 3d 901, 909-912 (N.D. Ill. 2014) (determining that FBI's disclosure of fingerprints of foreign-born U.S. citizen's fingerprints upon arrest to DHS pursuant to the Enhanced Border Security and Visa Entry Reform Act of 2002 is "compatible with the published purposes for which the FBI collected [the fingerprint data]" and its routine use that "permits disclosures '[t]o such recipients and under such circumstances and procedures as are mandated by Federal statute or treaty'"); Middlebrooks v. Mabus, No. 1:11cv46, 2011 WL 4478686, at *7 (E.D. Va. Sept. 23, 2011) (finding disclosure of personnel records about plaintiff, a nurse, to state nursing board, HHS, and other healthcare reporting entities fell within routine use); Alexander v. FBI, 691 F. Supp. 2d 182, 191 (D.D.C. 2010) (finding routine use exception applied to disclosure of individuals' background reports to White House to determine trustworthiness for granting White House access), aff'd, 456 F. App'x 1 (D.C. Cir. 2011); Lucido v. Mueller, No. 08-15269, 2009 WL 3190368, at *5-6 (E.D. Mich. Sept. 29, 2009) (finding routine use exception applied to FBI's disclosure of plaintiff's arrest and indictment on white-collar crimes to financial self-regulatory body where disclosure was required by federal law), aff'd, 427 F. App'x 497 (6th Cir. 2011); Contursi v. USPS, No. 98CV112, slip op. at 2-3 (S.D. Cal. July 6, 1999) (discussing disclosure to county agency in response to its request in connection with investigation of employee), aff'd, 238 F.3d 428 (9th Cir. 2000) (unpublished table decision); Jones v. Runyon, 32 F. Supp. 2d 873, 876 (N.D. W. Va. 1998) (discussing disclosure to credit reporting service of information about plaintiff when requesting employment reports in course of routine investigation of possible workers' compensation fraud), aff'd, 173 F.3d 850 (4th Cir. 1999) (unpublished table decision); Choe v. Smith, No. C-87-1764R, slip op. at 10-11 (W.D. Wash. Apr. 20, 1989) (discussing INS's disclosure to its informant during investigation "to elicit information required by the Service to carry out its functions and statutory mandates"), aff'd, 935 F.2d 274 (9th Cir. 1991) (unpublished table decision); Kimberlin v. DOJ, 605 F.

Supp. 79, 82-83 (N.D. Ill. 1985) (discussing BOP's disclosure of prisoner's commissary account record to probation officer), aff'd, 788 F.2d 434 (7th Cir. 1986); Burley v. DEA, 443 F. Supp. 619, 623-24 (M.D. Tenn. 1977) (analyzing transmittal of DEA records to state pharmacy board); Harper v. United States, 423 F. Supp. 192, 198-99 (D.S.C. 1976) (analyzing IRS's disclosure of plaintiff's identity to other targets of investigation); but cf. Sussman v. Marshals Serv., 494 F.3d 1106, 1122-23 (D.C. Cir. 2007) (vacating grant of summary judgment to Marshals Service because plaintiff's allegations that agents were "'yelling and screaming [their allegations and theories in an effort to intimidate]'" suggests disclosures went beyond what was 'necessary to obtain information or cooperation'" within terms of published routine use).

Courts have generally held that routine use disclosures to process an individual's application for a benefit, program participation, or a position are "compatible" disclosures under the routine use disclosure exception.

Similarly, the courts have concluded that where an individual is applying for a benefit, program, or position, an agency may disclose information during the application process as a compatible routine use. Puerta v. HHS, No. 99-55497, 2000 WL 863974, at *1-2 (9th Cir. June 28, 2000) (finding routine use exception permitted disclosure of plaintiff's grant proposal to qualified expert who was member of peer review group for evaluation of proposal), aff'g No. EDCV 94-0148, slip op. at 7 (C.D. Cal. Jan. 5, 1999); Budik v. United States, 949 F.Supp.2d 14, 29 (D.D.C. Mar. 7, 2013) (holding that disclosure of plaintiff's military performance assessment form for medical personnel by United States Army was compatible with use for which it was collected, "namely to 'manage credentials and privileges of health care providers in the Military Health System'"), aff'd, 2013 WL 6222903 (D.C. Cir. Nov. 19, 2013); Reed v. Navy, 910 F. Supp. 2d 32, 42-43 (D.D.C. 2012) (finding disclosures made in process of investigating allegations against plaintiff and his truthfulness about those allegations for purpose of assessing plaintiff's fitness for duty as police officer fell within defendant's "requesting information" routine use, whereby records may be disclosed to federal, state, and local authorities if necessary to evaluate plaintiff's fitness for duty); Doe v. DOJ, 660 F. Supp. 2d 31, 47-48 (D.D.C. 2009) (discussing disclosure of information regarding employee's mental state, collected for purpose of coordinating his reasonable accommodation request, to state unemployment commission and to contractor to determine employee's eligibility for benefits); Benham v. Rice, No. 0301127, 2005 WL 691871, at *5-6 (D.D.C. Mar. 24, 2005) (discussing disclosure of agency employee's

transfer request to AUSA, who had represented agency in prior discrimination suit brought by employee against agency, so that AUSA “could attempt to settle the pending litigation with [the employee]”); Fattahi v. ATE, 186 F. Supp. 2d 656, 661-64 (E.D. Va. 2002) (discussing disclosure of fact that plaintiff had applied for federal firearms license to condominium association’s counsel for purposes of determining whether firearms dealer could operate out of plaintiff’s specific residential unit), aff’d, 328 F.3d 176, 181 (4th Cir. 2003) (agreeing with district court “that ATF’s routine use must be given ‘a practical reading’ such that disclosures are in accordance with the routine use when they are ‘reasonably necessary to verify pertinent information, [and] not just [when] verification cannot conceivably be obtained by any other means’”); Mumme v. Labor, 150 F. Supp. 2d 162, 174 (D. Me. 2001) (disclosure to agency’s examining physician from investigation file detailing possible health care fraud by former government worker who was being examined regarding continuing eligibility for disability benefits), aff’d, No. 01-2256 (1st Cir. June 12, 2002); Blazy v. Tenet, 979 F. Supp. 10, 26 (D.D.C. 1997) (discussing CIA’s disclosure of information about employee to FBI while FBI was investigating employee’s application for FBI employment), summary affirmance granted, No. 97-5330, 1998 WL 315583 (D.C. Cir. May 12, 1998); Magee v. USPS, 903 F. Supp. 1022, 1029 (W.D. La. 1995) (discussing disclosure of employee’s medical records to clinical psychologist hired by agency to perform fitness-for-duty examination on employee), aff’d, 79 F.3d 1145 (5th Cir. 1996) (unpublished table decision); McNeill v. IRS, No. 93-2204, 1995 U.S. Dist. LEXIS 2372, at *6 (D.D.C. Feb. 7, 1995) (discussing disclosure of IRS personnel records to prospective federal agency employer); but cf. Brunotte v. Johnson, 892 F. Supp. 2d 199, 207 (D.D.C. 2012) (finding “unclear on the current record” whether disclosure to prospective employer of plaintiff’s prior “alleged travel reimbursement infractions” to “see if [p]laintiff had perpetrated another fraud by submitting false employment application information” was “compatible with the purpose for which the information was collected”).

Courts have generally held that routine use disclosures to other parties in litigation are “compatible” disclosures under the routine use exception.

The courts also have determined that disclosure to other parties in litigation constitutes a compatible routine use. Burnett v. DOJ, 213 F. App’x 526, 528 (9th Cir. 2006) (applying routine use exception to disclosure to criminal defendant, against whom plaintiff was to testify, of prior ruling that plaintiff was not credible); Pippinger v. Rubin, 129 F.3d 519, 531-32 (10th Cir. 1997) (finding routine use exception applied to

disclosure of plaintiff's personnel information to MSPB in deposition testimony in another individual's related MSPB proceeding, and to other individual, his attorney, and court reporter in conjunction with MSPB proceeding); Mount v. USPS, 79 F.3d 531, 534 (6th Cir. 1996) (finding routine use exception applied to disclosure of plaintiff's medical information to union official representing him in administrative action in which his mental health was central issue); (ElHelbawy v. Holder, 2015 WL 5676987 (D. Colo. 2015) (concluding that agency was authorized to disclose information from plaintiff's discrimination claim based on routine use permitting disclosure of information "to another federal agency, to a court, or to a party in litigation before a court or in an administrative proceeding being conducted by a federal agency when the government is a party to the judicial or administrative proceeding"); Feathers v. United States, 2015 WL 5263056 (N.D. Calif. 2015) (finding that routine use provided records may be used in proceedings involving federal securities laws in which SEC is party permitted disclosure in SEC case alleging violations of federal securities laws); Mandel v. OPM, 244 F. Supp. 2d 146, 152 (E.D.N.Y. 2003) (alternative holding) (discussing disclosure of information about plaintiff – including summary of charges, supporting information, and copy of OPM's investigation – to his former supervisors in connection with their testimony at plaintiff's MSPB hearing following determination that plaintiff was unsuitable for federal employment due to prior employment record and failure to disclose history), aff'd on other grounds, 79 F. App'x 479 (2d Cir. 2003); Lachenmyer v. Frank, No. 88-2414, slip op. at 4 (C.D. Ill. July 16, 1990) (holding disclosure of investigative report to persons at arbitration hearing is proper under routine use permitting disclosure of "record relating to a case or matter" in "hearing in accordance with the procedures governing such proceeding or hearing").

The Act's legislative history recognizes the "compatibility" of a routine use invoked to publicly file records in court. See 120 Cong. Rec. at 40,884, reprinted in Source Book at 858, 995, <https://www.justice.gov/opcl/pao-verbatim-sourcebook> (routine use appropriate where Justice Department "presents evidence [(tax information from IRS)] against the individual" in court).

Courts have generally held that routine use disclosures to Congress are "compatible" disclosures under the routine use disclosure exception.

Disclosures to Congress also have been deemed compatible routine uses by the courts. See Gowan v. Air Force, 148 F.3d 1182, 1187, 1194 (10th Cir.

1998) (stating disclosure of information regarding individual to Members of Congress in response to inquiries made pursuant to individual's letters requesting assistance was compatible and thus "would likely be protected under the routine use exception"); Feldman v. CIA, 797 F. Supp. 2d 29, 38-39 (D.D.C. 2011) (finding disclosure to Congressional oversight committee complies with statutory reporting requirements); Chang v. Navy, 314 F. Supp. 2d 35, 45-46 (D.D.C. 2004) (discussing disclosure to Members of Congress for purposes of responding to constituent inquiries where, if constituent is other than record subject, only information releasable under FOIA could be disclosed); Harry v. USPS, 867 F. Supp. 1199, 1206-07 (M.D. Pa. 1994) (discussing disclosure of documents regarding individual's employment history, including details of settlement agreement, in response to congressional inquiries "made at the prompting of that individual"), aff'd sub nom. Harry v. USPS, Marvin T. Runyon, 60 F.3d 815 (3d Cir. 1995) (unpublished table decision).

c. Actual Notice

The Ninth and D.C. Circuits also require that an agency give actual notice to an individual at the time the information is collected in accordance with the notice requirements of subsection (e)(3)(C). Covert, 876 F.2d at 754-756; USPS v. Nat'l Ass'n of Letter Carriers, 9 F.3d at 140; accord Puerta v. HHS, No. 99-55497, 2000 WL 863974, at *1-2 (9th Cir. June 28, 2000), aff'g No. EDCV 94-0148, slip op. at 7 (C.D. Cal. Jan. 5, 1999); cf. Stafford v. SSA, 437 F. Supp. 2d 1113, 1119-20 (N.D. Cal. 2006) (adhering to Covert and finding that SSA notified plaintiff of potential uses "on three occasions when collecting her information"; explaining that notice need not "anticipate and list every single potential permutation of a routine use in order to invoke this exception"; and stating, "The Court is not persuaded that Congress intended to place such an impractical burden on federal agencies, which would in effect severely curtail the very exception that Congress sought to carve out in the interest of practicality."). The Court of Appeals for the D.C. Circuit cited this aspect of Covert with approval and remanded a case for determination of whether (e)(3)(C) notice was provided, stating that "[a]lthough the statute itself does not provide, in so many terms, that an agency's failure to provide employees with actual notice of its routine uses would prevent a disclosure from qualifying as a 'routine use,' that conclusion seems implicit in the structure and purpose of the Act." USPS v. Nat'l Ass'n of Letter Carriers, 9 F.3d at 146; see also Minshew v. Donley, 911 F. Supp. 2d 1043, 1073 (D. Nev. 2012) ("While a report to a non-federal employer falls within a routine use, Air Force has failed to respond to [plaintiff's] argument that OPM did not inform

[plaintiff] on the form which OPM used to collect the information, or on a separate form provided to [plaintiff], that [plaintiff's] federal employer may make unsolicited disclosures to private employers regarding the circumstances surrounding [plaintiff's] separation from federal employment.”). But cf. Thompson v. State, 400 F. Supp. 2d 1, 16-17 (D.D.C. 2005) (discussed below under Agency Requirements, “5 U.S.C. § 552a(e)(3) - Inform Individuals when Asking to Collect Information”).

d. Additional Routine Use Matters

Some, but not all, courts of appeals have required agencies to invoke the routine use disclosure exception to disclose certain records to unions.

Four courts have required an agency to invoke a routine use to permit disclosure to unions of names of employees on the theory that refusal to so disclose was an unfair labor practice under the National Labor Relations Act. See NLRB v. USPS, No. 92-2358, 1994 WL 47743, at *3-4 (4th Cir. Feb. 16, 1994); NLRB v. USPS, 888 F.2d 1568, 1572-73 (11th Cir. 1989); NLRB v. USPS, 841 F.2d 141, 144-45 & n.3 (6th Cir. 1988); NLRB v. USPS, 790 F. Supp. 31, 33 (D.D.C. 1992); see also USPS v. Nat'l Ass'n of Letter Carriers, 9 F.3d at 141-46 (holding that “if the Postal Service *could* disclose the information under [its routine use] then it *must* disclose that information, because in the absence of a Privacy Act defense the arbitrator’s award must be enforced,” but remanding case for determination as to whether proper (e)(3)(C) notice was given before requiring invocation of routine use); FLRA v. Navy, 966 F.2d 747, 761-65 (3d Cir. 1992) (alternative holding) (en banc) (holding that release to union of home addresses of bargaining unit employees pursuant to routine use was required under Federal Service Labor-Management Relations Act). But cf. NLRB v. USPS, 660 F.3d 65, 70-72 (1st Cir. 2011) (ruling that USPS routine use for disclosure “[a]s required by applicable law . . . to a labor organization” did not require automatic disclosure of aptitude tests to union because National Labor Relations Act did not require that disclosure, but instead NLRB was required to balance “the interests of the Union in the information against the privacy interests of the employees”).

In addition, the Court of Appeals for the District of Columbia Circuit, in Air Force v. FLRA, granted enforcement of a Federal Labor Relations Authority decision requiring the Air Force to disclose to a union a disciplinary letter that was issued to a bargaining unit employee’s supervisor. 104 F.3d 1396, 1399, 1401-02 (D.C. Cir. 1997). The court held that the Federal Labor-Management Relations Statute required disclosure

of the letter; that because the “Union’s request f[ell] within the Act’s ‘routine use’ exception, the Privacy Act d[id] not bar disclosure”; and that the union therefore was entitled to disclosure of the letter. Id. at 1401-02.

The D.C. Circuit has held that the routine use disclosure exception does not permit disclosures solely based on a federal subpoena, as such disclosures are not permitted under the court order disclosure exception.

The D.C. Circuit concluded that a routine use for complying with a subpoena was inconsistent with the Privacy Act. See Doe v. Stephens, 851 F.2d 1457, 1465-67 (D.C. Cir. 1988) (holding that a VA routine use – permitting disclosure of records “in order for the VA to respond to and comply with the issuance of a federal subpoena” – was invalid under the Administrative Procedure Act because it was inconsistent with the Privacy Act as interpreted in Doe v. DiGenova, 779 F.2d at 78-84, which had found that disclosures pursuant to subpoenas were not permitted by the subsection (b)(11) court-order exception). But cf. Osborne v. USPS, No. 94-30353, slip op. at 6-9 (N.D. Fla. May 18, 1995) (holding on alternative ground that disclosure of plaintiff’s injury-compensation file to retired employee who had prepared file and who had been subpoenaed by plaintiff and was expecting to be deposed on matters documented in file was proper pursuant to routine use that “specifically contemplates that information may be released in response to relevant discovery and that any manner of response allowed by the rules of the forum may be employed”).

Notwithstanding the required FOIA disclosure and the consumer reporting agency disclosure exceptions, the Privacy Act disclosure provision does not provide for nonconsensual disclosures that are governed by other statutes, and agencies should rely on the routine use disclosure exception for such disclosures.

The Privacy Act does not provide for nonconsensual disclosures that are governed by other statutes except for the FOIA (subsection (b)(2)) and the Debt Collection Act (subsection (b)(12)). See, e.g., 42 U.S.C. § 653 (2018) (establishing “Parent Locator Service” and requiring agencies to comply with requests from HHS for addresses and places of employment of absent parents “[n]otwithstanding any other provision of law”). Recognizing this difficulty, the OMB 1975 Guidelines advise that “disclosures, which are in effect congressionally mandated ‘routine uses,’” should be deemed “routine uses” under subsections (e)(11) and (e)(4)(D). 40 Fed. Reg. at 28,954, https://www.justice.gov/paoverview_omb-75; cf. Zahedi v. DOJ, No. 10-694, 2011 WL 1872206, at *5-6 (D. Or. May 16, 2011)

(holding that plaintiff’s claim for improper dissemination “fails both because the disclosure was authorized by [foreign-intelligence sharing] statute and because the dissemination falls within [agency’s] published routine uses”).

4. 5 U.S.C. § 552a(b)(4) - Bureau of the Census

“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 unless the disclosure would be –

...

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of Title 13.” 5 U.S.C. § 552a(b)(4).

Comment:

For a discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,954, https://www.justice.gov/paoverview_omb-75.

5. 5 U.S.C. § 552a(b)(5) - Statistical Research

“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 unless the disclosure would be –

...

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable.” 5 U.S.C. § 552a(b)(5).

Comment:

OMB guidelines suggest that the statistical research disclosure exception is intended to reduce the likelihood that agencies utilize statistical records to “reconstruct” individually identifiable records.

The term “statistical record” is defined in the Act as a record that is not used

in making individual determinations. 5 U.S.C. § 552a(a)(6). One might question whether this exception to subsection (b) is anomalous, because the information to be released is arguably not a “record,” see 5 U.S.C. § 552a(a)(4), or a “disclosure,” see 5 U.S.C. § 552a(b), as it is not identifiable to any individual. The OMB 1975 Guidelines, however, provide a plausible explanation, stating, “[o]ne may infer from the legislative history and other portions of the Act that an objective of this provision is to reduce the possibility of matching and analysis of statistical records with other records to reconstruct individually identifiable records.” 40 Fed. Reg. at 28,954, https://www.justice.gov/paoverview_omb-75.

6. 5 U.S.C. § 552a(b)(6) - National Archives

“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 unless the disclosure would be –

...

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value.” 5 U.S.C. § 552a(b)(6).

Comment:

For a discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,955, https://www.justice.gov/paoverview_omb-75.

7. 5 U.S.C. § 552a(b)(7) - Law Enforcement Request

“No agency shall disclose any record which is contained in a system of records ...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure would be—

...

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which maintains the record specifying the particular portion desired

and the law enforcement activity for which the record is sought.” 5 U.S.C. § 552a(b)(7).

Comment:

The law enforcement request disclosure exception allows certain disclosures, upon written request, to another agency or instrumentality for civil or criminal law enforcement purposes.

This provision allows agencies to disclose records to federal law enforcement agencies and, “upon receipt of a written request, [to] disclose a record to another agency or unit of State or local government for a civil or criminal law enforcement activity.” OMB 1975 Guidelines, 40 Fed. Reg. at 28,955, https://www.justice.gov/paoverview_omb-75.

A request for records under the subsection (b)(7) exception must be for civil or criminal law enforcement purposes. See United States v. Collins, 596 F.2d 166, 169 (6th Cir. 1979) (holding, among other reasons, disclosure of reports authored by someone suspected of fraud satisfied criminal law enforcement activity disclosure condition); SEC v. Dimensional Entm’t Corp., 518 F. Supp. 773, 774-75, 777 (S.D.N.Y. 1981) (finding disclosure was proper because SEC asked Parole Commission to release transcript in question for purpose of assisting SEC with its attempt to secure injunctive relief against defendant after SEC presented evidence that defendant will likely continue his unlawful activity).

While the head of the agency or instrumentality must generally make the written request for the law enforcement request disclosure exception, agencies may, when necessary, delegate this responsibility to officials no lower than the “section chief” level.

The request must be submitted in writing and generally must be from the head of the agency or instrumentality. See Doe v. DiGenova, 779 F.2d 74, 85 (D.C. Cir. 1985) (concluding that VA’s disclosure of veteran’s medical records in response to federal grand jury subpoena was not authorized because federal grand jury subpoena is issued by federal prosecutors, not head of an agency); Doe v. Naval Air Station, 768 F.2d 1229, 1233 (11th Cir. 1985) (“[E]xemption (b)(7) requires a *written* request for disclosure by the head of the agency making such request to the agency which maintains the record.”); see also Reyes v. Supervisor of DEA, 834 F.2d 1093, 1095 (1st Cir. 1987) (noting the record lacked an indication that FBI, United States Probation Office, AUSA, and BOP made a written request for records);

Stafford v. SSA, 437 F. Supp. 2d 1113, 1121 (N.D. Cal. 2006) (finding improper disclosure because head of local agency did not request disclosed information from SSA in writing).

Record-requesting authority may be delegated to lower-level agency officials when necessary, but not below the “section chief” level. The Department of Justice has delegated record-requesting authority to the “head of a component or a United States Attorney, or either’s designee.” 28 C.F.R. § 6.40(c) (2014); cf. Lora v. INS, No. 2:02cv756, 2002 WL 32488472, at *2 (E.D. Va. Oct. 8, 2002) (applying subsection (b)(7) to disclosure of information from INS file upon request from Assistant United States Attorney), aff’d per curiam, 61 F. App’x 80 (4th Cir. 2003).

8. 5 U.S.C. § 552a(b)(8) - Health or Safety of an Individual

“No agency shall disclose any record which is contained in a system of records...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure would be—

...

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual.” 5 U.S.C. § 552a(b)(8).

Comment:

Under this exception, agencies may disclose records under emergency conditions that affect an individual’s health or safety. See Schwarz v. INTERPOL, No. 94-4111, 1995 WL 94664, at *1 n.3 (10th Cir. Feb. 28, 1995) (finding unsubstantiated allegations alone do not constitute “showing of compelling circumstances”); Stafford v. SSA, 437 F. Supp. 2d 1113, 1121 (N.D. Cal. 2006) (holding that SSA did not satisfy health and safety exception because agency did not provide plaintiff requisite notice after disclosing that plaintiff received disability benefits to state child protective services to investigate possible child abuse); Schwarz v. Treasury, 131 F. Supp. 2d 142, 146-47 (D.D.C. 2000) (citing and agreeing with Schwarz v. INTERPOL), aff’d, No. 00-5453, 2001 WL 67463 (D.C. Cir. May 10, 2001); DePlanche v. Califano, 549 F. Supp. 685, 703-04 (W.D. Mich. 1982) (emphasizing emergency nature of exception to be used “where consent cannot be obtained because of time and distance and instant action is required” and noting that “this subsection was intended to apply only to

such valid life and death situations as an airplane crash or epidemic”).

OMB guidelines, in apparent conflict with the text of the health or safety disclosure exception, states that the individual on whom the record pertains “need not necessarily be the individual whose health or safety is at peril.”

According to OMB 1975 Guidelines, the individual about whom records are disclosed “need not necessarily be the individual whose health or safety is at peril; e.g., release of dental records on several individuals in order to identify an individual who was injured in an accident.” 40 Fed. Reg. at 28,955, https://www.justice.gov/paoverview_omb-75 (unsubstantiated allegations that fail to be “compelling circumstances” also fail to justify the release of records to an individual who requested disclosure but who is not the subject of the records). This construction, while sensible as a policy matter, appears to conflict with the actual wording of subsection (b)(8), although the wording of this provision is not precise.

9. 5 U.S.C. § 552a(b)(9) - Congress

“No agency shall disclose any record which is contained in a system of records...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure would be—

...

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee.” 5 U.S.C. § 552a(b)(9).

Comment:

The congressional disclosure exception does not authorize the disclosure of a record to an individual Member of Congress acting on his or her own behalf, or on behalf of a constituent.

This exception allows for disclosure of records to Congress but does not authorize the disclosure of a Privacy Act-protected record to an individual Member of Congress acting on his or her own behalf or on behalf of a constituent. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,955, https://www.justice.gov/paoverview_omb-75; OMB Supplementary Guidance, 40 Fed. Reg. at 56,742, https://www.justice.gov/paoverview_omb-75-sup; see also Swenson v. USPS, 890 F.2d 1075, 1077 (9th Cir. 1989)

(determining disclosure was improper when subject of records USPS disclosed to congressman did not request disclosure); Lee v. Dearment, No. 91-2175, 1992 WL 119855, at *2 (4th Cir. June 3, 1992); cf. Chang v. Navy, 314 F. Supp. 2d 35, 45-47 (D.D.C. 2004) (discussing subsection (b)(9) and parties' dispute as to whether disclosure was allowable because it involved committee inquiry or not allowable because it involved constituent inquiry, but ultimately finding disclosure was proper pursuant to routine use permitting disclosure to Members of Congress making inquiries on behalf of constituents). See generally U.S. Dep't of Justice, Off. of Info. Pol'y, OIP Guidance: Congressional Access Under FOIA, in FOIA Update, Vol. V, No. 1, at 3-4, http://www.justice.gov/oip/foia_updates/Vol_V_1/page3.htm (interpreting counterpart provision of FOIA). (interpreting counterpart provision of FOIA).

The Second Circuit has held that an agency may disclose records consistent with the congressional disclosure exception, even if the agency knew or reasonably should have known that the information would subsequently become public.

The Court of Appeals for the Second Circuit in Devine v. United States, held that the unsolicited disclosure of an Inspector General letter to a congressional subcommittee chairman and member fell "squarely within the ambit of § 552a(b)(9)," and rejected the appellant's argument that subsection (b)(9) should not apply if the government agency knew or should have known that the information would eventually be released to the public. 202 F.3d 547, 551-53 (2d Cir. 2000).

10. 5 U.S.C. § 552a(b)(10) - Government Accountability Office

"No agency shall disclose any record which is contained in a system of records...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure would be—

...

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the G[overnment] Account[ability] Office." 5 U.S.C. § 552a(b)(10).

11. 5 U.S.C. § 552a(b)(11) - Court Order

"No agency shall disclose any record which is contained in a system of records...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure

would be—

...

(11) pursuant to the order of a court of competent jurisdiction.” 5 U.S.C. § 552a(b)(11).

Comment:

The Privacy Act does not prohibit the disclosure of relevant records during discovery when disclosed consistent with the Privacy Act’s disclosure provision; agencies frequently utilize the court order disclosure exception during discovery.

Subsection (b)(11) permits a court of competent jurisdiction to order disclosure of Privacy Act protected information that would otherwise be prohibited from disclosure without prior written consent of the individual to whom the record pertains.

As a general proposition, the Privacy Act does not act as a shield against discovery of relevant records that are otherwise protected under the Privacy Act, and the records may become discoverable through litigation if ordered by a court. Laxalt v. McClatchy, 809 F.2d 885 (D.C. Cir. 1987). The essential point of this exception is that the Privacy Act “cannot be used to block the normal course of court proceedings, including court-ordered discovery.” Clavir v. United States, 84 F.R.D. 612, 614 (S.D.N.Y. 1979); see also, Garraway v. Ciufo, No. 1:17-cv-00533, 2020 WL 1263562 (E.D. Cal. Mar. 16, 2020); Dawson v. Great Lakes Edu. Loan Services, Inc., No. 15-cv-475-JDP, 2018 WL 9539117 (W.D. Wis. Nov. 29, 2018); Adams v. Sotelo, No. 3:16-cv-02161, 2018 WL 30199288, at *2 (S.D. Cal. June 18, 2018); Ayers v. Lee, No. 14cv542-BGS, 2017 WL 2472840, at *3 (S.D. Cal. Jun. 8, 2017); Tidwell v. Brennan, No. 1:14-cv-553, 2015 WL 40922771 (S.D. Ohio July 6, 2015); United States v. Revland, No. 5:06–HC–2212, 2011 WL 7665381, at *1 (E.D.N.C. Nov. 30, 2011); Vinzant v. United States, No. 2:06-cv-10561, 2010 WL 2674609, at *7 (E.D. La. June 30, 2010) (stating that where defendant agency objected to disclosing Privacy Act records requested in discovery, “the ‘court order exception’ to the Privacy Act will preclude any future liability for disclosure, thereby alleviating the government’s concern and nullifying its objection”); SEC v. Gowrish, No. 09-05883 SI, 2010 WL 1929498, at *2 (N.D. Cal. May 12, 2010); In re Katrina Canal Breaches Consol. Litig., No. 05-4182, 2007 WL 1959193, at *6 (E.D. La. June 27, 2007); Rogers v. England, 246 F.R.D. 1, 3 n.6 (D.D.C. Mar. 15, 2007); B & H Towing, No. 6:05-cv-00233, 2006 WL 1728044, at *5 (S.D. W. Va. June 23, 2006); Martin v. United States, 1 Cl. Ct. 775, 780-82 (Cl. Ct. Mar. 17, 1983).

The court order disclosure exception does not, itself, confer federal jurisdiction or create a right of action to obtain a court order.

Nor does this exception confer federal jurisdiction or create a right of action to obtain a court order for the disclosure of records. See Sheetz v. Marti, No. 10-10844, 2010 WL 2034775, at *1 (D. Mass. May 19, 2010) (stating that “in the absence of federal question jurisdiction . . . , diversity jurisdiction . . . , or some other statutory grant of jurisdiction, this court lacks authority to issue a subpoena” against federal agency for records plaintiff sought in connection with his divorce proceedings); Haydon Bros. Contracting, Inc. v. SSA, No. 7:11-96, 2012 WL 38608, at *2-4 (E.D. Ky. Jan. 9, 2012) (stating that where plaintiff was seeking (b)(11) order to require agency to disclose third party’s records, “the Privacy Act permits disclosure of an individual’s records pursuant to a court order, it does not provide expressly for a private right of action to obtain such an order,” and “implying a civil remedy. . . is not consistent with the legislative scheme of the Privacy Act.”); see also Bryant v. SSA, No. 14CV5764, 2015 WL 6758094, at *4 (S.D.N.Y. Nov. 5, 2015).

Relevant case law focuses on two aspects of the court order disclosure exception: what constitutes an “order of a court,” and what constitutes a court of “competent jurisdiction.”

This (b)(11) court order exception – like the subsection (b)(3) routine use exception – has generated a great deal of uncertainty due to its lack of guidance on what constitutes an “order of a court” and a “court of competent jurisdiction.” Unfortunately, neither the Act’s legislative history nor the OMB 1975 Guidelines shed light on either of these meanings or illuminate whether there are specific requirements one must meet to rely on this exception. The relevant case law below provides guidance on both prongs of this exception, however: 1) the meaning of “order of a court” and 2) when a court has “competent jurisdiction.” See 120 Cong. Rec. at 36,959, reprinted in Source Book at 936, https://www.justice.gov/opcl/paoverview_sourcebook; OMB 1975 Guidelines, 40 Fed. Reg. at 28,955, https://www.justice.gov/paoverview_omb-75.

a. Meaning of “Court Order”

i. Judge Approved

Courts have generally interpreted the court order disclosure exception to require the “order of a court” to be specifically approved by a judge.

To constitute a court order under subsection (b)(11), a judge must approve the order. In Doe v. DiGenova, 779 F.2d 74, 77-85 (D.C. Cir. 1985), the D.C. Circuit decisively ruled that a subpoena routinely issued by a court clerk – such as a federal grand jury subpoena – is not a “court order” within the meaning of this exception because it is not “specifically approved” by a judge. Cf. Ricoma v. Standard Fire Ins. Co., No. 5:12-CV-18, 2013 WL 1164499, at *1 n.2 (E.D.N.C. Mar. 20, 2013) (finding proposed subpoena deficient on other grounds and discussing request for subpoena to be signed by judge in accordance with subsection (b)(11)); Hoffman v. Astrue, No. 3:10-CV-00214, 2011 WL 195617, at *4 (W.D. Ky. Jan. 18, 2011) (ruling that agency need not comply with state court subpoena to disclose records because all 12 exceptions under Privacy Act are “inapposite”).

Prior to Doe v. DiGenova, the courts were split on this point. Compare Bruce v. United States, 621 F.2d 914, 916 (8th Cir. 1980) (dictum) (finding subpoena is not court order), and Stiles v. Atlanta Gas Light Co., 453 F. Supp. 798, 800 (N.D. Ga. 1978) (finding that Privacy Act will prevent disclosure of subpoenaed documents unless “the court specifically orders them produced pursuant to section 552a(b)(11)”), with Adams v. United States Lines, No. 80-0952, slip op. at 2-3 (E.D. La. Mar. 16, 1981) (finding subpoena is court order). Cf. Moore v. USPS, 609 F. Supp. 681, 682 (E.D.N.Y. 1985) (finding subpoena is court order where it is required to be approved by judge under state law).

Note that an agency cannot avoid the result in Doe v. DiGenova by relying on a routine use that seeks to authorize disclosure pursuant to a subpoena. See Doe v. Stephens, 851 F.2d 1457, 1465-67 (D.C. Cir. 1988) (discussed in detail above under exception, “5 U.S.C. 552a(b)(3) - Routine Uses”).

ii. Standards for Issuance of a Court Order

Because the Privacy Act’s court order disclosure exception contains no standard that governs the issuance of a court order, courts have relied on a number of considerations, with varying degrees of clarity.

Under the Privacy Act’s subsection (b)(11) exception, there is no standard governing the issuance of a “court order.” Unlike other federal privacy-related or confidentiality statutes, subsection (b)(11) contains no standard governing the issuance of an order authorizing the disclosure of otherwise protected Privacy Act information. *See, e.g.*, 42 U.S.C. § 290dd-2 (2018) (listing “good cause” factors to be weighed by court in evaluating applications for orders permitting disclosure of records pertaining to substance abuse); 20 U.S.C. § 1232g(b)(2)(B) (prohibiting disclosure unless, inter alia, “information is furnished in compliance with a judicial order, or pursuant to any lawfully issued subpoena, upon condition that parents and the students are notified of all such orders or subpoenas in advance of the compliance therewith by the educational institution or agency”).

However, there are a number of considerations that the courts have used, with varying degrees of clarity, to assess whether a “court order” was issued. These considerations include:

a) Qualified Discovery Privilege

The Privacy Act does not create heightened discovery requirements.

Some courts have held, for example, that because the Privacy Act does not itself create a qualified discovery “privilege,” a showing of “need” is not a prerequisite to initiating discovery of protected records. *See Laxalt v. McClatchy*, 809 F.2d 885, 888-90 (D.C. Cir. 1987); *see also Weahkee v. Norton*, 621 F.2d 1080, 1082 (10th Cir. 1980) (noting that objection to discovery of protected records “does not state a claim of privilege”); *CFPB v. Navient Corp.*, No. 3:17-CV-101, 2018 WL 3824367 (M.D. Pa. Aug. 10, 2018) (agreeing “with the numerous courts that have found that the Privacy Act does not create a qualified discovery privilege”); *Bowden-Walker v. Wal-Mart*, No. 3:14-cv-917, 2015 WL 13450672 (S.D. Miss. July 22, 2015); *Ala. & Gulf Coast Ry., LLC v. United States*, No. CA 10-0352, 2011 WL 1838882, at *3-5 (S.D. Ala. May 13, 2011) (citing *Laxalt* in determining relevance of personnel files); *Bosaw v. NTEU*, 887 F.

Supp. 1199, 1215-17 (S.D. Ind. 1995) (citing Laxalt with approval, although ultimately determining that court did not have jurisdiction to rule on merits of case); Ford Motor Co. v. United States, 825 F. Supp. 1081, 1083 (Ct. Int'l Trade 1993) (“[T]he Privacy Act does not establish a qualified discovery privilege that requires a party seeking disclosure under 5 U.S.C. § 552a(b)(11) to prove that its need for the information outweighs the privacy interest of the individual to whom the information relates.”); Clavir v. United States, 84 F.R.D. 612, 614 (“[It] has never been suggested that the Privacy Act was intended to serve as a limiting amendment to . . . the Federal Rules of Civil Procedure.”); cf. Baldrige v. Shapiro, 455 U.S. 345, 360-62 (1981) (holding that Census Act constitutes statutorily created discovery “privilege” because it precludes all disclosure of raw census data despite need demonstrated by litigant).

b) Relevance

The D.C. Circuit has held that the only test for discovery of records is a “relevance” standard, in accordance with the Federal Rules of Civil Procedure.

The D.C. Circuit’s decision in Laxalt v. McClatchy establishes that the only test for discovery of Privacy Act-protected records is “relevance” under Rule 26(b)(1) of the Federal Rules of Civil Procedure. 809 F.2d at 888-90; *see also, e.g., Pa. v. Navient Corp.*, 348 F. Supp. 3d 394, 398 (M.D. Pa. 2018) (ordering production of all disputed records and requiring parties to resolve potential burden, scope and relevancy issues related to production of records); Ali v. Gilead Science, Inc., No. 18-cv-00677, 2018 WL 3629818, at *2 (N.D. Cal. July 31, 2018) (citing Laxalt and noting that “the Privacy Act does not protect information from disclosure in litigation pursuant to a valid discovery request”); Ali v. eBay, Inc., No. 17-cv-06589, 2018 WL 3368389 (N.D. Cal. July 10, 2018); Needham & Co., LLC, No. 15 Civ. 2487, 2017 WL 2779800, at *1 (S.D.N.Y. June 6, 2017); Meyer v. United States, No. 16-2411, 2017 WL 735750, at *4 (D. Kan. Feb. 24, 2017) (citing Laxalt and noting that requested information “is not only relevant to this action, it is potentially essential” and thereby, required to be disclosed, but parties were encouraged to address further privacy issues through protective order); Jackson v. Safeco Insurance Co. of Ill., No. CV 14-162, 2014 WL 12658918 (D. Mont. Dec. 19, 2014); Riascos-Hurtado v. United States, No. 09-CV-0003, 2011 U.S. Dist. LEXIS 28008, at *1 (E.D.N.Y. Mar. 17, 2011)

(citing Laxalt and granting plaintiff's motion to compel production of background investigation of former agency employee, which was "relevant to the action and may be relied upon by Plaintiffs in opposing the Government's motion" to dismiss); Buechel v. United States, No. 08-132, 2010 WL 3310243, at *1 (S.D. Ill. Aug. 19, 2010); R.T. Vanderbilt Co. v. United States, No. 95-283, 2010 WL 2706282, at *6 (Fed. Cl. July 8, 2010); SEC v. Gowrish, No. C 09-05883, 2010 WL 1929498, at *2 (N.D. Cal. May 12, 2010); Stiward v. United States, No. 05-1926, 2007 WL 2417382, at *1 (E.D. La. Aug. 24, 2007); Ezell v. Potter, No. 2:01 CV 637, 2006 WL 1094558, at *2 (N.D. Ind. Mar. 16, 2006); Hassan v. United States, No. C05-1066C, 2006 WL 681038, at *2 (W.D. Wash. Mar. 15, 2006); Snyder v. United States, No. 02-0976, 2003 WL 21088123, at *2-3 (E.D. La. May 12, 2003); Lynn v. Radford, No. 99-71007, 2001 WL 514360, at *3 (E.D. Mich. Mar. 16, 2001); Anderson v. Cornejo, No. 97 C 7556, 2001 WL 219639, at *3 (N.D. Ill. Mar. 6, 2001); Hernandez v. United States, No. 97-3367, 1998 WL 230200, at *2-3 (E.D. La. May 6, 1998); Forrest v. United States, No. 95-3889, 1996 WL 171539, at *2 (E.D. Pa. Apr. 11, 1996); Bosaw, 887 F. Supp. at 1216-17 (citing Laxalt with approval, although ultimately determining that court did not have jurisdiction to rule on merits of case); Ford Motor Co., 825 F. Supp. at 1083-84; Mary Imogene Bassett Hosp. v. Sullivan, 136 F.R.D. 42, 49 (N.D.N.Y. 1991); O'Neill v. Engels, 125 F.R.D. 518, 520 (S.D. Fla. 1989); Broderick v. Shad, 117 F.R.D. 306, 312 (D.D.C. 1987); In re Grand Jury Subpoenas Issued to USPS, 535 F. Supp. 31, 33 (E.D. Tenn. 1981); Christy v. United States, 68 F.R.D. 375, 378 (N.D. Tex. 1975).

c) Balancing Need for Information and Potential Harm

Other courts have assessed court orders by balancing the potential harm to the affected party from disclosure without restrictions and the requesting party's need for the record.

Courts have also assessed whether orders should be granted by balancing the potential harm to the affected party from disclosure without restrictions and the need of the requesting party for the particular information. See Perry v. State Farm Fire & Cas. Co., 734 F.2d 1441, 1447 (11th Cir. 1984) (asserting that requests for court orders "should be evaluated by balancing the need for the disclosure against the potential harm to the subject of the disclosure"); Pearlstein v. BlackBerry Ltd., No. 19-mc-91091, 2019 WL 6117145 (D. Mass. Nov. 18, 2019) (concluding that compelling disclosure without

notice, and without consideration of privacy interests of named individuals, ran afoul of privacy interests of individuals in nondisclosure of documents); Romeo v. Israel, No. 13-CV-61411, 2016 WL 3646858, at *2-6 (S.D. Fla. June 28, 2016) (balancing need for disclosure of information with potential harm to subjects of disclosure and determining that information was relevant, but in order to protect interests of individuals in case, documents would be reviewed in camera and only produced what is relevant to matter); Abidor v. Johnson, No. 10-CV-4059, 2016 WL 3102017, at *7 (E.D. N.Y. June 2, 2016); Verrill v. Battelle Energy All., No. 4:12-cv-00628, 2013 WL 5816632, at *2 (D. Idaho Oct. 28, 2013) (finding that either standard of “relevancy” or standard “balancing the need for the disclosure against the potential harm to the subject of the disclosure” was met and that harm to third-parties is limited since request is “narrowly circumscribed to involve only their performance reviews and documents pertaining to any investigation surrounding their termination” and that protective order would ensure confidentiality of information); Hall v. Hous. Auth. of Cnty. of Marin, No. 12-04922, 2013 WL 5695813, at *3 (N.D. Cal. Oct. 18, 2013) (finding that plaintiffs’ need for information to support claim seeking relief under 42 U.S.C. § 1983 for alleged violations of the U.S. Housing Act “outweighs any privacy interests, especially in light of the Protective Order and other steps, such as redaction, that can be taken to reduce privacy concerns”); Gutierrez v. Benavides, 292 F.R.D. 401, 404-06 (S.D. Tex. 2013) (finding that “in determining whether to grant a protective order, the court must balance the requesting party’s need for the information against the injury that might result if uncontrolled disclosure is compelled” and “[t]hrough this balancing process, courts should afford due weight to the affected party’s privacy interest”; and determining that personnel records of federal employees other than “records indicating official misconduct, abuse of power, or constitutional violations’ are to be protected from public disclosure”); Am. Modern Select Ins. Co. v. Sutherland, No. CV-12-S-1681, 2013 WL 1767827, at *2-3 (N.D. Ala. Apr. 18, 2013) (granting limited order for production of documents as plaintiff, an insurance company, “had a clear need for some of the documents in order to properly develop its arson defense,” which outweighed any potential harm to defendant, especially considering limited scope of order); United States v. Meyer, No. 2:11-cr-43, 2011 U.S. Dist. LEXIS 94270, at *1 (M.D. Fla. Aug. 23, 2011) (granting order after “balanc[ing] the need for disclosure against the potential harm from disclosure”); In re Becker v. Becker, No. 09-70173, 2010

WL 3119903, at *4 (Bnkr. W.D. Tex. Aug. 6, 2010) (ruling that although court was “authorized to order discovery of confidential records, it must balance the public interest in avoiding harm from disclosure against the benefits of providing relevant evidence”); Newman, No. 81-2480, slip op. at 3 (D.D.C. Sept. 13, 1982) (evaluating “legitimacy” of discovery requests and “need” for records as factors governing issuance of court order); cf. Hounshel v. Battelle Energy Alliance, LLC, No. 4:11-CV-00635, 2013 WL 5375833, at *2 (D. Idaho Sept. 24, 2013) (finding that “[r]esolution of a privacy objection requires a balancing of the need for the information sought against the privacy right asserted” and granting limited order allowing plaintiff access to third-party mental health records of employees of defendant); Ibrahim v. DHS, No. 06-00545, 2013 WL 1703367, at 6 (N.D. Cal. Apr. 19, 2013) (ordering disclosure under protective order and stating that “government may redact documents only to remove information relating to third parties who are private individuals and who are unrelated to plaintiff and her claims (relating to her challenge of being placed on government watch lists”). But cf. FDK Am., Inc. v. United States, 973 F. Supp. 2d 1315, 1318 (Ct. Int’l Trade Apr. 4, 2014) (holding motion for protective order in abeyance pending plaintiff’s certification of identity of third party who had control of documents plaintiff sought; subsequent determination of whether third-party provides consent, or was located outside territorial jurisdiction of the court).

iii. Limiting Discovery with Protective Order

Courts have held that a protective order limiting discovery under the Federal Rules of Civil Procedure is a proper procedural device for protecting records under the court order disclosure exception.

It is important to note that a protective order limiting discovery under Rule 26(c) of the Federal Rules of Civil Procedure (based, if appropriate, upon a court’s careful in-camera inspection) is a proper procedural device for protecting particularly sensitive Privacy Act-protected records when subsection (b)(11) court orders are sought. See Laxalt, 809 F.2d at 889-90; see also, e.g., Noble v. City of Fresno, No. 116CV01690DADBAM, 2017 WL 5665850, at *5 (E.D. Cal. Nov. 27, 2017) (stating that Defendant’s concerns could be assuaged by “tightly drawn” protective order specifying specific access and uses of information); Upstate Shredding, LLC v. Northeastern Ferrous, Inc., No. 3:12-CV-1015, 2016 WL 865299, at *16-17 (N.D.N.Y. Mar. 2, 2016)

(upholding protective order issued to protect Privacy Act information that was violated and awarding fees associated with filing motion to enforce protective order); Minshew v. Donley, No. 2:10-CV-01593, 2013 WL 12410940, at *2 (D. Nev. Mar. 19, 2013) (permitting “redaction of exhibits containing [p]laintiff’s personal identification including her address and social security number” in documents that were to be unsealed because “public interest in such information is outweighed by the privacy concerns in revealing information”); SEC v. Kovzan, No. 11-2017, 2013 WL 647300, at *5 (D. Kan. Feb. 21, 2013) (noting that Privacy Act was not intended to limit Federal Rules of Civil Procedure and stating “this court typically approves protective orders directing the release of information coming within the protections of the Privacy Act”); Nguyen v. Winter, 756 F. Supp. 2d 128, 129 (D.D.C. 2010) (stating that “[p]ersonnel files cannot be produced without a Privacy Act protective order”); Buechel v. United States, 2010 WL 3310243, at *3-4 (S.D. Ill. Aug. 19, 2010) (issuing protective order to address defendant’s concern that “institutional safety militates against disclosure of information regarding exposure to MRSA within [Federal correctional institution]”); SEC v. Gowrish, 2010 WL 1929498, at *3 (ordering production of Privacy Act-protected documents, but fashioning protective order permitting redaction of information which if disclosed “may compromise any ongoing, unrelated criminal investigation,” while simultaneously requiring submission of unredacted copies for in-camera review); United States v. Chromatex, Inc., No. 91-1501, 2010 WL 2696759, at *10 (M.D. Pa. July 6, 2010) (ordering disclosure in camera to “allow the court to determine whether a protected order pursuant to the Privacy Act may properly be issued”); Sattar v. Gonzales, No. 07-cv-02698, 2009 WL 2207691, at *1-2 (D. Colo. July 20, 2009) (granting defendants’ motion for protective order where plaintiff sought discovery of documents that defendants claimed were protected by Act); Lopez v. Chula Vista Police Dep’t, No. 07 CV 01272, 2008 WL 8178681, at *1 (S.D. Cal. Oct. 21, 2008) (issuing (b)(11) protective order to govern disclosure of Privacy Act records concerning ongoing investigations that may reveal confidential informant and investigatory techniques and methods); In re Katrina Canal Breaches Consol. Litig., No. 05-4182, 2007 WL 1959193, at *6 (E.D. La. June 27, 2007) (ordering that subsection (b)(11) of Privacy Act allowed disclosure of materials containing “sensitive personal information” as long as they were designated as confidential pursuant to “Master Protective Order”); Boudreaux v. United States, No. 97-1592, 1999 WL 499911, at *1-2 (E.D. La. July 14, 1999) (recognizing relevancy of subsection (b)(11) to court’s resolution of dispute over motion to compel responses to production of

documents subject to Privacy Act, but ordering in-camera review of documents so that legitimacy of agency objections may be determined “in the considered and cautious manner contemplated by the Privacy Act”); Gary v. United States, No. 3:97-cv-658, 1998 WL 834853, at *4 (E.D. Tenn. Sept. 4, 1998) (finding that while third party’s personnel file may contain relevant information, disclosure of that file must be made pursuant to protective order); Bosaw, 887 F. Supp. at 1216-17 (citing Laxalt with approval, although ultimately determining that court did not have jurisdiction to rule on merits of case); Clymer v. Grzegorek, 515 F. Supp. 938, 942 (E.D. Va. 1981); cf. Brown v. Narvais, No. CIV-06-228-F, 2009 WL 2230774, at *3 (W.D. Okla. July 22, 2009) (recommending that parties agree to protective order to protect privacy interests of subject of information where plaintiff served subpoena on BOP seeking disclosure of Privacy Act-protected information); Forrest, 1996 WL 171539, at *2-3 (ordering parties to “explore the possibility of entering into a voluntary confidentiality agreement regarding protecting the privacy interests of those individuals affected by disclosure”); Loma Linda Cmty. Hosp. v. Shalala, 907 F. Supp. 1399, 1405 (C.D. Cal. 1995) (“Even if release of the data . . . had unexpectedly included information not already known to [the recipient], a confidentiality order could have been imposed to protect the privacy interests in issue.”); Williams v. McCausland, No. 90 Civ. 7563, 1992 WL 309826, at *3-4 (S.D.N.Y. Oct. 15, 1992) (directing parties to agree on and execute appropriate protective stipulation for information sought in discovery that, under Privacy Act’s subsection (b)(2) standard, would not be required to be disclosed under FOIA). But cf. Jacobs v. Schiffer, 204 F.3d 259, 264-66 & n.5 (D.C. Cir. 2000) (recognizing superiority of First Amendment rights and observing that there is “critical distinction between disclosures in the attorney-client context and public disclosures,” and pointing to attorney’s “willingness to enter into a protective order” as relevant to balancing of “the employee’s interests in communication with the government’s interests in preventing communication” where information that employee wished to disclose to his private attorney was covered by Privacy Act).

In some instances, it even may be appropriate for a court to entirely deny discovery. See, e.g., Farnsworth v. Proctor & Gamble Co., 758 F.2d 1545, 1546-48 (11th Cir. 1985) (affirming lower court’s holding that keeping study participants’ names private outweighs appellant’s discovery interests); In re Becker, 2010 WL 3119903, at *4 (noting that hardship to defendants’ privacy rights would be severe where plaintiff failed to establish relevance for requested disclosure); Weems v. Corr.

Corp. of Am., No. CIV-09-443, 2010 WL 2640114, at *2 (E.D. Okla. June 30, 2010); Oslund v. United States, 125 F.R.D. 110, 114-15 (D. Minn. 1989); cf. Padberg v. McGrath-McKenchnie, No. 00-3355, 2007 WL 2295402, at *2 (E.D.N.Y. Aug. 9, 2007) (declining to decide “whether a court may ever order a government agency to disclose social security numbers despite the provisions of [the Social Security Act],” and refusing to order disclosure of social security numbers of class members who have not submitted claim forms pursuant to settlement agreement); Barnett v. Dillon, 890 F. Supp. 83, 88 (N.D.N.Y. 1995) (declining to order disclosure of FBI investigative records protected by Privacy Act to arrestees despite their assertion that records were essential to proper prosecution and presentment of claims in their civil rights lawsuit).

In Redland Soccer Club, Inc. v. Army, No. 1:CV-90-1072, slip op. 1-3 & accompanying order (M.D. Pa. Jan. 14, 1991), aff’d, rev’d & remanded, on other grounds, 55 F.3d 827 (3d Cir. 1995), the district court, recognizing the “defendants’ initial reluctance to respond to plaintiffs’ [discovery] requests without a specific order of court [as] a reasonable precaution in light of the terms of the Privacy Act,” solved the dilemma by ordering the Army to respond to “all properly framed discovery requests in th[e] proceeding” and that to deem responses “made pursuant to an order of court.” Id.; see also Long Island Sav. Bank v. United States, 63 Fed. Cl. 157, 159-160 (Fed. Cl. 2004) (concluding that “[t]he exception in the Privacy Act for actions taken under court order is satisfied here” because scheduling order “specifically incorporated [a provision of the local rules]” requiring parties to exchange “witness lists containing the addresses and telephone numbers of each witness”).

iv. Court Orders for Publicly Filing Protected Records with Courts

Agencies may affirmatively disclose Privacy Act-protected records during litigation, so long as the disclosure is made in accordance with the Privacy Act’s disclosure provision.

As noted above, the Act’s legislative history indicates that a court is not a “person” or “agency” within the meaning of subsection (b), and that the Act was “not designed to interfere with access to information by the courts.” 120 Cong. Rec. at 36,967, reprinted in Source Book at 958-59, https://www.justice.gov/opcl/paoverview_sourcebook.

However, when an agency publicly files protected records with a court

during the course of litigation without consent of the subject of the records, by definition the disclosure constitutes a subsection (b) disclosure. See Laningham v. Navy, No. 83-3238, slip op. at 2-3 (D.D.C. Sept. 25, 1984), summary judgment granted (D.D.C. Jan. 7, 1985), aff'd per curiam, 813 F.2d 1236 (D.C. Cir. 1987) (concluding that because court had issued an order allowing the Navy to file documents, Navy had “grounds for believing its actions lawful” pursuant to section 552a(b)(11)). Thus, such public filing is proper only if it is undertaken pursuant to: (1) the subsection (b)(3) routine use exception (previously discussed), or (2) the subsection (b)(11) court order exception.

Where the routine use exception is unavailable, an agency should obtain a subsection (b)(11) court order permitting such public filing. Cf. DiGenova, 779 F.2d at 85 n.20 (“This is not to say that a prosecutor, a defendant, or a civil litigant, cannot submit an in camera ex parte application for a [subsection (b)(11)] court order.”). However, in light of Laningham, agencies should take care to apprise the court of the Privacy Act-related basis for seeking the order. In Laningham, the district court ruled that the government’s nonconsensual disclosure of plaintiff’s “disability evaluation” records to the United States Claims Court was improper – even though such records were filed only after the agency’s motion for leave to file “out of time” was granted. Id. The court held that subsection (b)(11) applies only when “for compelling reasons, the court specifically orders that a document be disclosed,” and it rejected the agency’s argument that the exception applies whenever records happen to be filed with leave of court. Id. at 4.

The Court of Veterans Appeals has issued a “standing order” that permits the Secretary of Veterans Affairs to routinely file relevant records from veterans’ case files.

One unique solution to the problem of filing Privacy Act-protected records in court is illustrated by In re A Motion for a Standing Order, in which the Court of Veterans Appeals issued a “standing order” permitting the Secretary of Veterans Affairs to routinely file relevant records from veterans’ case files in all future proceedings with that court. 1 Vet. App. 555, 558-59 (Ct. Vet. App. 1990) (per curiam); cf. Perkins v. United States, No. 99-3031, 2001 WL 194928, at *3 (D.D.C. Feb. 21, 2001) (order) (authorizing parties to seek admission into evidence at trial of any materials subject to the court’s stipulated protective order pursuant to subsection (b)(11)).

b. Meaning of “Competent Jurisdiction”

The D.C. Circuit has equated the term “competent jurisdiction” with “personal jurisdiction.”

One of the few Privacy Act decisions to mention this oft-overlooked “competent jurisdiction” requirement is Laxalt v. McClatchy, 809 F.2d at 890-91. In that case, the Court of Appeals for the District of Columbia Circuit appeared to equate the term “competent jurisdiction” with “personal jurisdiction” and noted that the requests for discovery of the nonparty agency’s records “were within the jurisdiction of the District Court for the District of Columbia” as “[n]either party contends that the District Court lacked personal jurisdiction over the FBI’s custodian of records.” Id.

Of course, where an agency is a proper party in a federal case, the district court’s personal jurisdiction over the agency presumably exists, and thus, court-ordered discovery of the agency’s records is proper under subsection (b)(11).

However, where a party seeks discovery of a nonparty agency’s records pursuant to a subpoena duces tecum issued under Rule 45 of the Federal Rules of Civil Procedure, Laxalt suggests that the district court issuing the discovery order must have personal jurisdiction over the nonparty agency in order to be regarded as a court of “competent jurisdiction” within the meaning of subsection (b)(11). See 809 F.2d at 890-91; cf. Mason v. S. Bend Cmty. Sch. Corp., 990 F. Supp. 1096, 1097-99 (N.D. Ind. 1997) (determining that SSA’s regulations “generally do not authorize the release of . . . records upon order of a court, even a federal court, in the absence of a special circumstance as defined by the statutes and regulations,” and thus, finding SSA not to be in contempt of court for failure to comply with prior order compelling SSA, a nonparty, to produce documents). But cf. Lohrenz v. Donnelly, 187 F.R.D. 1, 8-9 (D.D.C. 1999) (finding that nonparty agency made requisite showing of good cause for court to enter protective order without discussing jurisdiction over nonparty agency). The issue of whether personal jurisdiction exists in this situation is not always clear – particularly where the nonparty agency’s records are kept at a place beyond the territorial jurisdiction of the district court that issued the discovery order. Indeed, this very issue was apparently raised but not decided in Laxalt, 809 F.2d at 890-91 (finding it unnecessary to decide whether federal district court in Nevada would have had jurisdiction to order discovery of FBI records located in District of Columbia).

Some, but not all, courts have held that state courts lack “competent jurisdiction” when issuing state court orders for the disclosure of a nonparty federal agency’s records.

Likewise, the existence of “competent jurisdiction” is questionable whenever a state court orders the disclosure of a nonparty federal agency’s records because the doctrine of “sovereign immunity” will ordinarily preclude state court jurisdiction over a federal agency or official. See, e.g., Boron Oil Co. v. Downie, 873 F.2d 67, 70-71 (4th Cir. 1989) (holding state court subpoena constitutes “action” against United States and thus sovereign immunity applied even though EPA was not party in suit); Bosaw, 887 F. Supp. at 1210-17 (finding state court lacked jurisdiction to order federal officers to produce documents because government did not explicitly waive its sovereign immunity and, because federal court’s jurisdiction in this case was derivative of state court’s jurisdiction, federal court was likewise barred from ordering officers to produce documents); Sharon Lease Oil Co. v. FERC, 691 F. Supp. 381, 383-85 (D.D.C. 1988) (holding state court subpoena quashed as state court lacked jurisdiction to compel nonparty federal official to testify or produce documents absent waiver of sovereign immunity); see also Moore v. Armour Pharm. Co., 129 F.R.D. 551, 555 (N.D. Ga. 1990) (citing additional cases on point); cf. Louisiana v. Sparks, 978 F.2d 226, 235 n.15 (5th Cir. 1992) (noting that “[t]here is no indication that [subsection (b)(11)] evinces congressional intent to broadly waive the sovereign immunity of [federal] agencies . . . when ordered to comply with state court subpoenas”); Longtin v. DOJ, No. 06-1302, 2006 WL 2223999, at *2-3 (D.D.C. Aug. 3, 2006) (citing Sparks, rejecting plaintiff’s argument that subsection (b)(11) is a “sweeping waiver of sovereign immunity”, and concluding that “neither the Superior Court of the District of Columbia nor the Circuit Court for Prince George’s County, Maryland constitute[s] a ‘court of competent jurisdiction’ . . . to issue an order compelling a federal official to comply with a state court subpoena”).

Nevertheless, in Robinett v. State Farm Mut. Auto. Ins. Co., No. 02-0842, 2002 WL 31498992, at *3-4 (E.D. La. Nov. 7, 2002), aff’d per curiam, 83 F. App’x 638 (5th Cir. 2003), the district court looked to subsection (b)(11) and held that State Farm “properly obtained” an order from the state court for release of plaintiff’s medical records where “plaintiff’s medical condition was relevant to the litigation.” The court upheld the Department of Veterans Affairs’ “determination that plaintiff’s records were subject to release based on the court order.” In upholding the district court’s decision, the Court of Appeals for the Fifth Circuit

specifically stated that the medical records were “released pursuant to the exception for orders of a court of competent jurisdiction contained in 5 U.S.C. § 552a(b)(11).” 83 F. App’x at 639; see also Moore v. USPS, 609 F. Supp. 681, 682 (E.D.N.Y. 1985) (assuming without explanation that state court subpoena, required by state law to be approved by judge, constituted proper subsection (b)(11) court order; issue of “competent jurisdiction” was not addressed).

In addition, at least one state court has ruled that it has “competent jurisdiction” to issue a subsection (b)(11) court order permitting the disclosure of a Privacy Act-protected record. Tootle v. Seaboard Coast Line R.R., 468 So. 2d 237, 239 (Fla. Dist. Ct. App. 1984); cf. Saulter v. Mun. Court for the Oakland-Piedmont Judicial Dist., 142 Cal. App. 3d 266, 275 (Cal. Ct. App. 1977) (suggesting that state court can order state prosecutor to subpoena federal records for purpose of disclosing them to criminal defendant in discovery).

Agencies that construe state court orders as providing authority to disclose under subsection (b)(11) should be aware that compliance with such an order might be taken by a court as acquiescence to the court’s jurisdiction, notwithstanding applicable principles of sovereign immunity.

12. 5 U.S.C. § 552a(b)(12) - Debt Collection Act

“No agency shall disclose any record which is contained in a system of records...except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains, unless the disclosure would be—

...

(12) to a consumer reporting agency in accordance with section 3711(e) of Title 31.” 5 U.S.C. § 552a(b)(12).

Comment:

This disclosure exception was added to the original eleven exceptions by the Debt Collection Act of 1982. It authorizes agencies to disclose bad-debt information to credit bureaus. 31 U.S.C. § 3711(e)(9)(F). Before doing so, however, agencies must complete a series of due process steps designed to validate the debt and to offer the individual an opportunity to repay it. See OMB Debt Collection Guidance, 48 Fed. Reg. 1,556, https://www.justice.gov/paoverview_omb-83-dca.

ACCOUNTING OF CERTAIN DISCLOSURES

“Each agency, with respect to each system of records under its control, shall--

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of--

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.” 5 U.S.C. § 552a(c)(1)-(4).

Comment:

With the exception of the need to know disclosure and the required FOIA disclosure exceptions, agencies are required to keep accurate accountings of their record disclosures.

Section 552a(c) of the Privacy Act establishes requirements for agencies to follow when accounting for disclosures of records. Subsection (c)(1) explicitly excepts both intra-agency “need to know” disclosures and FOIA disclosures from its coverage. See, e.g., Clarkson v. IRS, 811 F.2d 1396, 1397-98 (11th Cir. 1987) (per curiam) (finding IRS’s internal disclosure of records to its criminal investigation units does not require accounting).

While agencies do not need to account for disclosures made within the agency, the agency must account for all disclosures made outside of the agency, including disclosures pursuant to routine uses and law enforcement agencies (even though the law enforcement agency may be exempt from disclosures to the subject individual). OMB Memorandum for Heads of Departments and Agencies, Attachment B –

Instructions for Complying with the President's Memorandum of May 14, 1998, "Privacy and Personal Information in Federal Records" B.2.d. (Jan. 7, 1999) [hereinafter OMB Memo 99-05], https://www.justice.gov/paoverview_omb-99-05; see Quinn v. Navy, No. 94-56067, 1995 WL 341513, at *1 (9th Cir. June 8, 1995) (finding that disclosure of records within the Navy was exempt from accounting requirements).

OMB guidelines state that an agency must be able to maintain an accurate and complete accounting of disclosures so as to be able to respond to an individual's request for access to that accounting of disclosures.

Additionally, OMB stated that "[w]hile an agency need not keep a running tabulation of every disclosure at the time it is made, the agency must be able to reconstruct an accurate and complete accounting of disclosures so as to be able to respond to requests in a timely fashion." OMB Memo 99-05, B.2.d., https://www.justice.gov/paoverview_omb-99-05; see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,956, https://www.justice.gov/paoverview_omb-75. Accounting of disclosures made outside of the agency is required "even when such disclosure is . . . with the written consent or at the request of the individual." OMB 1975 Guidelines, 40 Fed. Reg. at 28,955, https://www.justice.gov/paoverview_omb-75.

In at least one district court case, the court noted that the records themselves do not need to contain the required accounting information.

In one case, a district court noted that although an agency is required pursuant to 5 U.S.C. § 552a(c) to keep an accurate accounting of each disclosure, there is no requirement that the "disclosed records themselves contain 'the date, nature and purpose' of each disclosure." Sieverding v. DOJ, 693 F. Supp. 2d 93, 105-06 (D.D.C. 2010), summary affirmance granted, No. 13-5060, 2013 WL 6801184 (D.C. Cir. Dec. 11, 2013) (per curiam). The district court also stated that the accounting requirement only "requires agencies to keep accurate accountings of their disclosures of records; they need not account for conversations or personal visits." Id. at 106.

Individuals have a right of access to an accounting of disclosures similar to the access right provided by subsection (d)(1), but are exempt from accessing such an accounting: (1) documenting law enforcement request disclosures under subsection (b)(7); and (2) subject to the Privacy Act exemption provisions, pursuant to subsection (j) or subsection (k).

It is important to recognize that subsection (c)(3) grants individuals a right of access to the accounting of disclosures similar to the access right provided by subsection (d)(1). See Standley v. DOJ, 835 F.2d 216, 219 (9th Cir. 1987) (entitling plaintiff to gain access to list, compiled by U.S. Attorney, of persons in IRS to whom disclosures of

grand jury materials about plaintiff were made); Ray v. DOJ, 558 F. Supp. 226, 228 (D.D.C. 1982) (requiring addresses of private persons who requested plaintiff's records to be released to plaintiff notwithstanding that "concern about possible harassment [sic] of these individuals may be legitimate"), aff'd, 720 F.2d 216 (D.C. Cir. 1983) (unpublished table decision); cf. Quinn, 1995 WL 341513, at *1 (finding no records to disclose in response to request for accounting because there were no disclosures that required accounting); Beaven v. DOJ, No. 03-84, 2007 WL 1032301, at *23 (E.D. Ky. Mar. 30, 2007) (finding accounting provisions not applicable for unauthorized disclosures because provisions only cover disclosures made under subsection (b)), aff'd in part & remanded in part on other grounds, 622 F.3d 540 (6th Cir. 2010).

However, subsection (c)(3) makes an explicit exception "for disclosures made under subsection (b)(7)." 5 U.S.C. § 552a(c)(3); see also Lora v. INS, No. 2:02cv756, 2002 WL 32488472, at *2 (E.D. Va. Oct. 8, 2002) (holding that plaintiff could not know whether AUSA had properly requested disclosed document from legacy INS because he was "not entitled to any accounting of disclosures" made under subsection (b)(7)) aff'd per curiam, 61 F. App'x 80 (4th Cir. 2003).

Of course, it should not be overlooked that certain Privacy Act exemptions – 5 U.S.C. § 552a(j) and (k) – are potentially available to shield an "accounting of disclosures" record from release to the subject thereof under subsection (c)(3). See Vazquez v. DOJ, 764 F. Supp. 2d 117, 120 (D.D.C. 2011) (ruling that "DOJ properly denied plaintiff's request under the Privacy Act on the basis that such records are" in a system "which the FBI has exempted" from the accounting provision pursuant to exemption (j)(2)); Zahedi v. DOJ, No. 10-694, 2011 WL 1872206, at *3 (D. Or. May 16, 2011) ("Plaintiff seeks an accounting of information obtained pursuant to a search warrant in the context of a criminal investigation, which falls squarely within the exemptions [(j)(2) and (k)(2)] to the Privacy Act's accounting provision."); Standley, 835 F.2d at 219 (remanding case for consideration of whether exemptions under 5 U.S.C. § 552a(j) and (k) are applicable); Hornes v. EOUSA, No. 04-2190, 2006 WL 792680, at *4 (D.D.C. Sept. 27, 2006) (finding, pursuant to exemption (j)(2), that "EOUSA has specifically exempted its system of 'Criminal Case Files' from the disclosure requirements of subsection (c)(3)"); Maydak v. DOJ, 254 F. Supp. 2d 23, 34-35 (D.D.C. 2003) (asserting that although agency's "conten[tion] that it 'is exempt from [the accounting provision] with respect to logs of disclosure' . . . is incorrect," and that "[e]xemption from the accounting requirement of § 552a(c) is not as expansive as seemingly being suggested by [the agency]," nevertheless finding that plaintiff failed to state claim and had no right of access where system was exempt from provisions of subsection (c)(3) pursuant to subsection (j)); Mittleman v. Treasury, 919 F. Supp. 461, 469 (D.D.C. 1995) (finding that "application of exemption (k)(2) . . . is valid" and that Department of the Treasury OIG's General Allegations

and Investigative Records System is exempt “because, inter alia, application of the accounting-of-disclosures provision . . . would alert the subject to the existence of an investigation, possibly resulting in hindrance of an investigation”), aff’d in part & remanded in part on other grounds, 104 F.3d 410 (D.C. Cir. 1997); Bagley v. FBI, No. 88-4075, slip op. at 2-4 (N.D. Iowa Aug. 28, 1989) (applying subsection (j)(2)); see also Hart v. FBI, No. 94 C 6010, 1995 WL 170001, at *2 n.1 (N.D. Ill. Apr. 7, 1995) (noting exemption of FBI’s Criminal Justice Information Services Division Records System), aff’d, 91 F.3d 146 (7th Cir. 1996) (unpublished table decision).

For a further discussion of general accounting procedures and practices, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,955-56, <https://www.justice.gov/paoverview omb-75>.

A plaintiff may seek damages for an agency’s failure to maintain an accurate accounting of disclosures.

Finally, a plaintiff may seek damages for an agency’s failure to maintain adequate accounting of disclosures. See Sussman v. Marshals Serv., 734 F. Supp.2d 138, 149 (D.D.C. 2010) (stating that “[t]he core elements of the claim are (1) failure . . . to maintain an accurate accounting of disclosures, and (2) a resultant adverse effect.” (quoting Sussman v. Marshals Serv., 494 F.3d 1106, 1124 (D.C. Cir. 2007))). An individual can recover damages for accounting failures regarding disclosures “only to the extent those disclosures involved materials in his records.” 494 F.3d at 1124.

INDIVIDUAL'S RIGHT OF ACCESS

"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 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." 5 U.S.C. § 552a(d)(1).

A. The Privacy Act and the FOIA

Comment:

The Privacy Act and the FOIA are often read in tandem; The Privacy Act allows individuals to access records about themselves, while the FOIA allows the public to access government information.

The Privacy Act provides individuals with a means to access government records about themselves. The right of access under the Privacy Act is similar to that of the Freedom of Information Act (FOIA), and the statutes do overlap, but not entirely. Compare 5 U.S.C. § 552a(d)(1) with 5 U.S.C. § 522(a)(3)(A); see generally Greentree v. U.S. Customs Serv., 674 F.2d 74, 76 (D.C. Cir. 1982) ("While the Privacy Act was designed to provide individuals with more control over the gathering, dissemination, and accuracy of agency information about themselves, FOIA was intended to increase the public's access to governmental information."). The FOIA is entirely an access statute and "is often explained as a means for citizens to know 'what their Government is up to.'" NARA v. Favish, 541 U.S. 157, 171-72 (2004) (quoting DOJ v. Reporters Comm. for Freedom of the Press, 489 U.S. 749, 773 (1989)); see generally FOIA Guide, at 1, <https://www.justice.gov/oip/page/file/1248371> (FOIA provides that "any person has a right, enforceable in court, to obtain access to federal agency records" that are not subject to any of its exemptions or exclusions). By comparison, the Privacy Act permits only an "individual" to seek access to only his own "record," and only if that record is maintained by the agency within a "system of records" – i.e., is retrieved by that individual requester's name or personal identifier – subject to ten Privacy Act exemptions (see the discussion "Ten Exemptions," below). See Sussman v. Marshals Serv., 494 F.3d 1106, 1121 (D.C. Cir. 2007) (concluding that Privacy Act gives individuals "access only to their own records, not to all information pertaining to them that happens to be contained in a system of records"); see also Burton v. Wolf, 803 F. App'x 120, 122 (9th Cir. 2020) (finding that plaintiff was not entitled to records retrievable only

with identifying information of his estranged wife); Aguilar v. DEA, 334 F. Supp. 3d 130, 146 (D.D.C. 2018) (request for information about GPS contractor did not relate to plaintiff's own records and was not accessible under Privacy Act); Goldstein v. IRS, 279 F. Supp. 3d 170, 187 (D.D.C. 2017) ("Plaintiff's Privacy Act claim fails because the information that Plaintiff seeks ... is not 'about' him.").

Thus, the primary difference between the FOIA and the access provision of the Privacy Act is the scope of information accessible under each statute.

Agencies should consider individuals' access requests under both the Privacy Act and the FOIA.

Agencies should process an individuals' access requests for their own records maintained in system of records under both the Privacy Act and the FOIA, regardless of the statute(s) cited. See 5 U.S.C. § 552a(t)(1) and (2) (prohibiting reliance on FOIA exemptions to withhold under Privacy Act, and vice versa); H.R. Rep. No. 98-726, pt. 2, at 16-17 (1984), as reprinted in 984 U.S.C.A.N. 3741, 3790-91 (regarding amendment of Privacy Act in 1984 to include subsection (t)(2) and stating: Agencies that had made it a practice to treat a request made under either [the Privacy Act or the FOIA] as if the request had been made under both laws should continue to do so"); FOIA Update, Vol. VII, No. 1, at 6, http://www.justice.gov/oip/foia_updates/Vol_VII_1/page5.htm; see also Martin v. Office of Special Counsel, 819 F.2d 1181, 1184 (D.C. Cir. 1987) ("[A]ccess to records under [FOIA and Privacy Act] is available without regard to exemptions under the other."); Shapiro v. DEA, 762 F.2d 611, 612 (7th Cir. 1985) ("Congress intends that the courts construe the Privacy Act and the Freedom of Information Act separately and independently so that exemption from disclosure under the Privacy Act does not exempt disclosure under the Freedom of Information Act, and vice versa."); Murray v. Shulkin, 273 F. Supp. 3d 87, (D.D.C. 2017) ("[A]gencies routinely process requests for records under both statutes, consistent with the overarching goal of 'open government, and especially, accessibility of government records.'" (citations omitted)); Espinoza v. DOJ, 20 F. Supp. 3d 232, 244 (D.D.C. 2014) (finding that "the Privacy Act specifically exempts from its nondisclosure provisions documents that are otherwise required to be disclosed under the FOIA"); Menchu v. HHS, 965 F. Supp. 2d 1238, 1246-47 (D. Or. 2013) (finding that "[t]he application of § 552a(d), rather than § 552a(b)(2), and the underlying goal of the legislature to allow individuals broad access to their own records, supports the conclusion that § 552a(t) requires disclosure of the records sought when allowed under either the [FOIA] or the Privacy Act" in light of fact that plaintiff was requesting information about himself and not about third party); Sussman v. DOJ, No. 03-3618, 2006 WL 2850608, at *4 (E.D.N.Y. Sept. 30, 2006) ("[A]n exemption under the FOIA is not a

bar to release files under the Privacy Act and . . . a Privacy Act exemption is not to bar release of files under the FOIA.”); Brown v. DOJ, No. 02-2662, slip op. at 18 n.36 (D. Ala. June 21, 2005) (concluding that plaintiff’s request must be analyzed under both FOIA and Privacy Act because “access to documents under these statutes [is] dissimilar”); Bogan v. FBI, No. 04-C-532-C, 2005 WL 1367214, at *6 (W.D. Wis. June 7, 2005) (explaining that if records are requested under both FOIA and Privacy Act, requester can gain access to those records by showing that they were accessible under either statute); Harvey v. DOJ, No. 92-176-BLG, slip op. at 8 (D. Mont. Jan. 9, 1996) (“Even though information may be withheld under the [Privacy Act], the inquiry does not end. The agency should also process requests under the FOIA, since the agency may not rely upon an exemption under the [Privacy Act] to justify nondisclosure of records that would otherwise be accessible under the FOIA. 5 U.S.C. § 552a(t)(2).”), aff’d, 116 F.3d 484 (9th Cir. 1997) (unpublished table decision); cf. Wren v. Harris, 675 F.2d 1144, 1146 & n.5 (10th Cir. 1982) (per curiam) (construing pro se complaint to seek information under either Privacy Act or FOIA even though only FOIA was referenced by name); Gonzales & Gonzales Bonds & Ins. Agency, Inc. v. DHS, 913 F. Supp. 2d 865, 868 n.3 (N.D. Cal. 2012) (noting DHS’ error in responding to plaintiff’s FOIA requests under the Privacy Act, and stating that “the FOIA and the Privacy Act are distinct mechanisms for obtaining government information, and it is legal error to conflate them”); Skurrow v. DHS, 892 F. Supp. 2d 319, 330 (D.D.C. 2012) (rejecting “plaintiff’s argument that [information related to plaintiff being on the watch list] should be released because plaintiff has requested the information under the Privacy Act, in addition to FOIA” because provision in TSA’s [Sensitive Security Information (SSI)] regulation specifically states that “records containing SSI are not available for public inspection or copying, nor does TSA . . . release such records to persons without a need to know”); Hunsberger v. DOJ, No. 92-2587, slip op. at 2 n.2 (D.D.C. July 22, 1997) (exempting system of records, from which documents at issue were retrieved, pursuant to Privacy Act exemption (j)(2); “[c]onsequently, the records were processed for release under the FOIA”); Freeman v. DOJ, 822 F. Supp. 1064, 1066 (S.D.N.Y. 1993) (accepting agency’s rationale that “because documents releasable pursuant to FOIA may not be withheld as exempt under the Privacy Act,” it is proper for the agency not to distinguish between FOIA and Privacy Act requests when assigning numbers to establish the order of processing, and quoting Report of House Committee on Government Operations, H.R. Rep. No. 98-726, which was cited by the agency as “mandat[ing]” such practice); Pearson v. DEA, No. 84- 2740, slip op. at 2 (D.D.C. Jan. 31, 1986) (construing pro se complaint to seek information under either Privacy Act or FOIA even though only FOIA was referenced by name).

Unlike the FOIA, see 5 U.S.C. § 552(a)(6)(A), the Privacy Act does not give a

requester the right to administratively appeal any adverse determination that an agency makes on his or her access request. However, because agencies should process an individual's access request under both statutes – which includes processing the request through any administrative appeal – there is no practical effect of this distinction. See, e.g., 28 C.F.R. § 16.45 (2020) (explaining DOJ Privacy Act regulation regarding appeals from denials of requests for access to records).

B. FOIA/Privacy Act Interface Examples: Access

Suppose John Q. Citizen writes to Agency: "Please send to me all records that you have on me."

For purposes of this example, assume that the only responsive records are contained in a system of records retrieved by Mr. Citizen's own name or personal identifier. Thus, both the Privacy Act and the FOIA potentially apply to the records.

1. If No Privacy Act Exemption Applies

Result: Mr. Citizen should receive access to his Privacy Act records where Agency can invoke no Privacy Act exemption.

The Agency cannot rely upon a FOIA exemption alone to deny Mr. Citizen access to any of his records under the Privacy Act. See 5 U.S.C. § 552a(t)(1) (FOIA exemptions cannot defeat Privacy Act access); see also Martin v. Office of Special Counsel, 819 F.2d 1181, 1184 (D.C. Cir. 1987) ("If a FOIA exemption covers the documents, but a Privacy Act exemption does not, the documents must be released under the Privacy Act." (emphasis added)); Hoffman v. Brown, No. 1:96cv53-C, slip op. at 4 (W.D.N.C. Nov. 26, 1996) (agreeing with plaintiff that "no provision of the Privacy Act allows the government to withhold or redact records concerning [his] own personnel records" and ordering production of e-mail and other correspondence regarding plaintiff's employment), aff'd, 145 F.3d 1324 (4th Cir. 1998) (unpublished table decision); Viotti v. Air Force, 902 F. Supp. 1331, 1336-37 (D. Colo. 1995) ("If the records are accessible under the Privacy Act, the exemptions from disclosure in the FOIA are inapplicable."), aff'd, 153 F.3d 730 (10th Cir. 1998) (unpublished table decision).

In other words, a requester is entitled to the combined total of what both statutes provide. See Clarkson v. IRS, 678 F.2d 1368, 1376 (11th Cir. 1982); Wren v. Harris, 675 F.2d 1144, 1147 (10th Cir. 1982) (remanding to the

district court for consideration of the request under the Privacy Act where the court “analyzed the request for documents solely under the FOIA” and “made no attempt to decide whether the documents were discoverable under the” Privacy Act) (per curiam); Kearns v. Fed. Aviation Admin., 312 F. Supp. 3d 97, 106 (D.D.C. 2018) (concluding that although the interaction between FOIA and Privacy Act exemptions “sounds like a sphinxian riddle,” “[t]he interaction between the two statutes ... boils down to a rather straightforward edict: ‘Where a request for documents is made under both FOIA and the Privacy Act, the responding agency must demonstrate that the documents fall within some exemption under each Act.’” (quoting Barouch v. DOJ, 962 F. Supp. 2d 30, 66 (D.D.C. 2013))); Fagot v. FDIC, 584 F. Supp. 1168, 1173 (D.P.R. 1984) (“[A]ccess to information request [that] falls under both the FOIA and the Privacy Act... is entitled to the cumulative result of what both statutes provide.”), aff’d in part & rev’d in part, 760 F.2d 252 (1st Cir. 1985) (unpublished table decision); see also 120 Cong. Rec. 40,406 (1974), reprinted in Source Book at 861, https://www.justice.gov/opcl/paoverview_sourcebook.

2. If a Privacy Act Exemption Applies

Result: Where a Privacy Act exemption applies, Mr. Citizen is not entitled to obtain access to his records under the Privacy Act.

But he may still be able to obtain access to his records (or portions thereof) under the FOIA. See 5 U.S.C. § 552a(t)(2) (Privacy Act exemption(s) cannot defeat FOIA access); Martin, 819 F.2d at 1184 (“[I]f a Privacy Act exemption but not a FOIA exemption applies, the documents must be released under FOIA.”) (emphasis added); Savada v. DOD, 755 F. Supp. 6, 9 (D.D.C. 1991) (citing Martin and holding that agency must prove that document is exempt from release under both FOIA and Privacy Act); see also Ehlmann v. DHS, No. 4:12 CV 1392, 2013 WL 3724906, at *1 (E.D. Mo. July 15, 2013); Shapiro v. DEA, 762 F.2d 611, 612 (7th Cir. 1985); Riser v. State, No. 09-3273, 2010 WL 4284925, at *6 (S.D. Tex. Oct. 22, 2010) (explaining that even if Privacy Act applied to record, “that statute cannot be used to withhold any record ‘which is otherwise accessible to [an] individual’ under FOIA”); Miller v. United States, 630 F. Supp. 347, 348-49 (E.D.N.Y. 1986); Nunez v. DEA, 497 F. Supp. 209, 211 (S.D.N.Y. 1980). The outcome will depend upon FOIA exemption applicability.

3. If No Privacy Act Exemption and No FOIA Exemption Apply

Result: The information should be disclosed.

4. If Both Privacy Act and FOIA Exemptions Apply

Result: The record should be withheld, unless the agency, after careful consideration, decides to disclose the record to the first-party requester as a matter of administrative discretion. See Memorandum from Eric Holder, Attorney General, for Dept. of Justice Heads of Exec. Dept. & Agencies, The Freedom of Information Act (FOIA) (Mar. 19, 2009), https://www.justice.gov/paoverview_agfoia [hereinafter AG FOIA 2009] (encouraging agencies “to make discretionary disclosures of information” when they may legally do so).

But remember: When an individual requests access to his own record (i.e., a first-party request) that is maintained in a system of records, an agency must be able to invoke properly both a Privacy Act exemption and a FOIA exemption in order to withhold that record.

Rule: ALL PRIVACY ACT ACCESS REQUESTS SHOULD ALSO BE TREATED AS FOIA REQUESTS.

Note also that Mr. Citizen’s first-party request – because it is a FOIA request as well – additionally obligates Agency to search for any records on him that are not maintained in a Privacy Act system of records. With respect to those records, only the FOIA’s exemptions are relevant; the Privacy Act’s access provision and exemptions are entirely inapplicable to any records not maintained in a system of records.

C. Records Requests and Searches

The Privacy Act does not require agencies to create records that do not exist.

The Privacy Act – like the FOIA – only requires agencies to search for existing records; it does not require “an agency to create records that do not exist.” DeBold v. Stimson, 735 F.2d 1037, 1041 (7th Cir. 1984); Schoenman v. FBI, 764 F. Supp. 2d 40, 48 (D.D.C. 2011) (reiterating that “agencies are under no obligation to create or generate records in the course of discharging their obligations under FOIA and the Privacy Act”); Harter v. IRS, No. 02-00325, 2002 WL 31689533, at *5 (D. Haw. Oct. 16, 2002) (“the Privacy Act does not require that the IRS create records in response to individual requests”); but see May v. Air Force, 777 F.2d 1012, 1015-17 (5th Cir. 1985) (finding that (k)(7) exemption for protecting source’s identity is subject to “reasonable segregation requirement” that obligates agency to create and release typewritten version of handwritten evaluation forms so as

not to reveal identity of evaluator under exemption (k)(7)); cf. ACLU v. DHS, 738 F. Supp. 2d 93, 117 (D.D.C. 2010) (concluding in a FOIA case that disclosure was appropriate where DHS produced typed renditions rather than handwritten notes).

Individuals must specify the documents requested, and agencies need only search for records consistent with the request.

Individuals seeking documents pursuant to the Privacy Act must identify with sufficient specificity the documents requested. Manga v. Knox, No. CV ELH-17-1207, 2018 WL 3239483, at *12 (D. Md. July 3, 2018) (summarily dismissing a plaintiff's claim because "[a]bsent a description of the documents sought, as well as details of the refusal to turn over the requested information, it is impossible to determine if [plaintiff] has stated a viable claim." (quoting Carroll v. SSA, WDQ-11-3005, 2012 WL 1454858, at *2 (D. Md. Apr. 24, 2012); Fleischman v. Comm'r of Soc. Sec., No. 3:15-CV-897-J-PDB, 2016 WL 7474577, at *3 (M.D. Fla. Dec. 29, 2016) (plaintiff's Privacy Act claim was dismissed because he did "not allege the substance of his request for records with sufficient specificity to indicate whether his request was proper"); cf. Marshall v. Cuomo, 192 F.3d 473, 485 (4th Cir. 1999) (affirming dismissal of FOIA claim where plaintiff failed to identify specific documents requested).

The Privacy Act only requires agencies to conduct a search consistent with the scope of the request. Ewell v. DOJ, 153 F. Supp. 3d 294, 302-03 (D.D.C. 2016) (the Privacy Act "does not obligate an agency to conduct a search for *all* records relating to a requester where a requester has asked the agency only to look for certain records") (emphasis in original).

The Privacy Act, consistent with the FOIA, requires an agency to conduct an adequate and reasonable search for records.

The standard for determining the adequacy of a search pursuant to the Privacy Act "is essentially the same" as that under the FOIA, and where the government satisfied the requirements for a reasonable search under FOIA, it also satisfied the Privacy Act search requirements. Jackson v. GSA, 267 F. Supp. 3d 617, 624 (E.D. Pa. 2017), aff'd, 729 F. App'x 206 (3d Cir. 2018); Hillier v. CIA, No. CV 16-CV-1836, 2018 WL 4354947, at *5 (D.D.C. Sept. 12, 2018).

Under both the Privacy Act and FOIA, an agency must conduct an adequate and reasonable search for relevant records. For example, the Court of Appeals for the District of Columbia Circuit applied the FOIA standard to an access claim brought under the Privacy Act in Chambers v. Interior, 568 F.3d 998, 1003 (D.C.

Cir. 2009). “In a suit seeking agency documents – whether under the Privacy Act or FOIA – ‘[a]t the summary judgment stage, where the agency has the burden to show that it acted in accordance with the statute, the court may rely on a reasonably detailed affidavit, setting forth the search terms and the type of search performed, and averring that all files likely to contain responsive materials (if such records exist) were searched.’” Id. (quoting McCready v. Nicholson, 465 F.3d 1, 14 (D.C. Cir. 2006), which in turn quotes Valencia-Lucena v. Coast Guard, 180 F.3d 321, 326 (D.C. Cir. 1999), FOIA case addressing agency adequacy of search obligations); cf. New Orleans Workers’ Ctr. for Racial Justice v. ICE, 373 F. Supp. 3d 16, 35 (D.D.C. 2019) (discussing adequacy of search in FOIA context); Schulze v. FBI, No. 1:05-CV-0180, 2010 WL 2902518, at *15 (E.D. Cal. July 22, 2010) (“While the court is of the opinion that there exists some doubt that Congress intended that the Privacy Act provide civil remedies for an agency’s failure to adequately search its files, . . . [t]he court, in the interests of giving fullest consideration to Plaintiff’s claims, will follow Chambers and apply FOIA standards to Plaintiff’s failure to search claims to the extent those claims are asserted under the Privacy Act.”).

An agency’s search obligations “are dictated by whether the scope of the search is reasonably calculated to uncover all relevant documents.” Mobley v. CIA, 924 F. Supp. 2d 24, 44 (D.D.C. 2013) (internal quotation marks omitted), aff’d, 806 F.3d 568 (D.C. Cir. 2015); Lane v. Interior, 523 F.3d 1128 (9th Cir. 2008) (“The search need only be reasonable, and the government may demonstrate that it undertook an adequate search by producing ‘reasonably detailed, nonconclusory affidavits submitted in good faith’”) (citation omitted); cf. SAI v. TSA, 315 F. Supp. 3d 218, 243 (D.D.C. 2018) (failure to uncover records does not mean that the search was inadequate).

In Chambers, the D.C. Circuit addressed the question of “whether [the agency] intentionally destroyed the [record sought] after [plaintiff] requested access to it.” Chambers, 568 F.3d at 1000. The court reversed the district court’s grant of summary judgment to the agency, reasoning that the agency’s “search would not be adequate under the Privacy Act if [agency] officials, aware of Chambers’s document requests, deliberately destroyed her performance appraisal before completing the search in order to avoid providing the document to her . . . Such a search would not be ‘reasonably calculated to uncover all relevant documents’ – which is what the Privacy Act, like FOIA, requires.” Id. at 1005. In remanding the case back to the district court, the Court of Appeals noted that “should Chambers prevail on [her access claim], the available remedies may be limited given that additional searches at this late date would likely prove futile,” but went on to state that “nonetheless, she may be entitled at a minimum to ‘reasonable attorney fees and other litigation costs.’” Id. at 1008. On remand, the

district court concluded that it “need not reach” the question of whether the agency intentionally destroyed the record at issue because the plaintiff “failed to sustain her burden of proof” on the question of “whether the document in question ever existed.” Chambers v. Interior, No. 05-0380, 2010 WL 2293262, at *2-3 (D.D.C. May 28, 2010).

A reasonably detailed affidavit describing the Privacy Act search can be sufficient to establish that the search was adequate.

Agencies can generally establish that a search was adequate by submitting “a reasonably detailed affidavit, setting forth the search terms and the type of search performed, and averring that all files likely to contain responsive materials (if such records exist) were searched.” Chambers v. Interior, 568 F.3d at 1003 (internal citations omitted); see also Elgabrownny v. CIA, No. 17-CV-00066, 2019 WL 1440345, at *7-11 (D.D.C. Mar. 31, 2019) (discussing the adequacy of several FOIA and Privacy Act requests); Demoruelle v. VA, No. CV 16-00562 LEK-KSC, 2017 WL 2836989, at *6 (D. Haw. June 30, 2017) (finding that whether requested information actually exists is “immaterial to whether or not the VA’s search was adequate” where VA provided a “detailed explanation of the records that it searched, the VA employee(s) who performed the search, and the process that it used for the search”).

An affidavit describing a FOIA and Privacy Act search is “reasonably detailed” if it includes “the search terms and the type of search performed, and aver[s] that all files likely to contain responsive materials (if such records exist) were searched.” Sandoval v. DOJ, No. CV 16-1013 (ABJ), 2019 WL 316168, at *4 (D.D.C. Jan. 24, 2019) (quoting Oglesby v. Army, 920 F. 2d 57, 68 (D.C. Cir. 2010)). On the other hand, agency affidavits that “do not denote which files were searched, or by whom, do not reflect any systematic approach to document location, and do not provide information specific enough to enable [the requester] to challenge the procedures utilized” are insufficient to support summary judgment. Sandoval v. DOJ, 2019 WL 316168, at *4, (quoting Weisberg v. DOJ, 627 F.2d 365, 371 (D.C. Cir. 1980)); see also SAI v. TSA, 315 F. Supp. 3d at 246 (concluding that “without evidence regarding the temporal scope” of the agency’s search, it was “impossible to know whether the search was adequate” and summary judgment was not appropriate); Defs. of Wildlife v. Border Patrol, 623 F. Supp. 2d 83, 92 (D.D.C. 2009) (finding declaration deficient where it failed to detail types of files searched, filing methods, and search terms used).

Agencies have the burden of justifying the withholding of records, and courts review those decisions de novo.

The Privacy Act places the burden to justify withholding of records on the agency, and provides for de novo review of decisions to withhold records. See 5 U.S.C. § 552a(g)(3)(A); Louis v. Labor, 419 F.3d 970, 977 (9th Cir. 2005); Becker v. IRS, 34 F.3d 398, 408 n.26 (7th Cir. 1994); Doe v. United States, 821 F.2d 694, 697–98 (D.C. Cir. 1987) (en banc); Erwin v. State, 2013 WL 6452758, at *3 (N.D. Ill. Dec. 9, 2013) (finding that “agency bears the burden of establishing that the search was adequate ... [b]ecause of the ‘asymmetrical distribution of knowledge’” in FOIA and Privacy Act cases “where the agency alone possesses, reviews, discloses, and withholds the subject matter of the request” (quoting Judicial Watch, Inc. v. FDA, 449 F.3d 141, 146 (D.C. Cir. 2006))). Thus, no deference is due an agency’s determination of which records to disclose and which are exempt. Doe v. Chao, 540 U.S. 614, 618-19 (2004) (distinguishing de novo review from “any form of deferential review”).

For a discussion of the unique procedures involved in processing first-party requests for medical records, see the discussion below under “Agency Rules, 5 U.S.C. § 552a(f)(3) - Establish Procedures for Disclosure of Records to Individuals.” For additional information regarding document searches in the FOIA context, see generally FOIA Guide at 57-58, <https://www.justice.gov/oip/page/file/1199421/download#page=40>.

D. Third Party Interests

Courts have split over how to handle records that, if released under the Privacy Act, would violate a third party’s privacy interests.

A particularly troubling and unsettled problem under the Privacy Act arises where a file retrieved by the requester’s name or personal identifier contains information pertaining to a third party that, if released, would invade that third party’s privacy.

This problem arises only when a requester seeks access to a record contained in a non-law enforcement system of records – typically a personnel or background security investigative system – inasmuch as agencies are generally permitted to exempt the entirety of their criminal and civil law enforcement systems of records from the subsection (d)(1) access provision pursuant to 5 U.S.C. §§ 552a(j)(2) and (k)(2).

The problem stems from the fact that unlike the FOIA, see 5 U.S.C. § 552(b)(6),

(7)(C), the Privacy Act does not contain any exemption that protects a third party's privacy. Cf. 5 U.S.C. § 552a(k)(5) (protecting only confidential source-identifying information in background security investigative systems). The Privacy Act's access provision simply permits an individual to gain access to "his record or to any information pertaining to him" that is contained in a system of records and retrieved by his name or personal identifier. 5 U.S.C. § 552a(d)(1).

The courts of appeals that have squarely addressed this issue have reached different conclusions. Compare Voelker v. IRS, 646 F.2d 332, 333-35 (8th Cir. 1981), with Sussman v. Marshals Serv., 494 F.3d 1106, 1120-21 (D.C. Cir. 2007). In Voelker, the Eighth Circuit held that where the requested information – contained in a system of records and retrieved by the requester's name – is "about" that requester within the meaning of subsection (a)(4)'s definition of "record," all such information is subject to the subsection (d)(1) access provision. Voelker v. IRS, 646 F.2d at 334. In construing subsection (d)(1), the Eighth Circuit noted that there is "no justification for requiring that information in a requesting individual's record meet some separate 'pertaining to' standard before disclosure is authorized [and i]n any event, it defies logic 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." Id. Relying on the importance of the access provision to the enforcement of other provisions of the Privacy Act, and the lack of any provision in the exemption portion of the statute to protect a third party's privacy, the Eighth Circuit rejected the government's argument that subsection (b) prohibited disclosure to the requester of the information about a third party. Id. at 334-35. A careful reading of Voelker reveals that the Eighth Circuit appeared to equate the term "record" with "file" for subsection (d)(1) access purposes. Cf. Wren v. Harris, 675 F.2d 1144, 1146-47 (10th Cir. 1982) (per curiam) (concluding that district court improperly relied on FOIA Exemption 6 to withhold certain third-party information without considering whether under Privacy Act request was for access "to his (own) record or to any information pertaining to him," or for "records" contained in a "system of records," and whether they were exempt from disclosure under Privacy Act exemptions); Henke v. Commerce, No. 94-0189, 1996 WL 692020, at *4 (D.D.C. Aug. 19, 1994) (rejecting government's argument that information contained in one individual's record is exempt from disclosure requirements of Privacy Act simply because same information is also contained in another individual's records), aff'd on other grounds, 83 F.3d 1445 (D.C. Cir. 1996); Ray v. DOJ, 558 F. Supp. 226, 228 (D.D.C. 1982) (ruling that requester was entitled to access, under subsection (c)(3), to addresses of private persons who had requested information about him because no Privacy Act exemption justified withholding such information, notwithstanding that agency's "concern about possible harassment [sic] of these individuals may be legitimate"), aff'd, 720 F.2d

216 (D.C. Cir. 1983) (unpublished table decision).

Other courts, however, have found that certain information, although contained in a file or document retrieved by an individual's name, did not qualify as a Privacy Act record because it was not "about" that individual. For example, Voelker's rationale was rejected by DePlanche v. Califano, 549 F. Supp. 685, 693-98 (W.D. Mich. 1982), a case involving a father's request for access to a social security benefits file indexed and retrieved by his social security number that contained the address of his two minor children. In denying the father access to the children's address, the court reasoned that such third-party information, although contained in the father's file, was not "about" the father, and therefore by definition was not his "record" within the meaning of subsection (a)(4), nor was it information "pertaining" to him within the meaning of the subsection (d)(1) access provision. Id. at 694-96. In distinguishing Voelker, the court relied upon an array of facts suggesting that the father might harass or harm his children if their location were to be disclosed. Id. at 693, 696-98; see also Murray v. BOP, 741 F. Supp. 2d 156, 161 (D.D.C. 2010) (concluding that, although names of individuals who visited plaintiff in prison and dates and times of their visits "certainly pertain[] to him in a generic sense," and "include[] his name and identifying number . . . , the balance of the information requested pertains to the third party visitors personally; the information is not 'about' the plaintiff and therefore is not a 'record'"); Nolan v. DOJ, No. 89-A-2035, 1991 WL 36547, at *10 (D. Colo. Mar. 18, 1991) (holding names of FBI agents and other personnel were not requester's "record" and therefore "outside the scope of the [Privacy Act]"), aff'd, 973 F.2d 843 (10th Cir. 1992); Haddon v. Freeh, 31 F. Supp. 2d 16, 22 (D.D.C. 1998) (applying Nolan and Doe, infra, holding that identities and telephone extensions of FBI agents and personnel were not "about" plaintiff and thus were properly withheld); Springmann v. State, No. 93-1238, slip op. at 8 & n.1 (D.D.C. Apr. 21, 1997) (citing Nolan and holding that name of foreign official who provided information to State Department and names of foreign service officers (other than plaintiff) who were denied tenure were "not accessible to plaintiff under the Privacy Act because the identities of these individuals d[id] not constitute information 'about' plaintiff, and therefore [we]re not 'records' with respect to plaintiff under the Privacy Act"); Hunsberger v. CIA, No. 92-2186, slip op. at 3-4 (D.D.C. Apr. 5, 1995) (citing Nolan and holding that names of employees of private insurance company used by Director of Central Intelligence and Director's unique professional liability insurance certificate number maintained in litigation file created as result of plaintiff's prior suit against CIA Director were not "about" plaintiff and therefore were not "record[s]" within meaning of Privacy Act); Doe v. DOJ, 790 F. Supp. 17, 22 (D.D.C. 1992) (citing Nolan and alternatively holding that "names of agents involved in the investigation are properly protected from disclosure"); cf. Allard v. HHS, No.

4:90-CV- 156, slip op. at 9-11 (W.D. Mich. Feb. 14, 1992) (citing DePlanche, *supra*, with approval and arriving at same result, but conducting analysis solely under FOIA Exemption 6), aff'd, 972 F.2d 346 (6th Cir. 1992) (unpublished table decision).

The District Court for the District of Columbia was confronted with a more complex version of this issue of third-party information when the subject of a letter requested access to it and the agencies withheld it to protect the author's privacy interests. Topuridze v. USIA, 772 F. Supp. 662 (D.D.C. 1991), reconsidering Topuridze v. FBI, No. 86-3120, 1989 WL 11709 (D.D.C. Feb. 6, 1989). In Topuridze, the issue of access to third-party information in a requester's file was further complicated by the fact that the information was "retrievable" by both the requester's identifier and the third party's identifier, i.e., "dual retrieval." Topuridze v. FBI, No. 86-3120, 1989 WL 11709, at *1 (D.D.C. Feb. 6, 1989). In apparent contradiction to the subsection (d)(1) access provision, subsection (b) prohibits the nonconsensual disclosure of an individual's record contained in a system of records retrieved by his name or personal identifier to any third party. See 5 U.S.C. § 552a(b). Because the letter was both the requester's and the third party's Privacy Act record, the government argued that subsection (b), though technically not an "exemption," nevertheless restricts first-party access under subsection (d)(1) where the record is about both the requester and the third-party author, and is located in a system of records that is "retrievable" by both their names. See Topuridze v. FBI, No. 86-3120, 1989 WL 11709, at *1 (D.D.C. Feb. 6, 1989); Topuridze v. USIA, 772 F. Supp. at 665-66. Although the court had previously ruled that the document was not about the author, see Topuridze v. FBI, No. 86-3120, 1989 WL 11709, at *2-3 (D.D.C. Feb. 6, 1989), on reconsideration it ruled that it need not reach that issue, finding that "[b]ecause the document is without dispute about the [requester], it must be released to him in any event." 772 F. Supp. at 665. On reconsideration, the court embraced Voelker and rejected the government's argument that subsection (b) created a "dual record exemption" to Privacy Act access. Id. at 665-66.

However, the D.C. Circuit reached a result different from those reached in Voelker and Topuridze, although the court did not mention either of those cases. Sussman, 494 F.3d 1106. The Sussman court concluded that information retrieved about the requestor and another third party could not be disclosed to the requestor unless the third party had consented. The U.S. Marshals Service had processed Sussman's subsection (d)(1) request "by searching for records indexed to his name" and found only one document. Sussman v. Marshals Serv., No. Civ. A. 03-610, 2005 WL 3213912, at *1 (D.D.C. Oct. 13, 2005). Sussman argued that the Marshals Service performed an inadequate search and identified a "Wanted Poster" that the Marshals Service had issued for Keith Maydak,

which listed “Michael Sussman” as an alias for “Keith Maydak.” 494 F.3d 1109. The Marshals Service conducted a second search, “now taking into account Sussman’s connections to Maydak.” Id. at 1110. The second search yielded more than 800 pages of documents “relating to Sussman.” Id. The district court stated that “the [Marshals Service] searched Keith Maydak’s files for records related or pertaining to [Sussman] or that mentioned [Sussman] by name.” 2005 WL 3213912, at *2. The Marshals Service disclosed only some of these records to Sussman. 494 F.3d at 1110. Sussman brought a subsection (d)(1) claim against the Marshals Service. Id. The D.C. Circuit “interpret[ed] 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.” Id. at 1121. The court explained that “[f]or an assemblage of data to qualify as one of Sussman’s records, it must not only contain his name or other identifying particulars but also be ‘about’ him. . . . That is, it must actually describe him in some way.” Id.; see also Aguirre v. SEC, 671 F. Supp. 2d 113, 122 (D.D.C. 2009) (declining to dismiss claim seeking access to record that “clearly contains plaintiff’s name and describes him, his history at the SEC and details related to his termination” because record “sufficiently describes plaintiff to satisfy the standard established by Sussman”). Thus, the court held, “the Marshals Service must disclose to Sussman those materials – and only those materials – contained in records about him, the release of which would not violate 5 U.S.C. § 552a(b).” Id. In a footnote, the court explained that “[i]f certain materials pertain to both Sussman and other individuals, from whom the Marshals Service has received no written consent permitting disclosure, the Privacy Act would both require (5 U.S.C. § 552a(d)(1)) and forbid (id. § 552a(b)) their disclosure.” Id. at n.9. In such a situation, subsection (d)(1) must give way because “the consent requirement in § 552a(b) is one of the most important, if not the most important, provisions in the Privacy Act.” Id.; see also Mobley v. CIA, 924 F. Supp. 2d 24, 57 (D.D.C. 2013) (following Sussman and denying plaintiff access to information about plaintiff but also about third-party individuals who did not provide written consent to have their information disclosed); Anderson v. Treasury, No. 76-1404, slip op. at 13 (D.D.C. July 19, 1977) (presaging Sussman by finding name of third-party complainant in requester’s file to be “about” complainant and, therefore, denying requester access to complainant’s name).

The D.C. Circuit’s opinion in Sussman seriously calls into question the validity of Topuridze, insofar as Topuridze could be read to require an agency to disclose to a requester “those materials -- contained in records about him” even if the release of those materials would violate the subsection (b) rights of the non-requesting party. See Sussman, 494 F.3d at 1121. While Sussman controls in the D.C. Circuit, which has universal venue for Privacy Act matters, the holding in Voelker remains undisturbed in the Eighth Circuit.

Individuals are not required to provide a reason for requesting access to records, but agencies must verify individuals' identities before releasing requested records.

A requester need not state his reason for seeking access to records under the Privacy Act, but an agency should verify the identity of the requester in order to avoid violating subsection (b). See OMB 1975 Guidelines, 40 Fed. Reg. at 28,957-58, https://www.justice.gov/paoverview_omb-75; see also 5 U.S.C. § 552a(i)(1) (criminal penalties for disclosure of information to parties not entitled to it); 5 U.S.C. § 552a(i)(3) (criminal penalties for obtaining records about individual under false pretenses); *cf., e.g.*, 28 C.F.R. § 16.41(d) (2020) (DOJ regulation requiring requestor to verify identity).

Agencies are not obligated to turn over documents that are created after the date of an access request, but, in the FOIA context, courts have held that agencies must act reasonably and notify the requestor when setting a cut-off date.

Although subsection (d)(1) “carries no prospective obligation to turn over new documents that come into existence after the date of the request,” Crichton v. Cmty. Servs. Admin., 567 F. Supp. 322, 325 (S.D.N.Y. 1983), the Courts have acknowledged that agencies may set a cut-off date for FOIA searches, but have imposed limitations such as reasonableness and notice to the requestor. For example, the D.C. Circuit has held that under the FOIA, a date-of-request cut-off policy regardless of circumstances – as opposed to a date-of-search cut-off policy – was unreasonable under the facts of that case. Pub. Citizen v. State, 276 F.3d 634, 644 (D.C. Cir. 2002); Leopold v. DOJ, 411 F. Supp. 3d 1094, 1102 (C.D. Cal. 2019) (“the agency generally uses the date the search was run as the cut-off date”); Prop. of the People, Inc. v. DOJ, 405 F. Supp. 3d 99, 120 (D.D.C. 2019) (“[T]he FBI’s ‘unpublicized temporal limitation of its searches’ was improper.” (quoting McGehee v. CIA, 697 F.2d 1095, 1101 (D.C. Cir. 1983))); Vento v. IRS, 714 F. Supp. 2d 137, 144–45 (D.D.C. 2010) (concluding that a date of request cutoff was appropriate and harmonizing Pub. Citizen v. State).

For further information regarding the Privacy Act exception for disclosures under the FOIA, see the discussion above under “Conditions of Disclosure to Third Parties, Twelve Exceptions to the ‘No Disclosure without Consent’ Rule, 5 U.S.C. § 552a(b)(2) - Required FOIA Disclosure.”

INDIVIDUAL'S RIGHT OF AMENDMENT

"Each agency that maintains a system of records shall--

...

(2) permit the individual to request amendment of a record pertaining to him and--

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either--

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed." 5 U.S.C. § 552a(d)(2)-(4).

Comment:

For a discussion of subsections (d)(2)-(4), see OMB 1975 Guidelines, 40 Fed. Reg. at 28,958-60, https://www.justice.gov/paoverview_omb-75. For a discussion of amendment lawsuits, see the section entitled “Civil Remedies, 5 U.S.C. § 552a(g)(1)(A) - Amendment Lawsuits” below.

If an agency refuses to amend an individual’s record, as requested, the individual has the right to file a statement of disagreement.

There have only been a few cases discussing statements of disagreement, and they confirm an individual’s right to file a statement as a separate remedy to the right to amendment. See, e.g., Strong v. OPM, 92 F. App’x 285, 288 (6th Cir. 2004) (“As [plaintiff] remains free to supplement his file to disprove [the reference’s] opinion, OPM did not violate the Privacy Act by refusing to remove [the reference’s] statement from [plaintiff’s] file.”); Gowan v. Air Force, 148 F.3d 1182, 1188-89 (10th Cir. 1998) (concluding that although plaintiff “does not have a Privacy Act cause of action to require the Air Force to amend the records or attach a statement of disagreement” to records maintained in a properly exempt system of records, agency may “voluntarily comply” with the statement of disagreement provision); Middlebrooks v. Mabus, No. 1:11cv46, 2011 WL 4478686, at *5 (E.D. Va. Sept. 23, 2011) (“Plaintiff’s allegations clearly challenge opinions. Specifically, she complains of her colleagues’ and supervisors’ assessments of her performance. Yet, if [plaintiff] believed that her evaluations were misleading or unfair, her proper recourse was to place a concise statement in [her] records which sets forth [her] disagreement with the opinions contained therein.” (quoting Subh v. Army, No. 1:10cv433, 2010 WL 4961613, at *3-4 (E.D. Va. Nov. 30, 2010), aff’d, 417 F. App’x 285 (4th Cir. 2011))).

AGENCY REQUIREMENTS

The Privacy Act requires agencies maintain systems of records according to certain standards. The Act includes 11 such requirements which are discussed in turn below.

A. 5 U.S.C. § 552a(e)(1) - Maintain Only Relevant and Necessary Information

“Each agency that maintains a system of records shall –

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President.”

5 U.S.C. § 552a(e)(1).

Comment:

Agencies can only keep records that are “relevant and necessary” for a purpose “required to be accomplished” by law.

This subsection “authorizes the Government to keep records pertaining to an individual only when they are ‘relevant and necessary’ to an end ‘required to be accomplished’ by law. NASA v. Nelson, 562 U.S. 134, 142 (2011); Reuber v. United States, 829 F.2d 133, 139-40 (D.C. Cir. 1987); Azmat v. Shalala, 186 F. Supp. 2d 744, 751 (W.D. Ky. 2001), aff’d per curiam sub nom. Azmat v. Thompson, No. 01-5282 (6th Cir. Oct. 15, 2002); Nat’l Fed’n of Fed. Emps. v. Greenberg, 789 F. Supp. 430, 433-34 (D.D.C. 1992), vacated & remanded on other grounds, 983 F.2d 286 (D.C. Cir. 1993); NTEU v. IRS, 601 F. Supp. 1268, 1271 (D.D.C. 1985); Chocallo v. Bureau of Hearings & Appeals, 548 F. Supp. 1349, 1368 (E.D. Pa. 1982), aff’d, 716 F.2d 889 (3d Cir. 1983) (unpublished table decision); see also AFGE v. HUD, 118 F.3d 786, 794 (D.C. Cir. 1997) (finding constitutional agency use of release form on employment suitability questionnaire in light of Privacy Act’s subsection (e)(1) requirement and “relying on the limitation that the release form authorizes the government to obtain only relevant information used to verify representations made by the employee”); Barlow v. VA, No. 92-16744, 1993 WL 355099, at *1 (9th Cir. Sept. 13, 1993) (holding that VA’s request for appellant’s medical records did not violate Privacy Act because VA is authorized to request such information and it is “relevant and necessary” to appellant’s claim for benefits; citing subsection (e)(1)); Press v. United States, No. JKB-17-1667, 2018 WL 3239495, at *2 (D. Md. Jul. 7, 2018) (finding subsection (e)(1) was improper vehicle for claim where plaintiff was not challenging legality of collecting information related to his security clearance); Kelley v. FBI, 67 F. Supp. 3d 240, 260-262 (D.D.C. 2014) (finding plaintiff alleged insufficient facts to

support plausible inference of intentional and willful conduct because it was relevant and legal for FBI and DOD to seek to understand nature of potentially inappropriate relationship involving military officer revealed by e-mails in record); Crummey v. SSA, 794 F. Supp. 2d 46, 56-57 (D.D.C. 2011) (ruling that SSA need not amend records because doing so “would require the SSA to maintain information about [plaintiff] that is neither relevant nor necessary to accomplishing any purpose of the SSA” where plaintiff – who believed that SSA created trust when it assigned him social security number and social security card and who had “drafted an agreement designed to reflect the alleged creation of the Trust” – requested amendment of his records “to include a copy of the Trust Agreement, or to reflect its contents”), summary affirmance granted, No. 11-5231, 2012 WL 556317 (D.C. Cir. Feb. 6, 2012); Thompson v. State, 400 F. Supp. 2d 1, 18 (D.D.C. 2005) (“While an agency normally would have no reason to maintain information on an employee’s personal relationships, in these circumstances plaintiff’s relationship was inextricably linked with allegations of favoritism by her supervisor.”); Felsen v. HHS, No. 95-975, slip op. at 59-61 (D. Md. Sept. 30, 1998) (discussing how subsection (e)(1) “refers to the types of information maintained and whether they are germane to the agency’s statutory mission,” and “does not incorporate [an] accuracy standard”); Jones v. Treasury, No. 82-2420, slip op. at 2 (D.D.C. Oct. 18, 1983) (ruling that maintenance of record concerning unsubstantiated allegation that ATF Special Agent committed crime was “relevant and necessary”), aff’d, 744 F.2d 878 (D.C. Cir. 1984) (unpublished table decision); Conyers v. VA, No. 16-CV-00013, 2018 WL 1867106, at *9 (E.D.N.Y. Jan. 29, 2018) (magistrate’s recommendation) (finding no subject matter jurisdiction over plaintiff’s claim that agency violated statute because plaintiff did not challenge counseling report as “relevant and necessary;” rather, plaintiff claimed agency “failed to utilize the information documented” in its benefit determination which was merely attack on determination and “rhetorical cover” for plaintiff’s challenge to his benefits determination), adopted, 2018 WL 1089736 (E.D.N.Y. Feb 26, 2018); Kalderon v. Finkelstein, No. 1:08 Civ. 09440, 2010 WL 9488933, at *28 (S.D.N.Y. Mar. 10, 2010) (magistrate’s recommendation), adopted in pertinent part, 2010 WL 3359473 (S.D.N.Y. Aug. 25, 2010), aff’d, 495 F. App’x 103 (2d Cir. 2012); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,960-61, https://www.justice.gov/paoverview_omb-75; 120 Cong. Rec. at 40,407, reprinted in Source Book at 863, https://www.justice.gov/opcl/paoverview_sourcebook.

B. 5 U.S.C. § 552a(e)(2) - Collect Information, to the Greatest Extent Practicable, Directly from the Individual

“Each agency that maintains a system of records shall –
...

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs." 5 U.S.C. § 552a(e)(2).

Comment:

In order to obtain relief under subsection (e)(2) of the Privacy Act, a plaintiff must establish that: (1) the agency failed to elicit information directly from the plaintiff to the greatest extent practicable; (2) the violation of the Act was intentional or willful; and (3) this action had an adverse effect on the plaintiff. Waters v. Thornburgh, 888 F.2d 870, 872 (D.C. Cir. 1989). Waters involved a Justice Department employee whose supervisor became aware of information that raised suspicions concerning the employee's unauthorized use of administrative leave. 888 F.2d at 871-72. Without first approaching the employee for clarification, the supervisor sought and received from a state board of law examiners verification of the employee's attendance at a bar examination. Id. at 872. In finding a violation of subsection (e)(2) on these facts, the D.C. Circuit ruled that "[i]n the context of an investigation that is seeking objective, unalterable information, reasonable questions about a subject's credibility cannot relieve an agency from its responsibility to collect that information first from the subject." Id. at 873 (emphasis added); accord Dong v. Smithsonian Inst., 943 F. Supp. 69, 72-73 (D.D.C. 1996) ("concern over Plaintiff's possible reaction to an unpleasant rumor" did not warrant Smithsonian Institution's "fail[ure] to elicit information regarding her alleged unauthorized courier trip directly from her"), rev'd on grounds of statutory inapplicability, 125 F.3d 877 (D.C. Cir. 1997) (ruling that "Smithsonian is not an agency for Privacy Act purposes").

The OMB 1975 Guidelines suggest several factors to be evaluated in determining whether it is impractical to contact the subject first. 40 Fed. Reg. at 28,961, https://www.justice.gov/paoverview_omb-75; see also 120 Cong. Rec. 40,407, reprinted in Source Book at 863, https://www.justice.gov/opcl/paoverview_sourcebook.

Courts generally have not required agencies to obtain information directly from the subject individual where the individual could interfere with evidence or is accused of misconduct.

The D.C. Circuit in Waters distinguished its earlier decision in Brune v. IRS, 861 F.2d 1284 (D.C. Cir. 1988), which had permitted an IRS supervisor to contact taxpayers to check on an agent's visits to them without first interviewing the agent, based upon the "special nature of the investigation in that case – possible

false statements by an IRS agent” and the concomitant risk that the agent, if contacted first, could coerce the taxpayers to falsify or secret evidence. Waters, 888 F.2d at 874; see also Velikonja v. Mueller, 362 F. Supp. 2d 1, 19-20 (D.D.C. 2004) (“seeking records from an electronic door log is very different from asking [plaintiff’s] colleagues, rather than her, about her schedule” as “[t]he door log provided the most objective source of information about her actual entry times to the building, and unlike the proof of bar exam attendance in Waters, the records could not be obtained from plaintiff”), aff’d in pertinent part & rev’d in part sub nom. Velikonja v. Gonzales, 466 F.3d 122 (D.C. Cir. 2006) (per curiam).

Consistent with Brune, two other decisions have upheld the IRS’s practice of contacting taxpayers prior to confronting agents who were under internal investigations. See Alexander v. IRS, No. 86-0414, 1987 WL 13958, at *6-7 (D.D.C. June 30, 1987); Merola v. Treasury, No. 83-3323, slip op. at 5-9 (D.D.C. Oct. 24, 1986).

In addition, the courts have often followed Brune rather than Waters where there was an indication that the subject of the records previously harassed or threatened other potential witnesses or where it would not have made a difference had the subject been contacted first. For example, the Court of Appeals for the Sixth Circuit relied on Brune and the OMB guidelines and regulations to hold that subsection (e)(2) had not been violated by an investigator looking into charges of misconduct by an Assistant U.S. Attorney who had interviewed others before interviewing her. Hudson v. Reno, 130 F.3d 1193, 1205 (6th Cir. 1997). Given that the district court had found that the AUSA “was suspected of making false statements and she was allegedly intimidating and threatening people and otherwise dividing the U.S. Attorney’s office,” the Sixth Circuit held that “[a]ll of these practical considerations demonstrate that [the investigator] did not violate the Privacy Act when he interviewed others before interviewing [her].” 130 F.3d at 1205.

Moreover, in a case involving a misconduct investigation into whether an agency employee had been intoxicated on the job, the Court of Appeals for the Fourth Circuit went so far as to observe that “[s]o long as the agency inevitably will need to interview both [the employee] and others, the Act takes no position on the order in which they [a]re approached.” Hogan v. England, 159 F. App’x 534, 537 (4th Cir. 2005). See also Carton v. Reno, 310 F.3d 108, 112-13 (2d Cir. 2002) (permitting “a preference to interview [plaintiff] last” when investigating misconduct complaint against him because of plaintiff’s “authority as an INS agent” and existing “specific allegations that [plaintiff] had already terrorized and intimidated the complainants”); Cardamone v. Cohen, 241 F.3d 520, 527-28 (6th Cir. 2001) (finding it “impracticable to think that charges of employee

mistreatment and harassment could be resolved by interviewing [the plaintiff] before others” because plaintiff “could not have verified any conclusions” as to “subjective allegations of employee mistreatment”); Carlson v. GSA, No. 04-C-7937, 2006 WL 3409150, at *6 (N.D. Ill. Nov. 21, 2006) (ruling that agency did not violate subsection (e)(2) “by not interviewing [an agency employee] first” since “[t]he issues under investigation [regarding the employee’s undisclosed arrest] could not have been resolved by objective evidence within [the employee’s] possession”; and concluding that “[t]he Act does not require the agency to undertake a piecemeal investigation by obtaining objective evidence first and then interviewing third party witnesses as to the more subjective claims”); Thompson v. State, 400 F. Supp. 2d 1, 10-11 (D.D.C. 2005) (finding that agency “sought information directly from plaintiff ‘to the extent practicable’” where agency interviewed plaintiff’s coworkers before interviewing her in the context of an investigation into allegations made by coworkers that plaintiff helped create a hostile work environment; and further stating that “[t]he order of interviews therefore would not have altered the investigation’s impact on plaintiff’s reputation”); Mumme v. Labor, 150 F. Supp. 2d 162, 173 (D. Me. 2001) (observing that “[w]hen conducting a criminal investigation of an individual . . . however, it may not be practicable for the investigating officers to collect information via direct questioning of the individual”), aff’d, No. 01-2256 (1st Cir. June 12, 2002); Jacobs v. Reno, No. 3:97-CV-2698-D, 1999 U.S. Dist. LEXIS 3104, at *19-22, 29-35 (N.D. Tex. Mar. 11, 1999) (finding no subsection (e)(2) violation in agency’s “extensive, multifaceted investigation of an entire district office” where plaintiff was “both a charging party in several complaints and an accused in several others,” as it “was not always practical” for agency to interview plaintiff first, given nature of allegations against him), subsequent decision, 1999 WL 493056, at *1 (N.D. Tex. July 9, 1999) (denying motion for relief from March 11, 1999, order because “newly-discovered evidence” would not have produced different result), aff’d, 208 F.3d 1006 (5th Cir. 2000) (unpublished table decision); Jones v. Runyon, 32 F. Supp. 2d 873, 876 (N.D. W. Va. 1998) (routine check for fraud falls within exception to requirement to contact plaintiff first and permits obtaining information from third parties), aff’d, 173 F.3d 850 (4th Cir. 1999) (unpublished table decision); but see Lasseigne v. White, No. 1:14-CV-3156-TWT-CMS, 2015 WL 10015298 (N.D. Ga. Dec. 21, 2015) (finding plaintiff sufficiently stated claim by alleging that SEC conducted questioning when plaintiff was not in office, that purpose of investigation was to retaliate against him, and that his supervisor provided false information to investigators); Brunotte v. Johnson, 892 F. Supp. 2d 199, 208-09 (D.D.C. 2012) (finding issue of fact under subsection (e)(2) despite defendant’s contention that it could not have practicably procured information from plaintiff rather than from previous government agency employer because of suspicions that plaintiff had falsified aspects of her job application with that employer; this fact does not excuse [agency] from seeking

information from her directly); Doe v. Goss, No. 04-2122, 2007 WL 106523, at *12-14 (D.D.C. Jan 12, 2007); (finding factual disputes precluded motion to dismiss where plaintiff was not timely interviewed in investigation despite agency's claim plaintiff was in position to intimidate third parties or encourage collusion).

The Eighth and D.C. Circuits have suggested that an agency does not "collect" information within the meaning of subsection (e)(2) when it already exists in its own files.

The Court of Appeals for the Eighth Circuit has examined the issue of whether a "collection" subject to the requirements of subsection (e)(2) occurs when an agency reviews its own files to obtain information. Darst v. SSA, 172 F.3d 1065 (8th Cir. 1999). The Eighth Circuit held that because the "situation merely involved a review of the agency's file," the agency "did not contact third party sources to gather information," and because "the indications of impropriety were apparent from the face of the documents and from the sequence of events" reflected in the file, there was "no need to interview Darst about the sequence of events," and thus no violation of subsection (e)(2). Id. at 1068. The Eighth Circuit further stated that "[a]s the district court noted, the Privacy Act does not require that the information be collected directly from the individual in all circumstances," and that "[h]ere the information in the [agency] file obviated the need to interview Darst or third persons." Id.; see also Brune v. IRS, 861 F.2d at 1287 (stating that "investigations of false statement charges, by their nature, involve a suspect who has already given the government his version of the facts"); Velikonja, 362 F. Supp. 2d at 20 (holding that agency was not required to interview plaintiff before examining "electronic door logs" to compare them with her sworn attendance sheets because objective proof – "electronic door logs" – could not be obtained from plaintiff).

Several courts have held that agencies generally meet the subsection (e)(2) requirement where they give individuals the opportunity to provide information.

In several cases, the courts have found that an agency satisfied its section (e)(2) obligations by giving an individual an opportunity to provide information, even if the individual did not actually provide it. See Olivares v. NASA, No. 95-2343, 1996 WL 690065, at *2-3 (4th Cir. Dec. 3, 1996) (finding that defendant had contacted plaintiff directly before contacting universities to verify academic credentials where plaintiff was given opportunity to provide information in his employment application and personal interview), aff'g per curiam 882 F. Supp. 1545 (D. Md. 1995); Hubbard v. EPA, 809 F.2d 1, 6 n.8 (D.C. Cir. 1986) (defendant was not forbidden from using relevant information from third parties in hiring decision and made "practicable" effort to collect information from plaintiff when

asked whether plaintiff knew source of leaks in previous investigation plaintiff had worked on), vacated in nonpertinent part & reh'g en banc granted (due to conflict within circuit), 809 F.2d 1 (D.C. Cir. 1986), resolved on reh'g en banc sub nom.; Ramey v. Marshals Serv., 755 F. Supp. 2d 88, 97 (D.D.C. 2010) (no issue of fact where voluminous record of plaintiff's statements in investigation showed defendant provided plaintiff "a fair shake at telling her side of the story"); McCready v. Principi, 297 F. Supp. 2d 178, 199-200 (D.D.C. 2003) (dismissing claim where defendant first attempted to obtain information from plaintiff about her leave history and her responsive memos did not clear up questions), aff'd in pertinent part & rev'd in part sub nom. McCready v. Nicholson, 465 F.3d 1 (D.C. Cir. 2006) (remanding for reasonable opportunity to complete discovery on count brought pursuant to subsection (e)(2) which did not require administrative exhaustion of remedies); Felsen v. HHS, No. CCB-95-975, slip op. at 62-65 (D. Md. Sept. 30, 1998) (granting defendants' summary judgment on alternative ground on subsection (e)(2) claim due to "lack of a 'practicable' need to collect information directly from the plaintiffs"); Magee v. USPS, 903 F. Supp. 1022, 1028-29 (W.D. La. 1995) (granting summary judgement where plaintiff refused to hand over medical report in face-to-face meeting and postmaster eventually obtained report by subpoena), aff'd, 79 F.3d 1145 (5th Cir. 1996) (unpublished table decision); Kassel v. VA, 709 F. Supp. 1194, 1203 (D.N.H. 1989) (granting summary judgement where board of inquiry did speak with plaintiff before completing its report); Bequette v. USPS, No. 88-802, slip op. at 10 (E.D. Va. July 3, 1989) (finding subsection (e)(2) requirements satisfied where information contained in records was derived from other records containing information collected directly from individual); cf. Conyers v. VA, No. 16-CV-00013, 2018 WL 1867106 (E.D.N.Y. Jan. 29, 2018) (magistrate's recommendation) (finding plaintiff's claim that department intentionally and willfully failed to collect information directly from him to be attack on defendant's decision-making rather than on recordkeeping requirements and, therefore, outside Court's purview) adopted, 2018 WL 1089736 (E.D.N.Y. Feb 26, 2018).

In a few cases, the courts have concluded that the subsection (e)(2) requirement was not triggered.

Agencies are not obligated to obtain information from the subject individual directly if those records are exempt from section (e)(2), the individual has not made a sufficiently detailed allegation, or the agency was authorized to obtain the information from another source. See Gadson v. John Doe, No. 3:15-CV-00040-KRG, 2016 WL 3469383 (W.D. Pa. May 24, 2016) (magistrate's recommendation) (because prison records were exempted from 552(e)(2), plaintiff prisoner could not state claim) adopted, 2016 WL 3546056 (W.D. Pa. Jun 21, 2016); Augustus v. McHugh, 825 F. Supp. 2d 245, 257-58 (D.D.C. 2011)

(finding plaintiff's bare allegation that she did not receive new job assignment as result of collection of third party information did not trigger agency's obligation to collect information from her); Kalderon v. Finkelstein, No. 08 Civ. 9440, slip op. at 73-77, 2010 WL 9488933 (S.D.N.Y. Mar. 10, 2010) (magistrate's recommendation) (finding plaintiff failed to state claim where defendant was authorized to obtain information directly from recipient of grant, grantee institution), adopted in pertinent part, 2010 WL 3359473 (S.D.N.Y. Aug. 25, 2010), aff'd, 495 F. App'x 103 (2d Cir. 2012).

C. 5 U.S.C. § 552a(e)(3) - Inform Individuals when Asking to Collect Information

"Each agency that maintains a system of records shall –

...

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual – (A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary; (B) the principal purpose or purposes for which the information is intended to be used; (C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and (D) the effects on him, if any, of not providing all or any part of the requested information." 5 U.S.C. § 552a(e)(3).

Comment:

OMB guidelines state that the subsection (e)(3) notice requirement is intended to give individuals sufficient information to enable them to decide whether to supply information.

The OMB 1975 Guidelines explain that "[i]mplicit in this subsection is the notion of informed consent since an individual should be provided with sufficient information about the request for information to make an informed decision on whether or not to respond." 40 Fed. Reg. at 28,961, <https://www.justice.gov/paoverview-omb-75>. The OMB 1975 Guidelines also note that subsection (e)(3) is applicable to both written and oral (i.e., interview) solicitations of personal information. Id.

Most courts have afforded agencies broad latitude in determining the content of their subsection (e)(3) notices.

Generally, an agency does not need to explain "all of [its] rules and regulations"

on “one small form” to meet the substantive requirements of subsection (e)(3). Glasgold v. Sec’y of HHS, 558 F. Supp. 129, 150 (E.D.N.Y. 1982); see also Field v. Brown, 610 F.2d 981, 987 (D.C. Cir. 1979) (holding that the agency’s form “contained all the elements required by 5 U.S.C. § 552a(e)(3)”).

In evaluating the requirements of subsection (e)(3)(A), “[n]othing in the Privacy Act requires agencies to employ the exact language of the statute to give effective notice.” United States v. Wilber, 696 F.2d 79, 80 (8th Cir. 1982) (per curiam) (finding that an IRS notice was in compliance with subsection (e)(3)(A) even though it did not use the word “mandatory”); see also Bartoli v. Richmond, No. 00-1043, 2000 WL 687155, at *3 (7th Cir. May 23, 2000) (finding that the IRS sufficiently gave notice pursuant to subsection (e)(3)(A) by citing section 6001 of the Internal Revenue Code as authority for its field examination); United States v. Bressler, 772 F.2d 287, 292-93 (7th Cir. 1985) (following Wilber); cf. Thompson v. State, 400 F. Supp. 2d 1, 17 (D.D.C. 2005) (finding that “[t]he very uses of the information to which plaintiff specifically objects (i.e., giving it to [other offices within the agency] and placing it in her security file) . . . can be reasonably inferred from the warning given,” which stated that the information was being collected for an “administrative inquiry regarding misconduct or improper performance”; further stating that plaintiff could infer from this warning that “if she provided information revealing misconduct by her, the agency might use it to make a determination adverse to her”).

The Court of Appeals for the Fifth Circuit has gone so far as to rule in favor of an agency even though the agency “clearly did not follow the Act’s requirements because the [form] did not indicate whether filling out the form was voluntary or mandatory or, alternatively, because [plaintiff’s] supervisors ordered him to fill out the form even though filling it out was voluntary.” Sweeney v. Chertoff, 178 F. App’x 354, 357 (5th Cir. 2006). The court held that the appellant’s injury was “sufficiently attenuated from any violation of the Act’s requirements to preclude a finding of causation.” Id. The court reasoned that the Privacy Act did not provide the remedy for the plaintiff’s damages – which arose from his punishment for insubordination based on his refusal to fill out the form – because “the Privacy Act is not the proper channel by which to challenge internal agency disciplinary actions with which one disagrees.” Id. at 358 & n.3.

One court has held that a notice that informed witnesses of an investigation into allegations of misconduct but did not warn of the investigation subject’s possible termination as an outcome, met the requirements of subsection (e)(3)(B) because the “text of the statute clearly requires” that the witnesses be notified of the “purpose” of the interview “not [its] possible results.” Cardamone v. Cohen, No. 3:97CV540H, slip op. at 4-5 (W.D. Ky. Sept. 30, 1999), aff’d, 241 F.3d 520, 529-30

(6th Cir. 2001); cf. Beller v. Middendorf, 632 F.2d 788, 798 n.6 (9th Cir. 1980) (noting that when plaintiff provided information to agency “albeit originally in connection with a check for a top secret security clearance,” he “must have known that information which disclosed grounds for being discharged could be used in discharge proceedings”), overruled on other grounds by Witt v. Department of Air Force, 527 F.3d 806, 820-821 (9th Cir. 2008); Thompson, 400 F. Supp. 2d at 16 (ruling that agency need not “tell an individual that she is the subject of an investigation” in order to provide her with “informed consent” where agency notified employee that purpose of collection was to assess her “suitability for continued employment”).

In addition, several courts have found in criminal cases that subsection (e)(3)(D) does not require an agency to provide notice of the specific criminal penalty that may be imposed for failure to provide information. See, e.g., United States v. Bishop, 946 F.2d 896, at *4 (6th Cir. Oct. 23, 1991) (unpublished table decision) (per curiam); Bressler, 772 F.2d at 292-93; United States v. Bell, 734 F.2d 1315, 1318 (8th Cir. 1984) (per curiam); Wilber, 696 F.2d 79, at 80; United States v. Annunziato, 643 F.2d 676, 678 (9th Cir. 1981); United States v. Rickman, 638 F.2d 182, 183 (10th Cir. 1980); United States v. Gillotti, 822 F. Supp. 984, 988 (W.D.N.Y. 1993).

Some courts have determined that an agency’s failure to provide notice of the routine uses which may be made of the information consistent with the subsection (e)(3) notice requirement precluded later reliance on that routine use to disclose the information in compliance with the Privacy Act’s disclosure provisions.

In Covert v. Harrington, a divided panel of the Court of Appeals for the Ninth Circuit held that an agency component’s failure to provide actual notice of a routine use under subsection (e)(3)(C), at the time at which information was submitted, precluded a separate component of the agency, the Inspector General, from later invoking that routine use as a basis for disclosing such information. 876 F.2d 751, 755-56 (9th Cir. 1989); see also Puerta v. HHS, No. 99-55497, 2000 WL 863974, at *1-2 (9th Cir. June 28, 2000) (following Covert, but finding that agency had provided notice of routine use on form used to collect information), aff’g No. EDCV 94-0148, slip op. at 7 (C.D. Cal. Jan. 5, 1999); USPS v. Nat’l Ass’n of Letter Carriers, 9 F.3d 138, 146 (D.C. Cir. 1993) (citing Covert with approval and remanding case for factual determination as to whether subsection (e)(3)(C) notice was given); McKinley v. United States, No. 3:14-cv-01931-HZ, 2015 WL 4663206, at *8 (interpreting Covert to require agency invoking routine use exception to first “inform[] the individual on the form used to collect information or on a separate form that can be retained by the individual about the routine uses that may be made of the information”); Cooper v. FAA, 816 F. Supp. 2d 778,

788-790 (N.D. Cal. 2008) (holding that disclosure of social security records to Transportation Department by SSA was improper because “the notice provided on the form [plaintiff] used to submit his information to SSA was insufficient” to notify plaintiff of reason for disclosure), rev’d on other grounds, 622 F.3d 1016 (9th Cir. 2010), rev’d, 566 U.S. 284 (2012), aff’d, 696 F.3d 1265 (9th Cir. 2012); Pontecorvo v. FBI, No. 00-1511, slip op. at 12 (D.D.C. Sept. 30, 2001) (stating that agency must comply with subsection (e)(3)(C) “to substantiate an exception for ‘routine use’”). But see OMB 1975 Guidelines, 40 Fed. Reg. at 28,961-62, https://www.justice.gov/paoverview_omb-75 (“It was not the intent of [subsection (e)(3)] to create a right the nonobservance of which would preclude the use of the information or void an action taken on the basis of that information.”).

The courts have split on whether the subsection (e)(3) notice requirement applies when the agency solicits information from a third party.

Some authorities have concluded that subsection (e)(3) is inapplicable when an agency solicits information about an individual from a third party. See Gardner v. United States, No. 96-1467, 1999 U.S. Dist. LEXIS 2195, at *19 (D.D.C. Jan. 29, 1999) (noting that although it is correct that the Privacy Act mandates actual notice of routine uses, “information in the instant case was not gathered from Plaintiff, but from third parties”), summary affirmance granted on other grounds, No. 99-5089, 1999 WL 728359 (D.C. Cir. Aug. 4, 1999) (per curiam); McTaggart v. United States, 570 F. Supp. 547, 550 (E.D. Mich. 1983) (finding individual lacks standing to complain of insufficient Privacy Act notice to third party); Truxal v. Casey, 2 Gov’t Disclosure Serv. (P-H) ¶ 81,391, at 82,043 (S.D. Ohio Apr. 3, 1981); cf. United States v. The Inst. for Coll. Access & Success, 956 F. Supp. 2d 190, 198 (D.D.C. 2013) (finding that “Privacy Act Notification is vague as to what the [agency] may demand from independent third parties unrelated to the federal government”), rev’d on other grounds, 27 F. Supp. 3d 106 (D.D.C. 2014). The OMB 1975 Guidelines support this view, but suggest that “agencies should, where feasible, inform third-party sources of the purposes for which information which they are asked to provide will be used.” 40 Fed. Reg. at 28,961, https://www.justice.gov/paoverview_omb-75.

On the other hand, the practice of not providing notice to third parties was condemned by the Privacy Protection Study Commission. See Privacy Commission Report at 514, https://www.justice.gov/paoverview_ppsc. In the same vein, several courts have followed the Commission’s views on this issue. See Usher v. Sec’y of HHS, 721 F.2d 854, 856 (1st Cir. 1983) (costs awarded to plaintiff due to agency “intransigence” in refusing to provide information specified in subsection (e)(3) to third party); Kassel v. VA, No. 87-217-S, slip op.

at 24-25 (D.N.H. Mar. 30, 1992) (in light of “the express language of § (e)(3) and the Privacy Act’s overall purposes . . . § (e)(3) applies to information supplied by third-parties”); Saunders v. Schweiker, 508 F. Supp. 305, 309 (W.D.N.Y. 1981) (plain language of subsection (e)(3) “does not in any way distinguish between first-party and third-party contacts”).

D. 5 U.S.C. § 552a(e)(4) - Publish System of Records Notice

“Each agency that maintains a system of records shall –

...

(4) [subject to notice and comment], publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include –

- (A) the name and location of the system;
- (B) the categories of individuals on whom records are maintained in the system;
- (C) the categories of records maintained in the system;
- (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
- (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
- (F) the title and business address of the agency official who is responsible for the system of records;
- (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
- (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its contents; and
- (I) the categories of sources of records in the system.” 5 U.S.C. § 552a(e)(4).

Comment:

An agency that is establishing or revising a system of records is required to

publish a system of records notice (SORN) in the Federal Register. The OMB 1975 Guidelines published just after the Privacy Act was enacted discuss this provision in detail, including the nine categories of information that must be included. See 40 Fed. Reg. at 28,962-64, https://www.justice.gov/paoverview_omb-75.

System of records notices (SORNs) are available on agency websites and are compiled by the Government Printing Office.

Privacy Act system notices are published in the Federal Register, and the National Archives' Office of the Federal Register also publishes a biennial compilation of all such system notices. See 5 U.S.C. § 552a(f). Those Privacy Act Compilation Issuances contain descriptions of federal agency systems of records maintained on individuals and procedures that federal agencies follow to assist individuals who request information about their records. Each issuance contains individual Privacy Act system descriptions and their governing regulations. Privacy Act Compilation Issuances beginning in 1995 are available on the Government Printing Office's (GPO) Federal Digital System (FDsys) website. See <https://www.govinfo.gov/app/collection/PAI/>. Bulk XML download of Privacy Act Issuances can be accessed at: <https://catalog.data.gov/dataset/privacy-act-issuances-bulk-xml>.

In order to provide more current and convenient access to system notices, OMB requires each agency to "list and provide links to complete, up-to-date versions of all agency SORNs," including citations and links to all Federal Register notices that comprise the SORN for each system of records. OMB Circular A-108, at 29-30, https://www.justice.gov/paoverview_omb-a-108. For an example, see the Department of Justice's publication of its systems of records. See DOJ Privacy Act Systems of Records, <https://www.justice.gov/opcl/doj-systems-records>.

The Tenth Circuit concluded that an agency was not required to publish a new SORN where the new system was composed of abstracts of two other systems of records that had published SORNs.

The only case to discuss the subsection (e)(4) SORN requirements in any depth is Pippinger v. Rubin, 129 F.3d 519 (10th Cir. 1997). In that case, the Court of Appeals for the Tenth Circuit addressed whether the Internal Revenue Service had complied with several of the requirements of subsection (e)(4) with regard to a computer database known as the "Automated Labor Employee Relations Tracking System [(ALERTS)]." Id. at 524-28. The database was used by the IRS to record all disciplinary action proposed or taken against any IRS employee and contained a limited subset of information from two existing Privacy Act systems

that the IRS had properly noticed in the Federal Register. See *id.* at 524-25. Of particular note is that the Tenth Circuit found that ALERTS, being an “abstraction of certain individual records” from other systems of records, did not constitute a new system of records requiring Federal Register publication, because it could be accessed only by the same users and only for the same purposes as those published in the Federal Register for the original systems of records. *Id.* at 526-27. Cf. Corr v. Bureau of the Pub. Debt, 987 F. Supp. 2d 711, 718 (S.D. W.Va. 2013) (finding that “SORN applies only to employee grievances filed under the Administrative Grievance Procedure” and plaintiff cannot obtain access to records and claim “benefit of this system after failing to comply with the requirements that would have brought his complaints within the scope of the SORN”).

E. 5 U.S.C. § 552a(e)(5) - Maintain Accurate, Relevant, Timely, and Complete Records

“Each agency that maintains a system of records shall –

...

(5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” 5 U.S.C. § 552a(e)(5).

Comment:

The subsection (e)(5) requirement establishes a standard against which the accuracy of a record is measured in other Privacy Act provisions, including agency dissemination and amendment requirements, and certain causes of action.

This provision (along with subsections (e)(1) and (e)(7)) sets forth the standard to which records must conform in the context of an amendment lawsuit, as well as in the context of a lawsuit brought under subsection (g)(1)(C) for damages. See 5 U.S.C. § 552a(g)(1)(A); 5 U.S.C. § 552a(g)(1)(C). The “accuracy, relevance, timeliness, and completeness” standard in subsection (e)(5) is also used in subsections (e)(6), relating to dissemination of information and (g)(1)(C). Subsection (e)(6) states that, prior to disseminating any record about an individual to any person other than an agency, the agency must reasonably ensure the records in question are accurate, complete, timely, and relevant for agency purposes. The one exception to this provision is records that are released in accordance with and as required under the Freedom of Information Act. Specifically, subsection (g)(1)(C) provides for civil remedies for a record that does not meet the “accuracy, relevance, timeliness, and completeness” standard.

As the D.C. Circuit has held, “whether the nature of the relief sought is injunctive or monetary, the standard against which the accuracy of the record is measured remains constant [and] that standard is found in 5 U.S.C. § 552a(e)(5) and reiterated in 5 U.S.C. § 552a(g)(1)(C).” Doe v. United States, 821 F.2d 694, 697 n.8 (D.C. Cir. 1987) (en banc).

In theory, a violation of this provision (or any other part of the Act) could also give rise to a damages action under 5 U.S.C. § 552a(g)(1)(D). Cf. Perry v. FBI, 759 F.2d 1271, 1275 (7th Cir. 1985), rev’d en banc on other grounds, 781 F.2d 1294 (7th Cir. 1986). However, the Court of Appeals for the District of Columbia Circuit has held that “a plaintiff seeking damages for noncompliance with the standard set out in subsection (e)(5) must sue under subsection (g)(1)(C) and not subsection (g)(1)(D).” Deters v. Parole Comm’n, 85 F.3d 655, 660-61 & n.5 (D.C. Cir. 1996) (noting that although court had suggested in Dickson v. OPM, 828 F.2d 32, 39 (D.C. Cir. 1987), that subsection (g)(1)(D) could cover violation of subsection (e)(5), “the holding in that case is limited to the scope of subsection (g)(1)(C)”).

Agencies that do not maintain records consistent with the standards set by subsection (e)(5) are not subject to damages claims if the records are maintained in a system of records that is properly exempted from this requirement.

Records systems that an agency has exempted from the Privacy Act in a Federal Register notice are not subject to civil damages actions for inaccurate or substandard recordkeeping of those records. See e.g., Dick v. Holder, 67 F. Supp. 3d 167, 184 (D.D.C. 2014) (concluding that records were exempt from the maintenance requirement of § 552a(e)(5) where Attorney General had “established regulations pursuant to this subsection that exempt materials in the FBI’s Central Records System from various provisions of the Privacy Act”); Barnett v. United States, 195 F. Supp. 3d 4, 8 (D.D.C. 2016) (holding that because BOP exempted certain inmate records from Privacy Act, it “follows that there remains no remedy under the Privacy Act for harm resulting from inaccuracies in the inmate records”); Ali v. ICE, No. 1:16-CV-037-BL, 2017 WL 4325785, at *6 (N.D. Tx. Aug. 29, 2017), report and recommendation adopted, No. 1:16-CV-037-C, 2017 WL 4296756 (N.D. Tex. Sept. 26, 2017). An agency’s exemption from certain Privacy Act provisions does not foreclose a plaintiff’s opportunity to allege violations of the Constitution, however. Cf. Abdelfattah v. U.S. Dept. of Homeland Sec., 787 F.3d 524, 534-538 (D.C. Cir. 2015) (“We have repeatedly recognized a plaintiff may request expungement of agency records for both violations of the Privacy Act and the Constitution.”).

The Federal Bureau of Prisons, a defendant in many amendment suits, exempted a number of its systems of records from the subsection (e)(5) requirement in 2002.

Among the most frequently litigated subsection (e)(5)/(g)(1)(C) claims are those brought by federal inmates against the Federal Bureau of Prisons (BOP). The discussion of subsection (e)(5), below, includes citations to numerous cases involving such claims. Note, however, that it was not until 2002 that the BOP exempted many of its systems of records in a published SORN – among them, notably, the Inmate Central Records System – from subsection (e)(5) pursuant to subsection (j)(2). See 28 C.F.R. § 16.97(j) (codifying 67 Fed. Reg. 51,754 (Aug. 9, 2002)). This came about as a result of Sellers v. BOP, 959 F.2d 307, 309-312 (D.C. Cir. 1992), in which the D.C. Circuit noted that “regulations governing the BOP . . . do not exempt [the agency’s] records from section (e)(5) of the Act” and, accordingly, remanded the case for a determination of “whether the [agency] met the requirements of sections (e)(5) and (g)(1)(C)” with regard to the items of information at issue.

While the subsection (e)(5) analyses contained in cases decided prior to the promulgation of that exemption regulation remain useful resources in interpreting subsection (e)(5), that inmates’ subsection (e)(5)/(g)(1)(C) claims arising subsequent to August 9, 2002, should not succeed. See, e.g., Blackshear v. Lockett, 411 F. App’x 906, 907-08 (7th Cir. 2011) (“[A]fter Sellers the [BOP] availed itself of a Privacy Act exemption that frees it from an obligation to keep accurate inmate files. . . . Accordingly, the damages remedy available to the plaintiff in Sellers is no longer applicable.”); Lane v. BOP, No. 09-5228, 2010 WL 288816, at *1 (D.C. Cir. Jan. 7, 2010) (“Sellers v. Bureau of Prisons . . . does not control here, as it was decided before the Bureau of Prisons exempted the relevant system of records from the accuracy provision.”), aff’d per curiam No. 08-1269, 2009 WL 1636422 (D.D.C. June 9, 2009); Fisher v. BOP, No. 06-5088, 2007 U.S. App. LEXIS 5140, at *1 (D.C. Cir. Mar. 1, 2007) (“[T]he statement in Sellers v. Bureau of Prisons . . . that the ‘regulations governing the Bureau of Prisons . . . do not exempt those agenc[y]’s records from section (e)(5) of the Act’ is no longer accurate.”), reh’g denied, 2006 U.S. App. LEXIS 28532 (D.C. Cir. Nov. 16, 2006), aff’d per curiam No. 05-0851, 2006 U.S. Dist. LEXIS 9738 (D.D.C. Feb. 21, 2006); Earle v. Holder, 815 F. Supp. 2d 176, 182-83 (D.D.C. 2011), aff’d per curiam, No. 11-5280, 2012 WL 1450574 (D.C. Cir. Apr. 20, 2012); Kates v. King, No. 3:11-CV-00951, 2011 WL 6937553, at *3 & n.1 (M.D. Pa. June 3, 2011), adopted, 2012 WL 10667 (M.D. Pa. Jan. 3, 2012); Davis v. United States, No. CIV-10-1136, 2011 WL 704894, at *5 (W.D. Okla. Jan. 4, 2011) (magistrate’s recommendation), adopted, 2011 WL 693639 (W.D. Okla. Feb. 18, 2011), appeal dismissed, 426 F. App’x 648 (10th Cir. June 14, 2011).

Courts have disagreed, however, on whether to permit claims to go forward that arose before August 9, 2002, but were filed after that date. Compare Patel v. United States, No. 08-1168, 2009 WL 1377530, at *1-2 (W.D. Okla. May 14, 2009) (declining to dismiss claim on ground that record was exempt from subsection (e)(5) because “the exemption . . . post-dates the allegedly false record”), aff’d, 399 F. App’x 355, 360 (10th Cir. 2010), with Truesdale v. DOJ, 731 F. Supp. 2d 3, 9 (D.D.C. 2010) (rejecting argument that “[b]ecause [plaintiff] had been allowed to contest the accuracy of sentencing-related information before 28 C.F.R. § 16.97(j) and (k) became effective . . . he should be allowed to pursue his Privacy Act claims”; “Plaintiff cites no authority for the proposition that he need not be subjected to a duly promulgated and published administrative regulation simply because he demands amendment of records in existence before the effective date of that regulation.”). See also Skinner v. BOP, 584 F.3d 1093, 1097 (D.C. Cir. 2009) (declining to decide whether “it would be impermissibly retroactive to apply [the exemption] to [prisoner’s] lawsuit” where claim arose before date of exemption but was filed after that date). This issue is discussed further under “Ten Exemptions, 5 U.S.C. § 552a(j)(2) - Two General Exemptions for Central Intelligence Agency and Criminal Law Enforcement,” below.

Agencies must take “reasonable” steps to meet the “accuracy, relevance, timeliness, and completeness” standard, including but not limited to, correcting erroneous facts.

An agency “need not keep perfect records, but must act reasonably” to assure accuracy, relevance, timeliness, and completeness. See Colley v. James, 254 F. Supp. 3d 45, 67-68 (D.D.C. 2017) (quoting Dickson v. OPM, 1991 WL 423968, at *15 (D.D.C. Aug. 27, 1991)). See Johnston v. Horne, 875 F.2d 1415, 1421 (9th Cir. 1989), overruled on other grounds, Irwin v. VA, 498 U.S. 89 (1990); DeBold v. Stimson, 735 F.2d 1037, 1041 (7th Cir. 1984); Edison v. Army, 672 F.2d 840, 843 (11th Cir. 1982) (“The use of ‘reasonableness’ language requires the balancing of competing interests: army resources and the ability to assure accurate and complete records versus the likelihood that inaccurate and incomplete records will cause injury to the individual.”); Vymetalik v. FBI, No. 82-3495, slip op. at 3-5 (D.D.C. Jan. 30, 1987); Marcotte v. Sec’y of Def., 618 F. Supp. 756, 762 (D. Kan. 1985); Smierka v. Treasury, 447 F. Supp. 221, 225-26 & n.35 (D.D.C. 1978), remanded on other grounds, 604 F.2d 698 (D.C. Cir. 1979); see also, e.g., Akl v. Sebelius, No. 1:08-cv-00461, slip op. at 13 (D.D.C. Sept. 7, 2012) (rejecting subsection (g)(1)(C) claim where “HHS made reasonable efforts to verify the accuracy and completeness of the information by requesting more detailed accounts, which resulted in the submission of the two amended reports, and by requesting additional information from the Hospital Center when the plaintiff raised additional arguments” (citation omitted)), summary affirmance granted per curiam, No. 12-5315, 2013 U.S. App. LEXIS 4857 (D.C. Cir. Mar. 11, 2013);

OVERVIEW OF THE PRIVACY ACT

Kvech v. Holder, No. 10-cv-545, 2011 WL 4369452, at *5-6 (D.D.C. Sept. 19, 2011) (concluding that plaintiff “has not asserted any facts to support a claim that the FBI failed to maintain accurate or complete records with reasonable fairness” where plaintiff “admit[ted] that she defended herself against the charges by submitting the very evidence she claims would have ‘corrected’ the records”); Crummey v. SSA, 794 F. Supp. 2d 46, 56-57 (D.D.C. 2011) (finding that “there can be no genuine dispute that the SSA has maintained its records ‘with the accuracy necessary to assure fairness’” where plaintiff had “failed to present even a scintilla of competent evidence suggesting that the SSA’s records are, in actuality, materially inaccurate or incomplete”), summary affirmance granted, No. 11-5231, 2012 WL 556317 (D.C. Cir. Feb. 6, 2012); Wilson v. CIA, No. 01-1758, slip op. at 6 (D.D.C. Aug. 29, 2002) (“No reasonable fact finder could accept plaintiff’s denial of a meeting having occurred twenty-five years ago over an official record prepared ‘less than two weeks’ after the meeting which memorialized the event.”), summary affirmance granted, No. 02-5282, 2003 U.S. App. LEXIS 1290 (D.C. Cir. Jan. 24, 2003); Halus v. Army, No. 87-4133, 1990 WL 121507, at *11 (E.D. Pa. Aug. 15, 1990) (holding erroneous information is not subject to amendment if it is merely a “picayune” and immaterial error); Jones v. Treasury, No. 82-2420, slip op. at 2-3 (D.D.C. Oct. 18, 1983) (ruling it reasonable for agency – without conducting its own investigation – to maintain record concerning unsubstantiated allegation of sexual misconduct by ATF agent conveyed to it by state and local authorities), aff’d, 744 F.2d 878 (D.C. Cir. 1984) (unpublished table decision); cf. Ramey v. Marshals Serv., 755 F. Supp. 2d 88, 97 (D.D.C. 2010) (finding that plaintiff who claimed that “the U.S. Marshals’s records which concluded that she [abandoned her post] are not accurate” had “not set forth specific facts showing a genuine issue for trial on the question of whether the U.S. Marshals relied on inaccurate information”); Powers v. Williams, No. CV 06-0665 (PLF), 2006 WL 8448057, at *3 (D.D.C. Nov. 17, 2006) (“As long as the Parole Commission complies with its procedures for conducting a parole hearing, it complies with the fairness standard set forth in 5 U.S.C. § 552a(e)(5).”); Griffin v. Ashcroft, No. 02-5399, 2003 WL 22097940, at *1 (D.C. Cir. Sept. 3, 2003) (per curiam) (finding that appellant had made no showing that facts regarding information in his presentence investigation report were inaccurate and “even if the information were inaccurate, appellant [had] not shown the BOP either had no grounds to believe maintaining the information was lawful or that it flagrantly disregarded his rights under the Privacy Act”); Sullivan v. BOP, No. 94-5218, 1995 WL 66711, at *1 (D.C. Cir. Jan. 17, 1995) (finding that “Parole Commission met the requirements of the Act by providing [plaintiff] with a parole revocation hearing at which he was represented by counsel and given the opportunity to refute the validity of his continued confinement”); Kirkland v. Gess-Valagobar, No. 1:08-CV-0239, 2008 WL 504394, at *4 (N.D. Ga. Feb. 21, 2008) (explaining that BOP properly included juvenile

record in presentence report because Sentencing Guidelines permit consideration of juvenile adjudications in some cases); Holz v. Westphal, 217 F. Supp. 2d 50, 56-57 (D.D.C. 2002) (finding that report of investigation was not “accurate or complete as to ensure its fairness to [individual],” and requiring removal of individual’s name from report of investigation when report contained notations of “Fatal Traffic Accident” and “Negligent Homicide” without further explanation, which thus suggested commission of crime even though individual was never found guilty of offense); Pons v. Treasury, No. 94-2250, 1998 U.S. Dist. LEXIS 5809, at *11-15 (D.D.C. Apr. 21, 1998) (entering judgment in favor of agency where agency presented “substantial evidence to suggest that [it] acted in the reasonable belief that there were no grounds to amend plaintiff’s records”; plaintiff failed to identify any records that contained alleged false statements and even if file did contain those statements, plaintiff never presented any evidence from which to conclude that statements were false); Smith v. BOP, No. 94-1798, 1996 WL 43556, at *3-4 (D.D.C. Jan. 31, 1996) (finding that plaintiff’s record was not inaccurate with respect to his pre-commitment status in light of BOP’s “full authority to promulgate rules governing the treatment and classification of prisoners” and “broad discretionary power,” and because there was “no evidence that the BOP’s interpretation of its own regulations was an abuse of discretion or discriminatorily administered,” “BOP officials reconsidered their decision at least once,” and “the determination of which plaintiff complains ha[d] been resolved in his favor”); Hampton v. FBI, No. 93-0816, slip op. at 3-6, 13-17 (D.D.C. June 30, 1995) (finding that FBI “acted lawfully under the Privacy Act in the maintenance of the plaintiff’s arrest record” when FBI refused to expunge challenged entries of arrests that did not result in conviction absent authorization by local law enforcement agencies that had originally submitted the information); Buxton v. Parole Comm’n, 844 F. Supp. 642, 644 (D. Or. 1994) (finding subsection (e)(5) fairness standard satisfied where Parole Commission complied with statutory procedures regarding parole hearings even though it did not investigate or correct alleged inaccuracies in presentence report).

Erroneous facts – as well as opinions, evaluations, and subjective judgments based entirely on erroneous facts – can be amended. See, e.g., Hewitt v. Grabicki, 794 F.2d 1373, 1378 (9th Cir. 1986); Westcott v. McHugh, 39 F. Supp. 3d 21, 27-33 (D.D.C. 2014); Rodgers v. Army, 676 F. Supp. 858, 860-61 (N.D. Ill. 1988); Ertell v. Army, 626 F. Supp. 903, 910-12 (C.D. Ill. 1986); R.R. v. Army, 482 F. Supp. 770, 773-74 (D.D.C. 1980); Murphy v. NSA, 2 Gov’t Disclosure Serv. (P-H) ¶ 81,389, at 82,036 (D.D.C. Sept. 29, 1981); Trinidad v. U.S. Civil Serv. Comm’n, 2 Gov’t Disclosure Serv. (P-H) ¶ 81,322, at 81,870-71 (N.D. Ill. Apr. 7, 1980); Turner v. Army, 447 F. Supp. 1207, 1213 (D.D.C. 1978), aff’d, 593 F.2d 1372 (D.C. Cir. 1979). As the Court of Appeals for the Seventh Circuit has noted, “[t]he Privacy Act merely requires an agency to attempt to keep accurate records,

and provides a remedy to a claimant who demonstrates that facts underlying judgments contained in his records have been discredited.” DeBold, 735 F.2d at 1040-41.

In addition, one court has held that where records contain disputed hearsay and reports from informants and unnamed parties, “the records are maintained with adequate fairness if they accurately reflect the nature of the evidence,” i.e., indicate that the information is a hearsay report from an unnamed informant. Graham v. Hawk, 857 F. Supp. 38, 40 (W.D. Tenn. 1994), aff’d, 59 F.3d 170 (6th Cir. 1995) (unpublished table decision); cf. Hass v. Air Force, 848 F. Supp. 926, 931 (D. Kan. 1994) (acknowledging possibility that agency relied upon incorrect information in making determination about plaintiff, finding still no Privacy Act violation because no evidence was suggested that information was recorded inaccurately).

Where agency records document judgements or evaluations based on a number of factors or a diverse set of facts, courts generally are reluctant to question the accuracy, relevance, timeliness, or completeness of those records.

As a general rule, courts are reluctant to disturb judgmental matters in an individual’s record when such judgments are based on a number of factors or when the factual predicates for a judgment or evaluation are diverse. As the D.C. Circuit has ruled, where a subjective evaluation is “based on a multitude of factors” and “there are various ways of characterizing some of the underlying [factual] events,” it is proper to retain and rely on the record. White v. OPM, 787 F.2d 660, 662 (D.C. Cir. 1986); see also Mueller v. Winter, 485 F.3d 1191, 1197 (D.C. Cir. 2007) (holding amendment claim to be “doom[ed]” where “subjective evaluation [was] based on a multitude of factors” and where “there [were] various ways of characterizing some of the underlying events”); Westcott, 39 F. Supp. 3d at 32 (“Even if the Court were to conclude that the plaintiff had established that the objectively verifiable facts contained in the Reprimand were false, several of the considerations cited by [the general] as factors influencing his decision” – such as the general’s perception of plaintiff’s attitude toward his duties – “are simply unassailable.”); Bernson v. ICC, 625 F. Supp. 10, 13 (D. Mass. 1984) (finding court cannot order amendment of opinions “to reflect the plaintiffs’ version of the facts”); cf. Phillips v. Widnall, No. 96-2099, 1997 WL 176394, at *2-3 (10th Cir. Apr. 14, 1997) (holding that appellant was not entitled to court-ordered amendment, nor award of damages, concerning record in her medical files that contained “physician’s notation to the effect that [appellant] was probably dependent upon a prescription medication,” as such notation “reflected the physician’s medical conclusion, which he based upon a number of

objective factors and [appellant's] own complaints of neck and low back pain," and "Privacy Act does not permit a court to alter documents that accurately reflect an agency decision, no matter how contestable the conclusion may be").

Courts have consistently determined that pure opinions and judgments do not require amendment to satisfy the subsection (e)(5) requirement.

Many courts have held that pure opinions and judgments are not subject to amendment. See, e.g., Barnett v. U.S., No. 15-1614 (BAH), 2016 WL 3350989 (D.D.C. June 15, 2016) (The Privacy Act is not "a vehicle for amending the judgments of federal officials . . . as those judgments are reflected in records maintained by federal agencies." (quoting Kleiman v. Energy, 956 F.2d 335, 337-38 (D.C. Cir. 1992))); see also Akl v. Sebelius, No. 12-5315, 2013 WL 1164488, at *1 (D.C. Cir. Mar. 11, 2013) (per curiam); Baker v. Winter, 210 F. App'x 16, 18 (D.C. Cir. 2006); Reinbold v. Evers, 187 F.3d 348, 361 (4th Cir. 1999); Hewitt, 794 F.2d at 1378-79; Blevins v. Plummer, 613 F.2d 767, 768 (9th Cir. 1980) (per curiam); Elhelbawy v. Pritzker, No. 14-cv-01707-CBS, 2015 WL 5535246 (D. Colo. Sept. 21, 2015); Hutton v. VA, No. 1:12CV190, 2013 WL 1331191, at *2 (M.D.N.C. Mar. 29, 2013); Middlebrooks v. Mabus, No. 1:11cv46, 2011 WL 4478686, at *5 (E.D. Va. Sept. 23, 2011); Feldman v. CIA, 797 F. Supp. 2d 29, 46-47 (D.D.C. 2011); Washington v. Donley, 802 F. Supp. 2d 539, 553-54 (D. Del. 2011); Kursar, 751 F. Supp. 2d at 170-71, aff'd per curiam, 442 F. App'x 565; Hardy v. McHugh, 692 F. Supp. 2d 76, 80 (D.D.C. 2010); Patel v. United States, No. CIV-08-1168, slip op. at 14-17 (W.D. Okla. Oct. 9, 2009) (magistrate's recommendation), adopted, 2009 WL 5168306 (W.D. Okla. Dec. 18, 2009), aff'd, 399 F. App'x 355, 360 (10th Cir. 2010); Register v. Lappin, No. 07-CV-136, 2007 WL 2020243, at *3 (E.D. Ky. July 6, 2007); Toolasprashad v. BOP, No. 04-3219, 2006 WL 2627931, at *4 (D.N.J. Sept. 13, 2006); Doyon v. DOJ, 304 F. Supp. 2d 32, 35 (D.D.C. 2004); Gowan v. Air Force, No. 90-94, slip op. at 28-30 (D.N.M. Sept. 1, 1995), aff'd, 148 F.3d 1182 (10th Cir. 1998); Webb, 880 F. Supp. at 25; Nolan v. DOJ, No. 89-A-2035, 1991 WL 134803, at *3 (D. Colo. July 17, 1991), appeal dismissed in pertinent part on procedural grounds, 973 F.2d 843 (10th Cir. 1992); Frobish v. Army, 766 F. Supp. 919, 926-27 (D. Kan. 1991); Daigneau v. United States, No. 88-54-D, slip op. at 3-4 (D.N.H. July 8, 1988); Brumley v. Labor, No. LR-C-87-437, slip op. at 4 (E.D. Ark. June 15, 1988), aff'd, 881 F.2d 1081 (8th Cir. 1989) (unpublished table decision); Rogers v. Labor, 607 F. Supp. 697, 699-700 (N.D. Cal. 1985); Fagot v. FDIC, 584 F. Supp. 1168, 1176 (D.P.R. 1984), aff'd in part & rev'd in part, 760 F.2d 252 (1st Cir. 1985) (unpublished table decision); cf. Strong v. OPM, 92 F. App'x 285, 289 (6th Cir. 2004) (finding that OPM did not violate Privacy Act by refusing to remove reference's statement as plaintiff failed to offer any evidence that reference's statement was inaccurate or irrelevant); Brim v. Copenhaver, No. 13-cv-00433, 2013 WL 5817990, at *7 (E.D. Cal. Oct. 29, 2013) ("Even if the Privacy Act were to

apply to court records, it appears that the BOP has complied with the statutory requirements because there is no indication that the BOP's files contain anything but true copies of the judgment and orders issued by the district court and the PSR as generated by the United States Probation Office."); Doe v. DOJ, 660 F. Supp. 2d 31, 43 (D.D.C. 2009) ("[P]laintiff's complaint objects to inaccurate 'conclusions drawn by lay employees' that were based on accurate records. . . . Thus, plaintiff objects not to erroneous . . . records but to misinterpretation of the records by DOJ employees, for which there is no remedy under the Privacy Act."); Davidson v. Daniels, No. 07-960, 2007 WL 3232608, at *2 (D. Or. Oct. 28, 2007) ("Respondent has no authority to alter court judgments. The correction of judgments [i]s the providence of the court."); Turner, 447 F. Supp. at 1212-13 (stating that rating "is a highly subjective process which requires the opinions and judgments of military professionals" and denying plaintiff's request, which was "in essence" that the court "determine de novo 'a fair and accurate' rating as to the 'quality' of his service").

The D.C. Circuit and a few district courts have found that agencies satisfy the subsection (e)(5) requirement by maintaining verifiable information; in the atypical case where information conflicts or the truth is not readily attainable, courts have assessed whether agencies maintained records in a fair and reasonable manner.

In determining what steps an agency must take in order to satisfy the accuracy standard of subsection (e)(5), the Court of Appeals for the District of Columbia Circuit has looked to whether the information at issue is capable of being verified. In Doe v. United States, 821 F.2d 694, 697-701 (D.C. Cir. 1987), the D.C. Circuit, sitting en banc, in a seven-to-four decision, held that the inclusion in a job applicant's record of both the applicant's and agency interviewer's conflicting versions of an interview (in which only they were present) satisfies subsection (e)(5)'s requirement of maintaining reasonably accurate records. In rejecting the argument that the agency and reviewing court must themselves make a credibility determination of which version of the interview to believe, the D.C. Circuit ruled that subsections (e)(5) and (g)(1)(C) "establish as the record-keeper's polestar, 'fairness' to the individual about whom information is gathered," and that "the 'fairness' criterion does not demand a credibility determination in the atypical circumstances of this case." Id. at 699 (emphasis added); see also Harris v USDA, 124 F. 3d 197 (6th Cir. 1997) (unpublished table decision) (ruling that agency "reasonably excluded" information from the plaintiff's record where there was "substantial evidence that the [information] was unreliable," and in the absence of "verifiable information which contradicted its investigators' records," the agency "reasonably kept and relied on the information gathered by its investigators when it terminated plaintiff"); Graham, 857 F. Supp. at 40 (asserting that agency was under no obligation to

resolve whether hearsay contained in report was true, so long as that information was characterized as hearsay); Doe v. FBI, No. 91-1252, slip op. at 6-7 (D.N.J. Feb. 27, 1992) (following Doe v. United States, 821 F.2d at 699, and holding that FBI fulfilled its obligations under Privacy Act by including plaintiff's objections to statements contained in FBI polygrapher's memorandum and by verifying to extent possible that polygraph was properly conducted).

Subsequently, the D.C. Circuit held that in a "typical" case, where the records at issue are "not ambivalent" and the facts described therein are "susceptible of proof," the agency and reviewing court must determine accuracy as to each filed item of information. Strang v. U.S. Arms Control & Disarmament Agency, 864 F.2d 859, 866 (D.C. Cir. 1989). In order to "assure fairness" and render the record "complete" under subsection (e)(5), an agency may even be required to include contrary or qualifying information. See Strang v. U.S. Arms Control & Disarmament Agency, 920 F.2d 30, 32 (D.C. Cir. 1990); Kassel v. VA, 709 F. Supp. 1194, 1204-05 (D.N.H. 1989).

Adhering to its holding in Strang, the D.C. Circuit later held:

As long as the information contained in an agency's files is capable of being verified, then, under sections (e)(5) and (g)(1)(C) of the Act, the agency must take reasonable steps to maintain the accuracy of the information to assure fairness to the individual. If the agency willfully or intentionally fails to maintain its records in that way and, as a result, it makes a determination adverse to an individual, then it will be liable to that person for money damages. . . . [T]he agency did not satisfy the requirements of the Privacy Act simply by noting in [the individual's] files that he disputed some of the information the files contained.

Sellers, 959 F.2d at 312. It is worth noting that Sellers was solely a subsection (e)(5)/(g)(1)(C) case; the system of records at issue was exempt from access under subsection (d). See also McCready v. Nicholson, 465 F.3d 1, 19 (D.C. Cir. 2006) (citing Sellers and Doe v. United States and remanding because court "fail[ed] to see how [plaintiff's] presence at a meeting is not a 'fact' capable of verification and why the [agency] need not correct that fact or show that it took reasonable steps to verify its accuracy"); Martinez v. BOP, 444 F.3d 620, 624 (D.C. Cir. 2006) (dicta) (explaining that BOP had contacted U.S. Parole Commission and U.S. Probation Office and was advised that BOP's records were accurate); Toolsprashad v. BOP, 286 F.3d 576, 583 (D.C. Cir. 2002) (citing Sellers and Doe v. United States and remanding so that "typicality issue" may be resolved and so that agency can prove inmate had "significant documented history of harassing and demeaning staff members"); Griffin v. Parole Comm'n, No. 97-5084, 1997

U.S. App. LEXIS 22401, at *3-5 (D.C. Cir. July 16, 1997) (citing Doe v. United States and Deters, and finding itself presented with “typical” case in which information was capable of verification; therefore vacating district court opinion that had characterized case as “atypical”), vacated & remanded No. 96-0342, 1997 U.S. Dist. LEXIS 2846 (D.D.C. Mar. 11, 1997); Deters, 85 F.3d at 658-59 (quoting Sellers and Doe v. United States, and although finding itself presented with “an atypical case because the ‘truth’ . . . is not readily ascertainable . . . assum[ing] without concluding that the Commission failed to maintain Deters’s records with sufficient accuracy,” because Commission had “not argued that this was an atypical case”); Hutton v. VA, No. 1:12CV190, 2013 WL 1331191, at *2 (M.D.N.C. Mar. 29, 2013) (“Because Plaintiff concedes in his Complaint that he was at one time a disabled veteran, there is no plausible basis for believing that the information that he seeks to have removed from his VA record, specifically, the ‘label’ of being a disabled veteran in the past, constitutes false or inaccurate information.”); Lopez v. Huff, 508 F. Supp. 2d 71, 77-78 (D.D.C. 2007) (finding that “BOP satisfied its [Privacy Act] obligations by contacting the appropriate [U.S. Probation Office] to verify the accuracy of the challenged information”); Brown v. Prob. Office, No. 03-872, 2005 WL 2284207, at *3 (E.D. Tex. Aug. 15, 2005) (concluding that BOP’s maintenance of inmate’s presentence report satisfied subsection (e)(5) because BOP “took affirmative steps to verify the information by contacting the state court and the probation officer who prepared the [report]”); Blazy, 979 F. Supp. at 20-21 (citing Sellers and Doe v. United States, and finding that alleged inaccuracies were either nonexistent, corrected, or “unverifiable opinions of supervisors, other employees and/or informants”); Bayless v. Parole Comm’n, No. 94CV0686, 1996 WL 525325, at *5 (D.D.C. Sept. 11, 1996) (citing Sellers and Doe v. United States, and finding itself presented with an “atypical” case because “truth concerning plaintiff[’]s culpability in the conspiracy and the weight of drugs attributed to him involves credibility determinations of trial witnesses and government informants and, therefore, is not ‘clearly provable’”); Webb, 880 F. Supp. at 25 (finding that record at issue contained “justified statements of opinion, not fact” and “[c]onsequently, they were not ‘capable of being verified’ as false and cannot be considered inaccurate statements” (quoting Sellers, 959 F.2d at 312, and citing Doe v. United States, 821 F.2d at 699)); Thomas v. Parole Comm’n, No. 94-0174, 1994 WL 487139, at *4-6 (D.D.C. Sept. 7, 1994) (discussing Doe v. United States, Strang, and Sellers, but finding that Parole Commission “verified the external ‘verifiable’ facts”; further holding that plaintiff should not be allowed to use Privacy Act “to collaterally attack the contents of his presentence report,” as he “originally had the opportunity to challenge the accuracy . . . before the judge who sentenced him”); Linneman, No. 89-505, slip op. at 11-22 (D.D.C. July 13, 1992) (applying Sellers and Doe v. United States to variety of items of which plaintiff sought amendment).

The D.C. Circuit has stated that subsection (e)(5) only requires an agency to address the accuracy of a record before using it to make a determination about an individual if the agency has no duty to amend the record pursuant to the Privacy Act's amendment provisions.

The D.C. Circuit has noted that where “an agency has no subsection (d) duty to amend, upon request, it is not clear what residual duty subsection (e)(5) imposes when an individual challenges the accuracy of a record.” Deters, 85 F.3d at 658 n.2. The court questioned whether subsection (e)(5) would still require an agency to amend or expunge a record upon the individual’s request, or whether the agency merely must “address the accuracy of the records at some point before using it to make a determination of consequence to the individual.” Id. Although stating that the Sellers opinion was “not entirely clear on this point,” the D.C. Circuit reasoned that “the language of subsection (e)(5) . . . suggests the latter course.” Id. (citing OMB 1975 Guidelines, 40 Fed. Reg. at 28,964 https://www.justice.gov/paoverview_omb-75). The court stated that subsection (e)(5) suggests that an agency has “no duty to act on an [individual’s] challenge and verify his record until the agency uses the record in making a determination affecting his rights, benefits, entitlements or opportunities,” 85 F.3d at 660; see also Bayless, 1996 WL 525325, at *6 n.19 (quoting Deters and determining that agency “fulfilled its requisite duty by ‘addressing’ plaintiff’s allegations prior to rendering a parole determination”); cf. Bassiouni v. FBI, No. 02-8918, 2003 WL 22227189, at *5 (N.D. Ill. Sept. 26, 2003) (holding that agency’s denial of request to amend alleged inaccurate records about plaintiff was in and of itself a “determination” under subsection (e)(5)), aff’d on other grounds, 436 F.3d 712 (7th Cir. 2006).

The Ninth Circuit Court of Appeals has held that an agency can comply with the subsection (e)(5) requirement by simply including a complainant’s rebuttal statements with the complainant’s records.

The Court of Appeals for the Ninth Circuit has held that an agency can comply with subsection (e)(5) by simply including a complainant’s rebuttal statement with an allegedly inaccurate record. Fendler v. BOP, 846 F.2d 550, 554 (9th Cir. 1988) (subsections (e)(5) and (g)(1)(C) lawsuit); see also Graham, 857 F. Supp. at 40 (citing Fendler and holding that where individual disputes accuracy of information that agency has characterized as hearsay, agency satisfies subsection (e)(5) by permitting individual to place rebuttal in file); cf. Harris, 124 F.3d at 197 (holding that although exclusion of information from appellant’s record due to unreliability of information was reasonable, it was “notabl[e]” that the appellant had not contested the district court’s finding that the agency “did not prevent him from adding to the file his disagreement with the [agency] investigators’

conclusions”). Fendler thus appears to conflict with both Doe v. United States and Strang, as well as with the D.C. Circuit’s earlier decision in Vymetalik v. FBI, 785 F.2d 1090, 1098 n.12 (D.C. Cir. 1986) (noting that subsection (d)(2) “guarantees an individual the right to demand that his or her records be amended if inaccurate” and that mere inclusion of rebuttal statement was not “intended to be [the] exclusive [remedy]”).

The Fifth Circuit and several other courts have held that to satisfy the subsection (e)(5) “timeliness” requirement, agencies must incorporate notes into a record at the time the records are used by the agency to make a determination about the individual.

In Chapman v. NASA, 682 F.2d 526, 528-30 (5th Cir. 1982), the Court of Appeals for the Fifth Circuit recognized a “timely incorporation” duty under subsection (e)(5). It ruled that a supervisor’s personal notes “evanesced” into Privacy Act records when they were used by the agency to effect an adverse disciplinary action, and that such records must be placed into the employee’s file “at the time of the next evaluation or report on the employee’s work status or performance.” Id. at 529. In reversing the district court’s ruling that such notes were not records within a system of records, the Fifth Circuit noted that such incorporation ensures fairness by allowing employees a meaningful opportunity to make refutatory notations, and avoids an “ambush” approach to maintaining records. Id.; see also Thompson v. DOT U.S. Coast Guard, 547 F. Supp. 274, 283-84 (S.D. Fla. 1982) (explaining Chapman). Chapman’s “timely incorporation” doctrine has been followed in several other cases. See, e.g., MacDonald v. VA, No. 87-544-CIV-T-15A, slip op. at 2-5 (M.D. Fla. Feb. 8, 1988) (stating that the counseling memorandum used in preparation of proficiency report “became” part of VA system of records); Lawrence v. Dole, No. 83-2876, slip op. at 5-6 (D.D.C. Dec. 12, 1985) (finding that notes not incorporated in timely manner cannot be used as basis for adverse employment action); cf. Hudson v. Reno, 103 F.3d 1193, 1205-06 & n.9 (6th Cir. 1997) (distinguishing facts in Chapman and holding that supervisor’s “notes about [p]laintiff’s misconduct which were kept in a locked drawer and labeled the ‘First Assistant’s’ files do not fall within th[e system of records] definition,” as they “were not used to make any determination with respect to [p]laintiff”); Manuel v. VA, 857 F.2d 1112, 1117-19 (6th Cir. 1988) (finding no duty to place records within system of records where records “are not part of an official agency investigation into activities of the individual requesting the records, and where the records requested do not have an adverse effect on the individual”); Magee v. United States, 903 F. Supp. 1022, 1029-30 (W.D. La. 1995) (finding plaintiff’s file kept in a supervisor’s desk, separate from other employee files, because of plaintiff’s concerns about access to it and with plaintiff’s acquiescence, did “not fall within the proscriptions of maintaining a ‘secret file’ under the Act”), aff’d, 79 F.3d 1145 (5th Cir. 1996) (unpublished table

decision).

The subsection (e)(5) requirement does not require agencies to maintain only the most recent information, but requires agencies to preserve records where the agency “reasonably foresees” use of the record.

Turning to the “timeliness” requirement of subsection (e)(5)’s “accuracy, relevance, timeliness, and completeness” standard, “timeliness” does not require that agency records contain only information that is “hot off the presses.” White v. OPM, 787 F.2d 660, 663 (D.C. Cir. 1986) (rejecting argument that use of year-old evaluation violates Act, as it “would be an unwarranted intrusion on the agency’s freedom to shape employment application procedures”); see also Beckett v. USPS, No. 88-802, slip op. at 12-14 (E.D. Va. July 3, 1989) (stating that “[a]ll of the record maintenance requirements of subsection 552a(e)(5), including timeliness, concern fairness,” and finding that as to records regarding “restricted sick leave,” “[w]iping the . . . slate clean after an employee has remained off the listing for only six months is not required to assure fairness to the individual”; also finding that maintenance of those records for six months after restricted sick leave had been rescinded “did not violate the relevancy requirement of subsection 552a(e)(5)”).

Agencies have a duty to preserve records where investigation and future litigation is “reasonably foreseeable.” See Gerlich v. DOJ, 659 F. Supp. 2d 1 (D.D.C. 2009), aff’d in part, rev’d in part & remanded, on other grounds, 711 F.3d 161 (D.C. Cir. 2013) (holding that summary judgment was inappropriately granted under subsections (e)(5) and (e)(7) claims and concluding “in light of the destruction of appellants’ records, that a permissive spoliation inference was warranted because the senior Department officials had a duty to preserve the annotated applications and internet printouts given that Department investigation and future litigation were reasonably foreseeable”). Agencies do not need to keep records indefinitely, however. The Court of Appeals for the Fourth Circuit has held that subsection (e)(5) is “not violated by the destruction of [a] record” that is destroyed “pursuant to [agency] records retention policy.” Vaughn v. Danzig, 18 F. App’x 122, 124-25 (4th Cir. 2001) (per curiam) (finding that where Navy maintained record at issue in its files “at the time of the adverse action,” the subsequent routine destruction of record was proper and, indeed, plaintiff “cited no authority” to show that “the Privacy Act requires that records be maintained in perpetuity”). Cf. Hunt v. VA, 888 F. Supp. 2d 48, 54 (D.D.C. 2012) (“Since plaintiff has not identified an agency record subject to testing for accuracy, the Court must deny his motion for summary judgment because he has not proffered any probative evidence of a Privacy Act violation.”), aff’d, 739 F.3d 706 (D.C. Cir. 2014); Cottrell v. Vilsack, 915 F. Supp. 2d 81, 91 (D.D.C. 2013)

(finding plaintiff had no subsection (e)(5) claim, stating that “[t]he Privacy Act does not require that [agencies] maintain computerized records of unapproved [agency program] applications”).

In addition to its accuracy and timeliness requirements, subsection (e)(5) requires agencies to reasonably maintain only records that are “relevant” to an agency determination about the individual.

Regarding the “relevance” prong of the “accuracy, relevance, timeliness, and completeness” standard, the District Court of the District of Columbia found that the inclusion of irrelevant documents in job candidates’ records was an appropriate basis for a subsection (e)(5) claim. See Gerlich v. DOJ, 659 F. Supp. 2d at 16. The plaintiffs, who had applied to work for the Justice Department, alleged that two members of the selection committee had taken the plaintiffs’ political and ideological associations into account in deselecting them for interviews. Id. at 6. Specifically, the plaintiffs alleged that one official “conducted Internet searches regarding candidates’ political and ideological affiliations, printed out such information when it revealed liberal associations and then attached the printouts and her own handwritten comments to the candidates’ applications in support of her recommendations to deselect them.” Id. The court noted that “[m]ost ‘adverse determination’ claims hinge on inaccurate or incomplete records.” Id. at 15. Here, however, the plaintiffs alleged that “irrelevant records (i.e., the records of their First Amendment activities) led to an adverse determination against them (i.e., deselection by the Screening Committee).” Id. The court rejected the Department’s argument that the plaintiffs’ failure to allege any inaccuracy was grounds for dismissal of plaintiffs’ (e)(5) claim: “By the plain language of (g)(1)(C), relevance stands on equal footing with accuracy, timeliness and completeness as a basis for pursuing money damages for an adverse determination.” Id. at 15-16. The court concluded that “plaintiffs have met their pleading burden with respect to their subsection (e)(5) claim” because they alleged “that they suffered an adverse determination (deselection/non-hiring), that DOJ maintained irrelevant records (regarding plaintiffs’ First Amendment activities) which undermined the fairness of the hiring process, that DOJ’s reliance on those records (or the reliance of its employees . . .) proximately caused the adverse determination, and that DOJ (again, through its employees . . .) acted intentionally or willfully in maintaining such records.” Id. at 16.

For a further discussion of subsection (e)(5), see OMB 1975 Guidelines, 40 Fed. Reg. at 28,964-65, https://www.justice.gov/paoverview_omb-75.

F. 5 U.S.C. § 552a(e)(6) - Review Records Prior to Dissemination

“Each agency that maintains a system of records shall –

...

(6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to [the subsection (b)(2) required FOIA disclosure exception], make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes.” 5 U.S.C. § 552a(e)(6).

Comment:

Prior to disseminating records, agencies must review them for accuracy, relevance, timeliness, and completeness.

Agencies are required to make a reasonable effort to review records prior to their dissemination. See NTEU v. IRS, 601 F. Supp. 1268, 1272 (D.D.C. 1985); see also Stewart v. FBI, No. 97-1595, slip op. at 4 (D. Or. Mar. 12, 1999) (holding (e)(6) was violated where agency failed to establish that it conducted reasonable efforts to ensure accuracy of information “of a factual nature” that was “capable of being verified”), withdrawn by stipulation as part of settlement, No. 97-1595, 2000 WL 739253 (D. Or. May 12, 2000); Gang v. Civil Serv. Comm’n, No. 76-1263, slip op. at 2-5 (D.D.C. May 10, 1977) (holding provision violated where agency failed to review personnel file to determine relevance and timeliness of dated material concerning political activities before disseminating it to Library of Congress).

Statements of opinion or judgment generally are not covered by the subsection (e)(6) requirement.

The District Court for the District of Columbia has held that an agency was not liable under subsection (e)(6) for damages for the dissemination of information that plaintiff had claimed was inaccurate but that the court determined consisted of statements of opinion and subjective evaluation that were not subject to amendment. Webb v. Magaw, 880 F. Supp. 20, 25 (D.D.C. 1995); see also Pontecorvo v. FBI, No. 00-1511, slip op. at 20 (D.D.C. Sept. 30, 2001) (finding that “if the information gathered and contained within an individual’s background records is the subjective opinion of witnesses, it is incapable of being verified as false and cannot constitute inaccurate statements under the Privacy Act”); cf. Bhatia v. Office of the U.S. Attorney, N. Dist. of Cal., No. C 09-5581, 2011 WL 1298763, at *6-7 (N.D. Cal. Mar. 29, 2011) (holding plaintiff failed to state a claim under § 552a(e)(6) because “the documents cited by [plaintiff do] not establish that the allegations in the pending criminal indictment are inaccurate”), aff’d,

507 F. App'x 649 (9th Cir. 2013); Doe v. DOJ, 660 F. Supp. 2d 31, 43 (D.D.C. 2009) (concluding that “[b]ecause plaintiff has failed to show that there was an ‘error in the records,’ . . . he cannot succeed under . . . (e)(6)’”).

Some courts have utilized the “intentional and willful” standard for damages suits in assessing agency compliance with the subsection (e)(6) requirement.

Other district courts considering claims under subsection (e)(6), have taken into account the requirements of causation and intentional and willful wrongdoing in Privacy Act damages actions, discussed below. Guccione v. Nat’l Indian Gaming Comm’n, No. 98-CV-164, 1999 U.S. Dist. LEXIS 15475, at *14-19 (S.D. Cal. Aug. 5, 1999). The court found that an administrative hearing concerning inconsistencies in plaintiff’s employment application “smacked generally of reprimand even though no talismanic phrases akin to reprimand were used,” and that therefore “there was no ‘intentional’ or ‘willful’ misconduct in the [agency’s] use of the term reprimand,” nor was there sufficient causation where the recipients of the information also had reviewed the transcript of the administrative hearing and could draw their own conclusions. Id. at *16-19; see also Conyers v. VA, No. 16-CV-00013, 2018 WL 1867106, at *11 (E.D. N.Y. Jan. 29, 2018) (holding plaintiff failed to state a claim under section 552a(e)(6) because plaintiff failed to “set forth allegations that the Department personnel with whom he had contact dealt, acted, or failed to act, in such a ‘patently egregious and unlawful [manner]’ so as to have ‘known the conduct . . . [was] unlawful.’ Plaintiff, at best, alleges ‘administrative error’ for which the Privacy Act does not provide relief” (internal citations omitted); Kelley v. FBI, No. 13-0825 (ABJ), 2014 WL 4523650 (D.D.C. Sept. 15, 2014) (holding plaintiff failed to state a claim upon which damages can be granted because the allegations “did not rise to the level of the flagrant and obvious disregard”).

The subsection (e)(6) requirement does not apply to intra- or inter-agency disclosures.

By its terms, this provision does not apply to intra- or inter-agency disclosures, see Lamb v. Millennium Challenge Corp., 228 F. Supp. 3d 28 (D.D.C. 2017) (holding “[t]he statutory language makes clear that [section 552a(e)(6)] does not apply when information is disclosed within the agency or to another agency.” (internal citations omitted)); see also Elhelbawy v. Pritzker, No. 14-cv-01707-CBS, 2015 WL 5535246 (D. Colo. Sept. 21, 2015); Singh v. DHS, No. 1:12-cv-00498, 2013 WL 1704296, at *22-23 (E.D. Cal. Apr. 19, 2013); Thompson v. State, 400 F. Supp. 2d 1, 21-22 (D.D.C. 2005), or to mandatory FOIA disclosures, see Smith v. United States, 817 F.2d 86, 87 (10th Cir. 1987); Kassel v. VA, 709 F. Supp. 1194, 1205 & n.5 (D.N.H. 1989); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,965, https://www.justice.gov/paoverview_omb-75.

The subsection (e)(6) requirement is not superseded by regulations governing the National Practitioners' Data Bank promulgated in accordance with the Health Care Quality Improvement Act.

In addition, the District Court for the District of Columbia has concluded that regulations promulgated by the Department of Health and Human Services pursuant to the Health Care Quality Improvement Act, which concern collection and dissemination of information contained in the National Practitioners' Data Bank, do not supersede the more stringent protections provided by subsection (e)(6) of the Privacy Act. Doe v. Thompson, 332 F. Supp. 2d 124, 129-32 (D.D.C. 2004).

G. 5 U.S.C. § 552a(e)(7) - Record Describing the Exercise of Rights Guaranteed by the First Amendment

Each agency that maintains a system of records shall --

...

(7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." 5 U.S.C. § 552a(e)(7).

Comment:

Generally, agencies are prohibited from maintaining records about individuals' First Amendment activities. The OMB 1975 Guidelines advise agencies determining whether a particular activity constitutes exercise of a right guaranteed by the First Amendment to "apply the broadest reasonable interpretation." 40 Fed. Reg. at 28,965, https://www.justice.gov/paoverview_omb-75; see also 120 Cong. Rec. at 40,406, reprinted in Source Book at 860, https://www.justice.gov/opcl/paoverview_sourcebook.

Records do not need to be in a system of records to be covered by the subsection (e)(7) requirement, but must meet the definition of a "record" in accordance with the Privacy Act.

The record at issue need not be within a system of records to violate subsection (e)(7). See Maydak v. United States, 363 F.3d 512, 516-20 (D.C. Cir. 2004); MacPherson v. IRS, 803 F.2d 479, 481 (9th Cir. 1986); Boyd v. Sec'y of the Navy, 709 F.2d 684, 687 (11th Cir. 1983) (per curiam); Clarkson v. IRS, 678 F.2d 1368, 1373-77 (11th Cir. 1982); Albright v. United States, 631 F.2d 915, 918-20 (D.C. Cir.

1980); Gerlich v. DOJ, 659 F. Supp. 2d 1, 13-15 (D.D.C. 2009), aff'd in part, rev'd in part & remanded, on other grounds, 711 F.3d 161 (D.C. Cir. 2013); McCready v. Principi, 297 F. Supp. 2d 178, 187 (D.D.C. 2003), aff'd in part & rev'd in part on other grounds sub nom. McCready v. Nicholson, 465 F.3d 1 (D.C. Cir. 2006). See also the discussion under "Definitions, System of Records, Protections for Records not within a System of Records," above.

That said, the information at issue must meet the "record" definition under the Privacy Act for subsection (e)(7) to be applicable. See e.g., Houghton v. State, 875 F. Supp. 2d 22, 31-32 (D.D.C. 2012) (finding that transcripts containing reference to plaintiff's work were not "about" plaintiff, and therefore, not record under Privacy Act to implicate application of subsection (e)(7)); Iqbal v. FBI, No. 3:11-cv-369, 2012 WL 2366634, at *5 (M.D. Fla. June 21, 2012) (finding allegation in complaint that stated "the agents [took] notes to aid the creation of official reports" sufficient to "satisfy the requirement that the agency maintain[ed] a record" in order to invoke application of subsection (e)(7)).

The record must implicate the individual's First Amendment rights to be within the scope of the subsection (e)(7) requirement.

The record at issue "must implicate an individual's First Amendment rights." Boyd, 709 F.2d at 684; accord Banks v. Garrett, 901 F.2d 1084, 1089 (Fed. Cir. 1990); see also Elnashar v. DOJ, 446 F.3d 792, 794-95 (8th Cir. 2006) (explaining that plaintiff "failed to identify how his First Amendment rights were implicated" when FBI contacted him "to determine whether he had expertise with chemical weapons"); Reuber v. United States, 829 F.2d 133, 142-43 (D.C. Cir. 1987) (noting threshold requirement that record itself must describe First Amendment-protected activity); Gerlich, 659 F. Supp. 2d at 13-15 (same); Pototsky v. Navy, 717 F. Supp. 2d 20, 22 (D. Mass. 1989) (same), aff'd, 907 F.2d 142 (1st Cir. 1990) (unpublished table decision).

Thus, subsection (e)(7) is not triggered unless the record describes First Amendment-protected activity. See e.g., Maydak, 363 F.3d at 516 (finding "it obvious that photographs of prisoners visiting with family, friends, and associates depict the exercise of associational rights protected by the First Amendment"); England v. Comm'r, 798 F.2d 350, 352-53 (9th Cir. 1986) (finding record identifying individual as having "tax protester" status does not describe how individual exercises First Amendment rights); Iqbal, 2012 WL 2366634, at *5 (holding allegation that FBI "agents were monitoring [plaintiff] during prayer and later commented on those prayers" was "sufficient (if barely so) to support an inference that the notes maintained by the FBI implicated [plaintiff's] exercise of his First Amendment rights."); Jacobs v. NSA, No. 19-CV-3439, 2019 WL

7168626, at *1 (D.D.C. Dec. 24, 2019) (finding no violation where the plaintiff's "[c]omplaint contains no factual allegations from which the Court could conclude that the NSA illegally recorded protected speech"); Kvech v. Holder, No. 10-cv-545, 2011 WL 4369452, at *6 (D.D.C. Sept. 19, 2011) (citing Maydak and finding argument that "the non-marital, non-familial relationship between [plaintiff] and the detective is not the type protected as freedom of expression under the First Amendment" to be "contrary to precedent"); Ramey v. Marshals Serv., 755 F. Supp. 2d 88, 97-98 (D.D.C. 2010) ("[Plaintiff's] statements to the Chief Judge were made in the course of her duties as a [court security officer] and receive no First Amendment protection."); Gerlich, 659 F. Supp. 2d at 13 (holding that plaintiff job applicants "met their pleading burden" where they alleged that agency official "conducted Internet searches regarding applicants' political and ideological affiliations" and "either created printouts of such information or made written comments on the applications throughout the process concerning the liberal affiliations of candidates"); Krieger v. DOJ, 529 F. Supp. 2d 29, 51-52 (D.D.C. 2008) (finding that documents announcing speeches to be given by plaintiff and complaints filed by plaintiff against his former law firm described how plaintiff exercises First Amendment rights); Weeden v. Frank, No. 1:91CV0016, slip op. at 7-8 (N.D. Ohio Apr. 10, 1992) (asserting that to read subsection (e)(7) as requiring a privacy waiver for the agency to even file plaintiff's request for religious accommodation is "a broad and unreasonable interpretation of subsection (e)(7)"; however, agency would need to obtain waiver to collect information in order to verify plaintiff's exercise of religious beliefs), aff'd, 16 F.3d 1223 (6th Cir. 1994) (unpublished table decision). Cf. Hartley v. Wilfert, 918 F. Supp. 2d 45, 54-56 (D.D.C. 2013) (concluding that Secret Service officer's "actions here did not involve the sort of collection of information contemplated by the Act; instead, his words were merely a threat to intimidate [plaintiff] from continuing in her speech" where officer informed demonstrator that if she remained on sidewalk in front of White House she would have to provide certain items of information about herself and would be "added to the Secret Service list" and "considered one of the crazies who protest in front of the White House").

Agencies are permitted to maintain a record describing how any individual exercises rights guaranteed by the First Amendment if the agency is authorized by statute to maintain that record.

Assuming that the challenged record itself describes activity protected by the First Amendment, subsection (e)(7) is violated unless maintenance of the record fits into one of the enumerated exceptions. Specifically, agencies may maintain record describing how any individual exercises rights guaranteed by the First Amendment "expressly authorized by statute." See, e.g., Abernethy v. IRS, 909

F. Supp. 1562, 1570 (N.D. Ga. 1995) (finding IRS “authorized by statute” to maintain copies of documents relevant to processing of plaintiff’s requests under FOIA and Privacy Act, which both “provide implied authorization to federal agencies to maintain copies for their own records of the documents which are released to requesters under those Acts”), aff’d per curiam, No. 95-9489 (11th Cir. Feb. 13, 1997); Hass v. Air Force, 848 F. Supp. 926, 930-31 (D. Kan. 1994) (finding agency’s maintenance of FOIA and Privacy Act requests “cannot logically violate the Privacy Act”); OMB 1975 Guidelines, 40 Fed. Reg. at 28,965, https://www.justice.gov/paoverview_omb-75 (Immigration and Nationality Act); cf. Abernethy, 909 F. Supp. at 1570 (finding maintenance of documents in congressional communications files “does not violate the Privacy Act” because IRS “must respond to Congressional inquiries” and maintenance was necessary to carry out that responsibility (citing Internal Revenue Manual 1 (15) 29, Chapter 500, Congressional Communications)); Gang v. U.S. Civil Serv. Comm’n, No. 76-1263, slip op. at 5-7 & n.5 (D.D.C. May 10, 1977) (recognizing that 5 U.S.C. § 7311, which prohibits individual from holding position with federal government if he advocates – or is member of organization that he knows advocates – overthrow of government, may be read together with subsection (e)(7) as permitting maintenance of files relating to membership in such groups, but ruling that “it cannot fairly be read to permit wholesale maintenance of all materials relating to political beliefs, association, and religion”; nor does 5 U.S.C. § 3301, which authorizes President to ascertain fitness of federal applicants for employment as to character, provide authorization for maintenance of such information).

Agencies are permitted to maintain record describing how any individual exercises rights guaranteed by the First Amendment with the expressed consent of the individual on whom the record pertains.

Agencies may also maintain record describing how any individual exercises rights guaranteed by the First Amendment if “expressly authorized . . . by the individual about whom the record is maintained.” See Abernethy, 909 F. Supp. at 1570 (“Plaintiff authorized the maintenance of the documents at issue by submitting copies to various components of the Defendant IRS.”); OMB 1975 Guidelines, 40 Fed. Reg. at 28,965, https://www.justice.gov/paoverview_omb-75 (“volunteered” information is properly maintained); see also Radford v. SSA, No. 81-4099, slip op. at 4-5 (D. Kan. July 11, 1985) (finding plaintiff’s publication of contents of offending record does not constitute “express authorization”); Murphy v. NSA, 2 Gov’t Disclosure Serv. (P-H) ¶ 81,389, at 82,036 (D.D.C. Sept. 29, 1981) (asserting consent to maintain may be withdrawn); cf. Weeden v. Frank, No. 93-3681, 1994 WL 47137, at *2 (6th Cir. Feb. 16, 1994) (finding reasonable Postal Service’s procedure requiring individual to expressly waive

subsection (e)(7) Privacy Act rights to allow agency to collect information regarding employee's exercise of religious beliefs so that accommodation could be established).

Agencies are permitted to maintain a record describing how any individual exercises rights guaranteed by the First Amendment that are pertinent to and within the scope of an authorized law enforcement activity; the circuits are split on the appropriate standard by which to determine if a record is pertinent to and within the scope of an authorized law enforcement activity.

Finally, agencies may maintain record describing how any individual exercises rights guaranteed by the First Amendment "pertinent to and within the scope of an authorized law enforcement activity."

The Third, Sixth, and D.C. Circuit Courts of Appeals have adopted a "relevance" standard to assess whether information is within the scope of the "law enforcement activity" exception. See Patterson v. FBI, 893 F.2d 595, 602-03 (3d Cir. 1990) (affirming dismissal of student's subsection (e)(7) claim, and concluding that a standard of "relevance" to a lawful law enforcement activity is "more consistent with Congress's intent and will prove to be a more manageable standard than employing one based on ad-hoc review"); Jabara v. Webster, 691 F.2d 272, 279-80 (6th Cir. 1982) (holding that FBI's overseas surveillance records were "relevant to an authorized criminal investigation or to an authorized intelligence or administrative one"); Sieverding v. U.S. Dep't of Justice, 693 F. Supp. 2d 93, 105 (D.D.C. 2010), aff'd, No. 13-5060, 2013 WL 6801184 (D.C. Cir. Dec. 11, 2013), aff'd, No. 13-5060, 2013 WL 6801184 (D.C. Cir. Dec. 11, 2013) (to be excepted from 5 U.S.C. § 552a(e)(7), records need only be "relevant to an authorized criminal investigation or to an authorized intelligence or administrative one." Nagel v. HEW, 725 F.2d 1438, 1441 n.3 (D.C. Cir. 1984) (quoting Jabara, 691 F.2d at 280).

The Courts of Appeals for the Eleventh and the Ninth Circuits adopted narrower standards, however. See MacPherson v. IRS, 803 F.2d at 482-85 (ruling ruled that applicability of exception could be assessed only on "individual, case-by-case basis" and that "hard and fast standard" was inappropriate, but concluding that agency appropriately maintained notes and purchased tapes of tax protester's speech as "necessary to give the [IRS and Justice Department] a complete and representative picture of the events," notwithstanding that no investigation of specific violation of law was involved and no past, present, or anticipated illegal conduct was revealed or even suspected); Clarkson v. IRS, 678 F.2d at 1374-75 (Eleventh Circuit quoted with approval standard set forth by district court decision in Jabara (subsequently vacated and remanded by Sixth Circuit) and

held that exception does not apply if record is “unconnected to any investigation of past, present or anticipated violations of statutes [the agency] is authorized to enforce”).

The circuits also are split on how long a record describing an individual’s First Amendment activities continue to be “pertinent” to an authorized law enforcement investigation.

The circuits have generally interpreted the law enforcement exception broadly and concluded that it applies to closed investigative files. For example, the Court of Appeals for the District of Columbia Circuit interpreted the law enforcement exception in a closed investigation and concluded that, because “[m]aterials may continue to be relevant to a law enforcement activity long after a particular investigation undertaken pursuant to that activity has been closed,” “[i]nformation that was pertinent to an authorized law enforcement activity when collected does not later lose its pertinence to that activity simply because the information is not of current interest (let alone ‘necessity’) to the agency.” L. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 602-03 (D.C. Cir. 1996). The panel majority held that the Privacy Act does not require an agency to expunge records when they are no longer pertinent to a current law enforcement activity. Id. at 605; see also Afifi v. Lynch, 101 F. Supp. 3d 90, 107 (D.D.C. 2015) (finding that closed investigation of plaintiff did not render FBI records invalid under section (e)(7) because records may permit “the FBI to verify or evaluate any new intelligence received, assess the reliability of other sources, and ensure accountability regarding how the FBI responded to the information it received”); Bassiouni v. FBI, 436 F.3d 712, 724-25 (7th Cir. 2006) (rejecting plaintiff’s argument in national security context that FBI must be “currently involved in law enforcement investigation” for exception to apply, concluding that FBI was not required “to purge, on a continuous basis, properly collected information with respect to individuals that the agency has good reason to believe may be relevant on a continuing basis in the fulfillment of the agency’s statutory responsibilities”).

The Court of Appeals for the Seventh Circuit addressed the law enforcement exception in the context of national security and reached a conclusion similar to that in MacArthur. See Bassiouni v. FBI, 436 F.3d at 723-25. At issue in Bassiouni was whether the law enforcement exception covered the FBI’s maintenance of records pertaining to a law professor who once presided over two Arab-American associations. 436 F.3d at 724. The court found that records maintained by the FBI for the purpose of national security (specifically, intelligence related to international terrorism) was within subsection (e)(7)’s law enforcement activity exception even though the FBI was not at the time involved

in a law enforcement activity or investigation. Id. at 723-25. The court reached its decision based on the FBI's assertion that it needed to maintain the records because (1) the FBI had amended its investigative activities to make protection of the United States against terrorist attack its top priority, (2) the FBI anticipated "that it [would] continue to receive information about [the plaintiff]" owing to "the nature of these investigative activities" and "the breadth of [the plaintiff's] contacts with the Middle East," and (3) "the records [were] important for evaluating the continued reliability of [the FBI's] intelligence sources." Id. at 724. The court opined that these purposes "fall within 'authorized law enforcement activity' conducted by the FBI," noting that "the realm of national security belongs to the executive branch, and we owe considerable deference to that branch's assessment in matters of national security." Id.

Other courts have taken a similar approach in the national security context. Palmieri v. United States, 896 F.3d 579, 585-86 (D.C. Cir. 2018) (holding that Naval Criminal Investigative Service did not violate subsection (e)(7) when it assembled records concerning a government contractor's exercise of his First Amendment activities, including his associations and travel with Syrian nationals, and quoting Maydak, 363 F.3d at 517, to conclude that "law enforcement activities" is "interpreted . . . broadly to include an authorized criminal, intelligence, or administrative investigation") (internal citation and quotation marks omitted).

The Ninth Circuit, however, recently held that "unless a record is pertinent to an ongoing authorized law enforcement activity, an agency may not maintain it under § (e)(7) of the Privacy Act." Garris v. FBI, 937 F.3d at 1288 (9th Cir. 2019). As the term "maintain" is defined by the Privacy Act to include both maintain and collect, the court strictly interpreted subsection (e)(7) to read that the record at issue must be pertinent to an authorized law enforcement activity both at the time of collection and at the time of maintenance. Id. at 1295. The court further found that its interpretation was consistent with its findings and holding in MacPherson, 803 F.2d at 481-84, which upheld the maintenance of MacPherson's public speeches on tax protests, and also Becker v. IRS, 34 F.3d 398, 409 (7th Cir. 1994), where the 7th Circuit held that the IRS did not sufficiently justify the maintenance of documents in Becker's files. Id. at 1296. The court in Garris also relied on Bassiouni, at 724-25, which concluded that the FBI's continued maintenance of records describing Bassiouni's First Amendment activities did not violate § (e)(7) of the Privacy Act, because "the act ha[d] no separate and distinct maintenance requirement, but rather . . . the records were of *continuing relevance* to an authorized law enforcement activity." Id.

Finally, the Ninth Circuit in Garris distinguished the D.C. Circuit's decision in J.

Roderick MacArthur Found., 102 F.3d 600, finding that the verb “maintain” is “pertinent to and within the scope of an authorized law enforcement activity” exception, and not just to the record itself. Id. at 1297. The court in Garris reasoned that first, “the ‘pertinent to ... an authorized law enforcement activity’ clause does not modify only the noun ‘record,’ because the noun ‘record’ cannot be divorced from the verb ‘maintain’; second, the D.C. Circuit majority’s reading also requires reading into the text words not written by Congress, that is, by inserting the record is before ‘pertinent to and within the scope of an authorized law enforcement activity,’ rather than relying on the word “maintain” at the beginning of the (e)(7), which is a term explicitly defined in the Privacy Act; and third, Congress demonstrated its ability to limit certain provisions of the Privacy Act to only to collection, and not maintenance, as shown in subsections (e)(2), (k)(2), and (k)(5). Id. at 1297-98. Although the investigation into Garris had concluded, the court found that the retention of the FBI memo on Garris could still be pertinent to an unauthorized law enforcement activity. Id. at 1298. The court concluded though that the FBI memo and threat assessment herein did not reveal a threat to national security, any direct nexus to terrorism, or a threat of compromising current FBI investigations, and did not show was relevant to a broader authorized law enforcement activity that might require its maintenance. Id. In closing, the court in Garris stated the following:

Thus, we hold that to maintain a record, the government must demonstrate that the maintenance of the record is pertinent to a specific authorized law enforcement activity. We want to be exceedingly clear. We are not holding that whenever an agency closes an investigation, the agency must expunge the file because the law enforcement activity for which the record was created (or received) has ended. What we are holding is that, if the investigation is closed (or even if it is not), and if the government cannot articulate a sufficient law enforcement activity to which the maintenance of the record is pertinent, the maintenance of the record violates the Privacy Act. The reason for maintenance, so long as it is valid and not pretextual, need not be the same reason the record was created. Thus, in plenty of cases, the end of an investigation will not require a record to be expunged because the maintenance of the record will have some pertinence to an articulable, authorized law enforcement activity ... Maintenance for maintenance's sake, without pertinence to national security or other authorized law enforcement activity, is precisely what the Act was intended to prevent.

Id. at 1300; see also Becker v. IRS, 34 F.3d at 407-09 (adopting strict application of law enforcement exception by ordering IRS to expunge information in closed investigative file because court determined after in camera inspection that it

could not “be helpful in future enforcement activity;” court, however, appeared to confusingly engraft the timeliness requirement of subsection (e)(5) onto subsection (e)(7) and to confuse access under subsection (k)(2) with requirements of subsection (e)(7)); cf. J. Roderick MacArthur Found. v. FBI, 102 F.3d 600, 607 (D.C. Cir. 1996) (Tatel, J., dissenting) (opining in favor of requirement that information be maintained only if pertinent to current law enforcement activity).

Courts have upheld the subsection (e)(7) law enforcement exception in numerous and varied law enforcement contexts.

The courts have upheld the law enforcement exception’s applicability in a variety of contexts. See Doe v. FBI, 936 F.2d 1346, 1354-55, 1360-61 (D.C. Cir. 1991) (holding that appellant was foreclosed from obtaining relief because he had “not suffered any adverse effect,” and (e)(7) was not violated because law enforcement exception applied to FBI records concerning investigation of appellant’s “unauthorized possession of an explosive device” and reported advocacy of “violent overthrow of the Government”); Wabun-Inini v. Sessions, 900 F.2d 1231, 1245-46 (8th Cir. 1990) (discussing FBI maintenance of photographs seized with probable cause); Lochen v. VA, No. 88-6138, slip op. at 6-7 (9th Cir. Apr. 5, 1989) (discussing VA evaluative report concerning operation of VA facility and job performance of public employee that contained remarks by plaintiff); Nagel v. HEW, 725 F.2d 1438, 1441 & n.3 (D.C. Cir. 1984) (citing Labara with approval and holding that records describing statements made by employees while at work were properly maintained “for evaluative or disciplinary purposes”); Smith v. B A Blackmon Warden FCI Marianna, No. 5:18cv40, 2019 WL 3047081, at *7 (N.D. Fla. May 21, 2019) (holding that incident reports prepared as part of Bureau of Prison’s inmate disciplinary process, which is clearly central to BOP’s law enforcement mission in maintaining security and good order within institutions, falls within scope of its authorized law enforcement activity as permitted by subsection (e)(7)); Falwell v. Exec. Office of the President, 158 F. Supp. 2d 734, 742-43 (W.D. Va. 2001) (holding that FBI did not violate subsection (e)(7) by maintaining document entitled “The New Right Humanitarians” in its files, “because the document pertained to and was within the scope of a duly authorized FBI counterintelligence investigation” of Communist Party USA); Abernethy, 909 F. Supp. at 1566, 1570 (holding that maintenance of documents that quoted plaintiff on subject of reverse discrimination were “relevant to and pertinent to authorized law enforcement activities” in file pertaining to EEO complaint, that documents were kept due to belief that conflict of interest might exist through plaintiff’s representation of complainant and, citing Nagel, that maintenance was “valid” in files concerning possible disciplinary action against plaintiff); Maki v. Sessions, No. 1:90-CV-587,

1991 U.S. Dist. LEXIS 7103, at *27-28 (W.D. Mich. May 29, 1991) (holding that, although plaintiff claimed FBI investigation was illegal, uncontested evidence was that plaintiff was subject of authorized investigation by FBI); Kassel v. VA, No. 87-217-S, slip op. at 27-28 (D.N.H. Mar. 30, 1992) (citing Nagel and Jabara, inter alia, and holding that information about plaintiff's statements to media fell within ambit of administrative investigation); Pacheco v. FBI, 470 F. Supp. 1091, 1108 n.21 (D.P.R. 1979) (“[A]ll investigative files of the FBI fall under the exception.”); AFGE v. Schlesinger, 443 F. Supp. 431, 435 (D.D.C. 1978) (stating reasonable steps agencies take to prevent conflicts of interest are within exception); see also Scott v. Conley, 937 F. Supp. 2d 60, 80-82 (D.D.C. 2013) (dismissing former federal prisoner's subsection (e)(7) claim based on BOP's maintenance of records of his phone calls and other communications after his release as plaintiff never alleged facts to suggest BOP's maintenance lacked a law enforcement purpose when collected and noting that “the passage of time does not cause records to lose their relevance to law enforcement activity”); Felsen v. HHS, No. 95-975, slip op. at 68-72 (D. Md. Sept. 30, 1998) (finding no violation of subsection (e)(7) where report was relevant to authorized law enforcement activity of HHS and also was related to possible past violation of statute that HHS is empowered to enforce).

Courts have not upheld the subsection (e)(7) law enforcement exception where agencies failed to demonstrate a link between the records and an authorized law enforcement investigation.

However, some courts have not upheld the use of this exception where there does not appear to be a link between the records and an investigation. See Garcia v. Pompeo, No. 1:18-CV-01822, 2020 WL 134865, at *10 (D.D.C. Jan. 13, 2020) (denying State's motion to dismiss where the agency did not provide “any affidavits or declarations that would give the court insight into the purpose for which the information about Plaintiff was collected and maintained,” and whether the information was “connected to a security certification investigation” such that it fell within the law enforcement exception); Patel v. Bureau of Prisons, 125 F. Supp. 3d 44, 58-59 (D.D.C. 2015) (finding that law enforcement exception did not apply to memorandum documenting prisoner's letter to local news station complaining about preferential inmate treatment absent evidence regarding how the alleged memorandum was actually prepared, maintained, or used); Iqbal v. DOJ, No. 3:11-cv-369-J-37, 2013 WL 5421952, at *4 (M.D. Fla. Sept. 26, 2013) (finding “unclear how records of [p]laintiff's religious practices might relate to [offense regarding fraud and false statements]”); Maydak, 363 F.3d at 516-17 (remanding to district court to determine whether portions of BOP's declarations stating that certain institutions maintained and reviewed “photographs of prisoners visiting with family, friends and associates” for

“investigative and informative value” is consistent with subsection (e)(7)’s law enforcement exception); Levering v. Hinton, No. 2:07-CV-989, 2008 WL 4425961, at *8 (S.D. Ohio Sept. 25, 2008) (refusing to apply law enforcement exception to maintenance of “running record of practically all of Plaintiff’s speech at work”).

Finally, even if records are found to be maintained in violation of subsection (e)(7), it does not follow that those records must be disclosed. See Bassiouni v. CIA, 392 F.3d. 244, 247-48 (7th Cir. 2004); see also Irons v. Bell, 596 F.2d 468, 470-71 & n.4 (1st Cir. 1979).

H. 5 U.S.C. § 552a(e)(8) - Notice of Court Disclosure

“Each agency that maintains a system of records shall --

...

(8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record.” 5 U.S.C. § 552a(e)(8).

Comment:

This provision becomes applicable when subsection (b)(11) “court order” disclosures occur. See, e.g., Robinett v. State Farm Mut. Auto. Ins. Co., No. 02-0842, 2002 WL 31498992, at *3-4 (E.D. La. Nov. 7, 2002), aff’d per curiam, 83 F. App’x 638 (5th Cir. 2003); Moore v. USPS, 609 F. Supp. 681, 682 (E.D.N.Y. 1985); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,965, https://www.justice.gov/paoverview_omb-75. By its terms, it requires notice not prior to the making of a legally compelled disclosure, but rather at the time that the process becomes a matter of public record. See Kassel v. VA, No. 87-217-S, slip op. at 30 (D.N.H. Mar. 30, 1992); see also Moore, 609 F. Supp. at 682 (stating that the Privacy Act “§ 552a(e)(8) does not speak of advance notice of release”); cf. Mangino v. Army, No. 94-2067, 1994 WL 477260, at *11-12 (D. Kan. Aug. 24, 1994) (citing Moore for proposition that subsection (e)(8) does not require advance notice, although finding no allegation that disclosure at issue was made “under compulsory legal process”).

I. 5 U.S.C. § 552a(e)(9) - Rules of Conduct

“Each agency that maintains a system of records shall --

...

(9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the

requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance.” 5 U.S.C. § 552a(e)(9).

Comment:

Courts have given agencies deference on the manner by which they develop, and instruct their employees on, their rules of conduct to satisfy the subsection (e)(9) requirement.

Pursuant to this provision, agencies are required to establish rules of conduct governing the maintenance of systems of records but have broad latitude to determine what those rules of conduct will be so long as the rules are “reasonable.” “[A]gencies have broad discretion to [choose] among alternative methods of securing their records commensurate with their needs, objectives, procedures, and resources” and “[c]ivil liability is reserved for those lapses that constitute an extraordinary departure from standards of reasonable conduct.” Convertino v. DOJ, 769 F. Supp. 2d 139, 153 (D.D.C. 2011) (quoting Kostyu v. United States, 742 F. Supp. 413, 417 (E.D. Mich.1990)), rev’d and remanded on other grounds, 684 F.3d 93 (D.C. Cir. 2012) (reversing district court’s summary judgment and ruling that district court committed abuse of discretion in denying appellant’s motion to stay summary judgment to allow for further discovery).

In Convertino, the court concluded that the Privacy Act “only requires that each covered employee understand the proper handling of systems of records over which he or she has responsibility as well as records that he or she is responsible for maintaining” and “[j]ust because certain DOJ employees did not associate their knowledge and training regarding records system management with the words ‘Privacy Act’ does not mean that they were not, in fact, properly instructed in records system management.” Convertino v. DOJ, 769 F. Supp. 2d at 153-54; see also Doe v. DOJ, 660 F. Supp. 2d 31, 43 (D.D.C. 2009) (“[A]lthough plaintiff suggests that DOJ violated (e)(9) by failing to formally train [an agency employee], the Privacy Act does not specify how the agency must ‘instruct’ its personnel, and plaintiff has provided no support for his suggestion that listing rules and requirements on the Internet is inappropriate.” (citations omitted)); Fleury v. USPS, No. 00-5550, 2001 WL 964147, at *2 (E.D. Pa. Aug. 21, 2001) (finding that plaintiff’s “proof” that confidential information did not reach the intended recipient “would not establish that defendant failed to instruct supervisors and managers regarding Privacy Act requirements in violation of” 552a(e)(9)); but see Ciralsky v. CIA, 689 F. Supp. 2d 141, 159 (D.D.C. 2010) (denying DIA’s motion for summary judgment because if CIA handled plaintiffs records as alleged “it can be plausibly inferred that the CIA did not properly establish rules of conduct for and provide instruction to the responsible Agency

employees as required by § 552a(e)(9)'').

For additional discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,965, https://www.justice.gov/paoverview_omb-75.

J. 5 U.S.C. § 552a(e)(10) - Establish Safeguards

"Each agency that maintains a system of records shall --

...

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." 5 U.S.C. § 552a(e)(10).

Comment:

Some, but not all, courts have deferred to agencies on the manner by which they promulgate rules or implement administrative, technical, or physical safeguards to satisfy the subsection (e)(10) requirement.

This provision may come into play when documents are allegedly "leaked" or an agency allegedly fails to adequately safeguard documents. See, e.g., Pilon v. DOJ, 796 F. Supp. 7, 13 (D.D.C. 1992) (stating that because subsection (e)(10) is more specific than subsection (b), it governs with regard to allegedly inadequate safeguards that resulted in disclosure); Kostyu v. United States, 742 F. Supp. at 414-17 (finding alleged lapses in IRS document-security safeguards were not willful and intentional); cf. Paige v. DEA, 665 F.3d 1355, 1361 (D.C. Cir. 2012) (finding that even though plaintiff did not raise subsection (e)(10) claim at district court and finding no violation of subsection (b), stating "the widespread circulation of the accidental discharge video demonstrates the need for every federal agency to safeguard video records with extreme diligence in this internet age of iPhones and YouTube with their instantaneous and universal reach; DEA's treatment of the video-recording – particularly the creation of so many different versions and copies – undoubtedly increased the likelihood of disclosure and, although not an abuse of a system of records, is far from a model of agency treatment of private data").

Although section (e)(10) requires agencies to enact appropriate safeguards, "the Act does not prescribe specific technical standards, leaving the agencies to manage their own information security." Atkins v. Mabus, No. 12CV1390, 2014 WL 2705204, at *5,*7 (S.D. Cal. June 13, 2014) (finding plaintiff's evidentiary

showing regarding “appropriateness” of agency’s safeguards sufficient to withstand summary judgment, but ultimately granting summary judgment for agency because plaintiff failed to demonstrate willful or intentional failure to safeguard), rev’d & remanded on other grounds, 654 F. App’x 878 (9th Cir. 2016).

Similarly, where an agency has made efforts to promulgate rules or enact safeguards, the courts have generally relied on those steps as a sufficient agency defense. Dick v. Holder, 67 F. Supp. 3d 167, 186 (D.D.C. 2014) (granting motion to dismiss on basis that “DOJ, and by extension the FBI, has ‘promulgated extensive regulations . . . that safeguard its Privacy Act-protected records” and plaintiff “failed to identify any rule or safeguard that was breached or that should have been in place but was not” (quoting Doe v. DOJ, 660 F. Supp. 2d 31, 43 (D.D.C. 2009))); Thompson v. State, 400 F. Supp. 2d 1, 23 (D.D.C. 2005) (concluding that “a reasonable jury could not find that this failure amounted to a reckless disregard of plaintiff’s rights” where agency kept record “in a sealed envelope that was addressed to [plaintiff] and clearly marked ‘To Be Opened Only by Addressee,’” but did not “take the further precaution of keeping confidential information in a locked file cabinet” (internal quotation marks omitted)), aff’d, 210 F. App’x 5 (D.C. Cir. 2006) (unpublished tabled decision); see also Conyers v. VA, No. 16CV00013, 2018 WL 1867106, at *11 (E.D.N.Y. Jan. 29, 2018) (magistrate’s recommendation) (dismissing for failure to state claim because plaintiff “fail[ed] to identify any specific rule or regulation that the [VA] failed to develop or implement”) (citing Doe, 660 F. Supp. 2d at 43), adopted, (E.D.N.Y. Feb. 26, 2018); Delaittre v. Berryhill, No. C15-1905, 2017 WL 6310483, at *3, *5 (W.D. Wash. Dec. 11, 2017) (non-Privacy Act case rejecting plaintiff’s motion to lift confidentiality designations of documents citing agency’s obligations under (e)(10)). Another district court has held that conclusory allegations predicated on the fact that confidential information was forwarded to an unintended recipient are not sufficient to establish a subsection (e)(10) violation. See Fleury v. USPS, No. 00-5550, 2001 WL 964147, at *2 (E.D. Pa. Aug. 21, 2001).

Courts have found that repeated warnings of information security risks that go unheeded can be evidence of a willful or intentional failure to safeguard systems of records in accordance with the subsection (e)(10) requirement.

Even so, however, the agency’s authority is not without limits. For example, repeated warnings of information security risks that go unheeded are evidence of a willful or intentional failure to safeguard. Compare In re OPM Data Sec. Breach Litig., 928 F.3d 42, 64 (D.C. Cir. 2019) (OPM’s decision “to continue operating in the face of [] repeated and forceful [information security] warnings, without implementing even the basic steps needed to minimize the risk of a

significant data breach, is precisely the type of willful failure to establish appropriate safeguards that makes out a claim under the Privacy Act.”) and AFGE v. Hawley, 543 F. Supp. 2d 44, 52 (D.D.C. 2008) (finding that plaintiff “alleged “recurring, systemic, and fundamental deficiencies in [defendant’s] information security,” as demonstrated in an Office of Inspector General report, “if proven, would support a finding that defendants were warned of the deficiencies in their information security but failed to establish proper safeguards”), with Kelley v. FBI, 67 F. Supp. 3d 240, 263-64 (D.D.C. 2014) (finding that “citation of multiple [media] articles does not suffice to create an inference of intentional and willful failure to establish safeguards, especially since the entities involved already had several published safeguards in place.”). One district court has found that disclosures that are the result of “official decisions” by an agency “cannot be the basis for a claim under subsection (e)(10).” Chasse v. DOJ, No. 1:98-CV-207, slip op. at 16-17 (D. Vt. Jan. 14, 1999) (magistrate’s recommendation), adopted, (D. Vt. Feb. 9, 1999), aff’d on other grounds sub nom. Devine v. United States, 202 F.3d 547 (2d Cir. 2000).

Additionally, another district court held that a genuine issue of material fact existed as to whether the VA intentionally or willfully violated subsection (e)(10) by failing to install “patches” on its computer system to allow tracing of a user’s access to the social security numbers of certain employees. See Schmidt v. VA, 218 F.R.D. 619, 634-35 (E.D. Wis. 2003).

To establish that an agency violated the subsection (e)(10) requirement, an individual must establish an adverse effect and causation between the agency’s violation and the established adverse effect.

In order to state a claim under the Privacy Act for a violation of this subsection, plaintiffs must allege that an agency’s failure to comply “ha[d] an adverse effect” on him and establish a “causal connection between the agency violation and the adverse effect.” Lugo v. DOJ, 214 F. Supp. 3d 32, 41 (D.D.C. 2016), citing Doe v. DOJ, 660 F. Supp. 2d 31, 49 (D.D.C. 2009) (quoting Mandel v. OPM, 244 F. Supp. 2d 146, 153 (E.D.N.Y. 2003)), aff’d sub nom. Lugo v. DOJ, No. 16-5297, 2018 WL 1896491 (D.C. Cir. Apr. 3, 2018); accord Albright v. United States, 732 F.2d 181, 186 (D.C. Cir. 1984); see also 5 U.S.C. § 552a(g)(1)(D).

For a further discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,966, https://www.justice.gov/paoverview_omb-75, and “Civil Remedies, 5 U.S.C. § 552a(g)(1)(D) - Damages Lawsuits for Failure to Comply with Other Privacy Act Provisions” section, below.

K. 5 U.S.C. § 552a(e)(11) - Publish New or Intended Use

“Each agency that maintains a system of records shall --

...

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection [routine uses], publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency.” 5 U.S.C. § 552a(e)(11).

Comment:

For a discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,966, https://www.justice.gov/paoverview_omb-75.

AGENCY RULES

To implement the Privacy Act, “each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of [5 U.S.C. § 553, relating to notice and comment rulemaking].” 5 U.S.C. § 552a(f).

For examples of the DOJ’s Privacy Act regulations, see 28 C.F.R. Part 16, Subpart D (2020). For a case involving this section, see United States v. Tate, NMCCA 201200399, 2013 WL 951040, at *1 (Mar. 12, 2013) (setting aside a guilty finding of an individual who violated regulations DOD had promulgated to the Privacy Act regulations because the regulation is not punitive in nature).

Note also that subsection (f) provides that the Office of the Federal Register shall biennially compile and publish the rules outlined below and agency notices published under subsection (e)(4) in a form available to the public at low cost.

A. 5 U.S.C. § 552a(f)(1) - Establish Notification Procedures

“The rules shall –

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him.” 5 U.S.C. § 552a(f)(1).

Comment:

For a discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,967, https://www.justice.gov/paoverview_omb-75.

B. 5 U.S.C. § 552a(f)(2) - Define Time, Place, and Requirements for Identifying Individuals

“The rules shall –

...

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual.” 5 U.S.C. § 552a(f)(2).

Comment:

For a discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at

28,967, https://www.justice.gov/paoverview_omb-75.

C. 5 U.S.C. § 552a(f)(3) - Establish Procedures for Disclosure of Records to Individuals

“The rules shall –

...

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him.” 5 U.S.C. § 552a(f)(3).

Comment:

Many, but not all, courts have held that agency rules for the disclosure of medical records to an individual may not create, in effect, a new substantive exemption from accessing such medical records not otherwise authorized by the Privacy Act; agencies, however, have the freedom to promulgate special procedures to limit the potential harm from such access.

In the past, a typical regulation consistent with this provision would have allowed an agency to advise an individual requester that his medical records would be provided through a designated physician who would determine which records should be disclosed to the individual. However, as a result of a Court of Appeals for the District of Columbia Circuit opinion, Benavides v. BOP, 995 F.2d 269 (D.C. Cir. 1993), such regulations are no longer valid. In Benavides, the D.C. Circuit held that subsection (f)(3) is “strictly procedural . . . merely authoriz[ing] agencies to devise the manner in which they will disclose properly requested non-exempt records” and that “[a] regulation that expressly contemplates that the requesting individual may never see certain medical records [as a result of the discretion of the designated physician] is simply not a special procedure for disclosure to that person.” Id. at 272. The D.C. Circuit concluded that the Justice Department’s subsection (f)(3) regulation at issue, 28 C.F.R. § 16.43(d) (1992), “in effect, create[d] another substantive exemption” to Privacy Act access, and was, therefore, “ultra vires.” 995 F.2d at 272-73.

Nevertheless, the D.C. Circuit in Benavides rejected the argument that the Privacy Act requires direct disclosure of medical records to the individual. Recognizing the “potential harm that could result from unfettered access to medical and psychological records,” the court provided that “as long as agencies guarantee the ultimate disclosure of the medical records to the requesting individual . . . they should have freedom to craft special procedures to limit the

potential harm.” Id. at 273; accord Bavidó v. Apfel, 215 F.3d 743, 748-50 (7th Cir. 2000) (finding that the “Privacy Act clearly directs agencies to devise special procedures for disclosure of medical records in cases in which direct transmission could adversely affect a requesting individual,” but that “these procedures eventually must lead to disclosure of the records to the requesting individual”; further finding exhaustion “not required” because agency’s regulations “trapped” plaintiff by requiring him to “formally designate[] a representative” and “[t]o name such a representative would amount to conceding his case”); Melvin v. SSA, No. 5:09-CV-235, 2010 WL 1979880, at *5 & n.3 (E.D.N.C. May 13, 2010) (explaining that “SSA amended the regulation [at issue in Bavidó] in such a way that ensures the ultimate disclosure of records” and, therefore, allowing plaintiff to proceed with her Privacy Act claims), aff’d per curiam, 442 F. App’x 870 (4th Cir. 2011); cf. Simmons v. Reno, No. 97-2167, 1998 WL 964228, at *1 (6th Cir. Dec. 29, 1998) (citing Benavides and questioning district court’s reliance on SSA regulation that required designation of medical representative for receipt of all medical records), vacating & remanding No. 4:96CV214 (W.D. Mich. Sept. 30, 1997).

As a result of the Benavides decision, prior case law applying (and thus implicitly upholding) subsection (f)(3) regulations, such as the Justice Department’s former regulation on this point, is unreliable. See, e.g., Cowsen-El v. DOJ, 826 F. Supp. 532, 535-37 (D.D.C. 1992); Becher v. Demers, No. 91-C-99-S, 1991 WL 333708, at *4 (W.D. Wis. May 28, 1991); Sweatt v. Navy, 2 Gov’t Disclosure Serv. (P-H) ¶ 81,038, at 81,102 (D.D.C. Dec. 19, 1980), aff’d per curiam, 683 F.2d 420 (D.C. Cir. 1982).

Nevertheless, some courts, without addressing the holding in Benavides, have upheld the denial of access pursuant to agency regulations that require the designation of a representative to review medical records. See Hill v. Blevins, No. 3-CV-92-0859, slip op. at 5-7 (M.D. Pa. Apr. 12, 1993) (finding SSA procedure requiring designation of representative other than family member for receipt and review of medical and psychological information valid), aff’d, 19 F.3d 643 (3d Cir. 1994) (unpublished table decision); Besecker v. SSA, No. 91-C-4818, 1992 WL 32243, at *2 (N.D. Ill. Feb. 18, 1992) (dismissing for failure to exhaust administrative remedies where plaintiff failed to designate representative to receive medical records), aff’d, 48 F.3d 1221 (7th Cir. 1995) (unpublished table decision); cf. Polewsky v. SSA, No. 95-6125, 1996 WL 110179, at *1-2 (2d Cir. Mar. 12, 1996) (affirming lower court decision which held that plaintiff’s access claims were moot because he had ultimately designated representative to receive medical records and had been provided with them (even though prior to filing suit, plaintiff had refused to designate representative); stating further that plaintiff decided voluntarily to designate representative and thus although issue

was “capable of repetition” it had “not been shown to evade review”).

Although there is no counterpart provision qualifying a requester’s independent right of access to his medical records under the FOIA, the D.C. Circuit found it unnecessary in Benavides to confront this issue. See 995 F.2d at 273. In fact, only two courts have addressed the matter of separate FOIA access and the possible applicability of 5 U.S.C. § 552a(t)(2) (addressing access interplay between Privacy Act and FOIA), one of which was the lower court in a companion case to Benavides. See Smith v. Quinlan, No. 91-1187, 1992 WL 25689, at *4 (D.D.C. Jan. 13, 1992) (stating court did “not find Section 552a(f)(3) as implemented [by 28 C.F.R. § 16.43(d)] and Section 552a(t)(2) to be incompatible”; reasoning that “if Congress had intended Section 552a(t) to disallow or narrow the scope of special procedures that agencies may deem necessary in releasing medical and psychological records, it would have so indicated by legislation”), rev’d & remanded sub nom. Benavides v. BOP, 995 F.2d 269 (D.C. Cir. 1993); Waldron v. SSA, No. CS-92-334, slip op. at 10-15 (E.D. Wash. June 1, 1993) (upholding Smith, but with regard to SSA regulation); cf. Hill, No. 3-CV-92-0859, slip op. at 7 (M.D. Pa. Apr. 12, 1993) (interpreting subsection (f)(3) incorrectly as constituting an “exempting statute” under FOIA).

For further discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,957, 28,967, https://www.justice.gov/paoverview_omb-75, and the Report of the House Committee on Government Operations, H.R. Rep. No. 1416, 93d Cong., 2d Sess. at 16-17 (1974), reprinted in Source Book at 309-10, https://www.justice.gov/opcl/paoverview_sourcebook.

D. 5 U.S.C. § 552a(f)(4) - Establish Procedures for Requests and Appeals

“The rules shall –

...

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section;” 5 U.S.C. § 552a(f)(5).

Comment:

For a discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,967, https://www.justice.gov/paoverview_omb-75.

E. 5 U.S.C. § 552a(f)(5) - Establish Copying Fees

“The rules shall –

...

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record.” 5 U.S.C. § 552a(f)(5).

Comment:

For a discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,968, https://www.justice.gov/paoverview_omb-75.

CIVIL REMEDIES

The Privacy Act provides four separate and distinct civil causes of action. See 5 U.S.C. § 552a(g). Two civil causes of action provide for injunctive relief – amendment lawsuits under (g)(1)(A) and access lawsuits under (g)(1)(B). The remaining two causes of action provide for compensatory relief in the form of monetary damages – damages lawsuits under (g)(1)(C) and (g)(1)(D).

A. 5 U.S.C. § 552a(g)(1)(A) - Amendment Lawsuits

“Whenever any agency . . . makes a determination under subsection (d)(3) . . . not to amend an individual’s record in accordance with his request, or fails to make such review in conformity with that subsection . . . the individual may bring a civil action against the agency.” 5 U.S.C. § 552a(g)(1)(A).

Comment:

When an agency does not amend an individual’s record as requested or does not otherwise comply with the requirements of subsection (d)(3) -- which also establishes, e.g., time limits and notification requirements -- the Privacy Act specifically authorizes individuals to seek redress in federal court. This section discusses the requirements for such amendment lawsuits.

1. Exhaustion of Administrative Remedies

Individuals must exhaust their administrative remedies prior to bringing amendment suits against an agency.

In order to pursue a civil action for amendment of a record, an individual must exhaust administrative remedies by making an amendment request to the agency and requesting administrative review. See 5 U.S.C. § 552a(d)(2)-(3). The requirement to make an amendment request to the agency and to seek administrative review before filing an action in civil court is jurisdictional in nature because it is imposed by the Act itself. As explained in greater detail below under “5 U.S.C. § 552a(g)(1)(B) - Access Lawsuits,” it is important to note that the requirement to exhaust administrative remedies in Privacy Act access lawsuits is only jurisprudential in nature, as it is not imposed by the Act itself.

The exhaustion principle is well established in the Privacy Act case law in the amendment context. Courts have consistently required the individual to file a request for amendment of his or her records, in conformity with the

agency's regulations, before commencing a subsection (g)(1)(A) lawsuit. See, e.g., Quinn v. Stone, 978 F.2d 126, 137-38 (3d Cir. 1992); (per curiam); Nagel v. HEW, 725 F.2d 1438, 1441 (D.C. Cir. 1984); Hill v. Air Force, 795 F.2d 1067, 1069 (D.C. Cir. 1986); McKoy v. Spencer, No. 1:16-CV-01313, 2019 WL 400615, at *5-6 (D.D.C. Jan. 31, 2019); Otero v. DOJ, 292 F. Supp. 3d 245, 251-52 (D.D.C. 2018); Dick v. Holder, 67 F. Supp. 3d 167, 188-89 (D.D.C. 2014); Lowe v. Colvin, No. SA-13-CV-145, 2014 WL 690644, at *4-5 (W.D. Tex. Feb. 21, 2014); Olsen v. SSA, No. 10-CV-0474, 2013 WL 3190346, at *3 (E.D.N.Y. June 18, 2013); Hutton v. VA, No. 1:12CV190, 2013 WL 1331191, at *1-2 (M.D.N.C. Mar. 29, 2013); Jones v. Office of Worker's Comp. Programs, No. 2:11-CV-2799, 2012 WL 5213148, at *3 (E.D. Cal. Oct. 22, 2012) (magistrate's recommendation); Middlebrooks v. Mabus, No. 1:11cv46, 2011 WL 4478686, at *5 n.10 (E.D. Va. Sept. 23, 2011); Kvech v. Holder, No. 10-cv-545, 2011 WL 4369452, at *4 n.10 (D.D.C. Sept. 19, 2011); Washington v. Donley, 802 F. Supp. 2d 539, 553-54 (D. Del. 2011); Reitz v. USDA, No. 08-4131, 2010 WL 786586, at *10 (D. Kan. Mar. 4, 2010); Pototsky v. DHS, No. CV 07-144, 2009 WL 10695555, at *3 (D. Ariz. Jan. 15, 2009), aff'd, 368 F. App'x 832 (9th Cir. 2010); Watson v. Mineta, No. 4:05-CV-007, 2007 WL 3102196, at *2 (M.D. Ga. Oct. 23, 2007) (dicta); Brown v. DOJ, No. 02-2662, slip op. at 24-26 (D. Ala. June 21, 2005); Pontecorvo v. FBI, No. 00-1511, slip op. at 21-22 (D.D.C. Sept. 30, 2001); Murphy v. United States, 121 F. Supp. 2d 21, 28 (D.D.C. 2000), aff'd per curiam, 64 F. App'x 250 (D.C. Cir. 2003); M.K. v. Tenet, 99 F. Supp. 2d 12, 20 (D.D.C. 2000); Blazy v. Tenet, 979 F. Supp. 10, 18-19 (D.D.C. 1997), summary affirmance granted, No. 97-5330, 1998 WL 315583 (D.C. Cir. May 12, 1998); Olivares v. NASA, 882 F. Supp. 1545, 1552 (D. Md. 1995), aff'd, 103 F.3d 119 (4th Cir. 1996) (unpublished table decision); Gergick v. Austin, No. 89-0838-CV-W-2, 1992 U.S. Dist. LEXIS 7338, at *13-16 (W.D. Mo. Apr. 29, 1992), aff'd, No. 92-3210 (8th Cir. July 9, 1993); Simon v. DOJ, 752 F. Supp. 14, 23 n.6 (D.D.C. 1990), aff'd, 980 F.2d 782 (D.C. Cir. 1992); Campbell v. USPS, No. 86-3609, 1990 WL 36132, at *4 (E.D. La. Mar. 28, 1990); Green v. USPS, No. 88-0539, 1989 U.S. Dist. LEXIS 6846, at *6-7 (S.D.N.Y. June 19, 1989); and Ross v. USPS, 556 F. Supp. 729, 735 (N.D. Ala. 1983); cf. New-Howard v. Shinseki, No. 09-5350, 2012 WL 2362546, at *6 (E.D. Pa. June 21, 2012) (finding plaintiff's amendment request "flawed [] as she asserts her claim against an entity that no longer has control of the documents" because at time plaintiff filed amendment request, she had filed Merit Systems Protection Board (MSPB) action, and thus, records that would "ordinarily be under the control of" OPM were "covered by the appropriate MSPB or [EEOC] system of records").

It also has been held that a plaintiff cannot "boot-strap" an access claim under (g)(1)(B) into a (g)(1)(A) amendment violation, even though the

plaintiff argued that by denying her request for access the agency had prevented her from exercising her right to request amendment. See Smith v. Cont'l Assurance Co., No. 91 C 0963, 1991 WL 164348, at *2 (N.D. Ill. Aug. 22, 1991); accord Mumme v. Labor, 150 F. Supp. 2d 162, 173 (D. Me. 2001), aff'd, No. 01-2256 (1st Cir. June 12, 2002); see also M.K., 99 F. Supp. 2d at 20 n.15 (holding that plaintiffs must exhaust administrative remedies by requesting amendment of records even though plaintiffs had argued that “they cannot ask the CIA[] to amend that which the CIA refuses to admit exists”).

In amendment suits, exhaustion of administrative processes generally includes exhaustion of administrative appeals.

In addition, many courts have required an individual to administratively appeal the agency’s denial of his or her amendment request before commencing a subsection (g)(1)(A) lawsuit. See Jernigan v. Air Force, No. 97-35930, 1998 WL 658662, at *2 (9th Cir. Sept. 17, 1998); Dickson v. OPM, 828 F.2d 32, 40 (D.C. Cir 1987); Hewitt v. Grabicki, 794 F.2d 1373, 1377-78 (9th Cir. 1986); Clutter v. Perdue, No. H-18-310, 2019 WL 1589942, at *7 (S.D. Tex. Jan. 28, 2019); Conley v. United States, No. 2:10-cv-444, 2011 WL 1256611, at *7 (S.D. Ohio Mar. 31, 2011); Pearson v. DHS, No. 3:08-CV-1885-B, 2009 WL 4016414, at *8 (N.D. Tex. Nov. 17, 2009); Leighton v. CIA., 412 F. Supp. 2d 30, 34-35 (D.D.C. 2006); Finnerty v. USPS, No. 03-558, 2006 WL 54345, at *6-8 (D.N.J. Jan. 9, 2006); Hass v. Air Force, 848 F. Supp. 926, 930 (D. Kan. 1994); Freude v. McSteen, No. 4-85-882, slip op. at 4-5 (D. Minn. Oct. 23, 1985), aff'd, 786 F.2d 1171 (8th Cir. 1986) (unpublished table decision); and Beaver v. VA, No. 1-82-477, slip op. at 2 (E.D. Tenn. Apr. 6, 1983). Cf. Williams v. Bezy, 97 F. App’x 573, 574 (6th Cir. 2004) (affirming district court’s dismissal of plaintiff’s subsection (e)(5) claim for failure to exhaust administrative remedies without specifically discussing whether claim was brought under subsection (g)(1)(A) or subsection (g)(1)(C)); Doe v. Goss, No. 04-2122, 2007 WL 106523, at *8 n.14 (D.D.C. Jan. 12, 2007) (“Plaintiff cannot circumvent the exhaustion requirement by styling his ‘equitable right’ as a constitutional claim where, as here, Congress has provided administrative machinery for the resolution of the statutory claim.”). But cf. Duke v. United States, 305 F. Supp. 2d 478, 488 (E.D. Pa. 2004) (finding that “although plaintiff [had] not exhausted administrative remedies” court had “subject matter jurisdiction over this claim” because “this exhaustion requirement is not a jurisdictional requirement” but a “practical” one).

An agency's failure to meet its own deadlines does not exempt an individual from the exhaustion requirement; court jurisdiction exists, however, as soon as an agency fails to comply with the amendment provision's administrative appeal time requirement.

Although subsection (d)(2)(A) requires an agency to “acknowledge in writing such receipt” of an amendment request within ten working days, subsection (d)(2)(B) merely requires an agency to “promptly” make the requested correction or inform the individual of its refusal to amend. In construing this language, the Court of Appeals for the District of Columbia Circuit has held that “[t]he statute provides no exemption from administrative review when an agency fails, even by several months, to abide by a deadline, and none is reasonably implied.” Dickson v. OPM, 828 F.2d 32, 40-41 (D.C. Cir. 1987) (requiring exhaustion of subsection (d)(3) administrative appeal remedy even when agency did not respond to initial amendment request for 90 days (citing Nagel, 725 F.2d at 1440-41)). But see Schaeuble v. Reno, 87 F. Supp. 2d 383, 389-90 (D.N.J. 2000) (holding further exhaustion of administrative remedies is not required where plaintiff had requested amendment and agency had not responded for six months; stating that “[a] six month delay is not a ‘prompt’ response,” and that “[m]oreover, not only has the [agency] not indicated that it will make a final determination . . . by any certain date, the Privacy Act does not bind the [agency] to any definite timeframe for administrative action, which weighs in favor of waiving the exhaustion requirement”).

In contrast to subsection (d)(2)(B), subsection (d)(3) requires an agency to make a final determination on administrative appeal from an initial denial of an amendment request within 30 working days (unless, for good cause shown, the head of the agency extends this 30-day period). Thus, court jurisdiction exists as soon as an agency fails to comply with the time requirements of subsection (d)(3); “[t]o require further exhaustion would not only contradict the plain words of the statute but also would undercut [C]ongress’s clear intent to provide speedy disposition of these claims.” Diederich v. Army, 878 F.2d 646, 648 (2d Cir. 1989).

Individuals who are not informed of their right to administratively appeal an agency decision are treated as having “exhausted” administrative remedies.

After denying an amendment request, an agency must inform the complainant of the right to administratively appeal that denial or the complainant is not penalized for failing to exhaust his or her administrative remedies before filing a civil action. In Harper v. Kobelinski, 589 F.2d 721

(D.C. Cir. 1978) (per curiam), and Liguori v. Alexander, 495 F. Supp. 641 (S.D.N.Y. 1980), the agencies denied amendment requests but failed to inform the plaintiffs of their rights to administratively appeal those decisions. In light of the Act's requirement that agencies inform complainants whose amendment requests have been denied of the available administrative remedies, 5 U.S.C. § 552a(d)(2)(B)(ii), the courts in Harper and Liguori refused to penalize the plaintiffs for their failures to exhaust. Harper, 589 F.2d at 723; Liguori, 495 F. Supp. at 646-47; see also Germane v. Heckler, 804 F.2d 366, 369 (7th Cir. 1986) (discussing Harper and Liguori with approval); Mahar v. Nat'l Parks Serv., No. 86-0398, slip op. at 7-11 (D.D.C. Dec. 23, 1987) (same); cf. Ertell v. Army, 626 F. Supp. 903, 909-10 (C.D. Ill. 1986) (rejecting agency's exhaustion defense where it first told employee, in response to his amendment request, that it had destroyed the record but later used same record against him, ruling that employee was not required to make new request or appeal initial action).

The D.C. Circuit has held that individuals must seek judicial review of adverse employment decisions under the Administrative Procedures Act prior to filing civil Privacy Act suit.

D.C. courts have held that civil suits may not be filed until the individual has sought judicial review under the Administrative Procedures Act ("APA"). For example, in White v. U.S. Civil Serv. Comm'n, 589 F.2d 713, 715-16 (D.C. Cir. 1978) (per curiam), the D.C. Circuit held that, notwithstanding any exhaustion of administrative remedies, an amendment action is "inappropriate and premature" where the individual had not yet sought judicial review (under the APA) of adverse employment decisions, because granting Privacy Act relief "would tend to undermine the established and proven method by which individuals . . . have obtained review from the courts." Cf. Douglas v. Farmers Home Admin., No. 91-1969, 1992 U.S. Dist. LEXIS 9159, at *4-5 (D.D.C. June 26, 1992) (dismissing damages action under Privacy Act where plaintiff had not sought review under Administrative Procedure Act of allegedly inaccurate property appraisal). But see Churchwell v. United States, 545 F.2d 59, 61 (8th Cir. 1976) (finding probationary employee could proceed with due process claim for hearing even though Privacy Act remedy was available to her because "the failure to pursue one particular remedy has [no] bearing on the viability of the other form of relief").

2. Standard and Scope of Review

"In any suit brought under the provisions of subsection (g)(1)(A) of this

section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo." 5 U.S.C. § 552a(g)(2)(A).

Comment:

After an individual exhausts his or her administrative remedies by making an amendment request to the agency and requesting administrative review pursuant to subsections (d)(2) and (d)(3), the individual may challenge the agency's refusal to amend the individual's record in federal district court. In such amendment actions, brought under subsection (g)(1)(A), "the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct," and "may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred" in any case in which the complainant has "substantially prevailed." 5 U.S.C. § 552a(g)(2)(A), (B).

Amendment suits are reviewed in the federal courts de novo.

In a subsection (g)(1)(A) action, the court "shall determine the matter de novo." 5 U.S.C. § 552a(g)(2)(A). "De novo review does not contemplate that the court will substitute its judgment for the [agency's], but rather that the court will undertake an independent determination of whether the amendment request should be denied." Nolan v. DOJ, No. 89-A-2035, 1991 WL 134803, at *3 (D. Colo. July 17, 1991), appeal dismissed in pertinent part on procedural grounds, 973 F.2d 843 (10th Cir. 1992); see also Doe v. United States, 821 F.2d 694, 697-98 (D.C. Cir. 1987) (holding that "[d]e novo means . . . a fresh, independent determination of 'the matter' at stake"). The applicable standards in amendment lawsuits are accuracy, relevancy, timeliness, and completeness. 5 U.S.C. § 552a(d)(2)(B)(i). But see Doe v. United States, 821 F.2d at 697 n.8, 699 (stating that "whether the nature of the relief sought is injunctive or monetary, the standard against which the accuracy of the record is measured remains constant" and "[t]hat standard is found in 5 U.S.C. § 552a(e)(5) and reiterated in 5 U.S.C. § 552a(g)(1)(C)"). The burden of proof is on the individual. See Mervin v. FTC, 591 F.2d 821, 827 (D.C. Cir. 1978) (per curiam); Thompson v. Coast Guard, 547 F. Supp. 274, 282 (S.D. Fla. 1982); OMB 1975 Guidelines, 40 Fed. Reg. at 28,969, https://www.justice.gov/paoverview_omb-75.

Individuals may not bring civil suit for an agency's failure to amend records that do not exist.

"[A]n individual's request for amendment must relate to an existing record that is maintained within one of the agency's systems of records."
Crummey v. SSA, 794 F. Supp. 2d 46, 58 (D.D.C. 2011), aff'd per curiam, No. 11-5231, 2012 WL 556317 (D.C. Cir. Feb. 6, 2012). The plaintiff in Crummey – who "believe[d] that the Social Security Administration created a trust . . . when it assigned him a Social Security Number and a Social Security Card" – had "draft[ed] an agreement designed to reflect the alleged creation of the Trust." 794 F. Supp. 2d at 49. The plaintiff brought a subsection (g)(1)(A) claim seeking a court order requiring the SSA "to amend its records to add the Trust Agreement to the SSA's Master Files, or to somehow incorporate its contents therein." Id. at 52. The court reviewed the categories of records listed in the applicable system of records notice, see 75 Fed. Reg. 82,123 (Dec. 29, 2010), and determined that "[n]one of the information set forth in the Trust Agreement falls within this universe." 794 F. Supp. 2d at 58. "In short," the court concluded, "the Trust Agreement and the information contained therein do not correspond to an 'item, collection, or grouping' of information in the Master Files," and granted summary judgment to the SSA. Id. at 59.

Once records have been amended, the amendment claim is moot.

Once a request for amendment is complied with and the identified records have been amended, the amendment claim is moot. See, e.g., Conley, 2011 WL 1256611, at *7; Blanton v. Warden, No. 7:10-cv-00552, 2011 WL 1226010, at *2-3 (W.D. Va. Mar. 30, 2011); Garza v. Pearson, No. 5:08-cv-300, 2009 WL 2500116, at *1 (S.D. Miss. Aug. 13, 2009); Blazy v. Tenet, 979 F. Supp. 10, 19 (D.D.C. 1997), summary affirmance granted, No. 97-5330, 1998 WL 315583 (D.C. Cir. May 12, 1998).

There are several matters that are not subject to court review under the amendment provisions of the Privacy Act, including tax liability determinations, judicial and quasi-judicial decisions, and criminal convictions and sentences.

Tax liability determinations are not subject to court review under the Privacy Act. In the Internal Revenue Code, Congress expressly removed the jurisdiction of the district courts under Privacy Act subsection (g) to order the amendment of IRS records concerning tax liability. 26 U.S.C. § 7852(e) (providing that subsection (g), as well as subsections (d)(2), (3) and (4), "shall not apply, directly or indirectly," to any "determination of the

existence or possible existence of liability (or the amount thereof) of any person for any tax, penalty, interest, fine, forfeiture, or other imposition or offense” to which title 26, United States Code, applies). See, e.g., Schlabach v. IRS, 491 F. App’x 854, 854-55 (9th Cir. 2012); Gardner v. United States, 213 F.3d 735, 740-41 & n.5 (D.C. Cir. 2000); England v. Comm’r, 798 F.2d 350, 351-52 (9th Cir. 1986); Meyer v. Comm’r, No. 10-767, 2010 WL 4157173, at *8 (D. Minn. Sept. 27, 2010) (magistrate’s recommendation), adopted, 2010 WL 4134958, at *8 (D. Minn. Oct. 19, 2010); Gulden v. United States, No. 8:06-CV-2327-T-27MSS, 2007 WL 3202480, at *3 (M.D. Fla. Oct. 29, 2007); Singer v. IRS, No. 98-0024, 1998 U.S. Dist. LEXIS 13301, at *10-11 (E.D. Pa. Aug. 10, 1998); Chandler v. United States, No. 93-C-812A, 1994 WL 315759, at *1 (D. Utah Mar. 8, 1994); Fuselier v. IRS, No. 90-0300, slip op. at 1 (W.D. La. Oct. 25, 1990); Mallas v. Kolak, 721 F. Supp. 748, 751 (M.D.N.C. 1989), aff’d in part, vacated in nonpertinent part & remanded, on other grounds, Mallas v. United States, 993 F.2d 1111 (4th Cir. 1993); Schandl v. Heye, No. 86-6219, slip op. at 2 (S.D. Fla. Sept. 30, 1986); Dyrdra v. Comm’r, No. 85-0-41, slip op. at 2 (D. Neb. Oct. 28, 1985); Conklin v. United States, No. 83-C-587, slip op. at 2-3 (D. Colo. Feb. 26, 1985); Green v. IRS, 556 F. Supp. 79, 80 (N.D. Ill. 1982), aff’d, 734 F.2d 18 (7th Cir. 1984) (unpublished table decision); see also Gardner v. United States, No. 96-1467, 1999 U.S. Dist. LEXIS 2195, at *18 (D.D.C. Jan. 29, 1999) (finding that by virtue of § 7852(e) the IRS is “exempt” from amendment provisions of Privacy Act), summary affirmance granted on other grounds, No. 99-5089, 1999 WL 728359 (D.C. Cir. Aug. 4, 1999) (per curiam).

In addition, consistent with the OMB 1975 Guidelines, courts have routinely expressed disfavor toward litigants who attempt to invoke the subsection (g)(1)(A) amendment remedy as a basis for collateral attacks on judicial or quasi-judicial determinations recorded in agency records. See 40 Fed. Reg. at 28,969, https://www.justice.gov/paoverview_omb-75; see also Jackson v. GSA, 729 F. App’x. 206, 209 (3d Cir. 2018) (per curiam) (citing Reinbold, infra, and denying expungement of “derogatory information,” where district court determined that records supported IRS’s determination that employment offer was rescinded based on fingerprint check); Sydnor v. OPM, 336 F. App’x 175, 180 (3d Cir. 2009) (concluding that “a collateral attack upon that which has been or could have been the subject of a judicial, quasi-judicial or administrative proceeding” lies “outside the scope of the Privacy Act”); Jones v. MSPB, 216 F. App’x 608, 609 (8th Cir. 2007) (affirming dismissal of amendment claim because “the statements accurately reflect administrative decisions”); Cooper v. Treasury, No. 05-0314, 2006 WL 637817, at *2-3 (11th Cir. Mar. 15, 2006) (finding law-of-the-case doctrine bars relitigation of claim under Privacy Act that had been decided against

plaintiff in district court and affirmed by court of appeals); Reinbold v. Evers, 187 F.3d 348, 361 (4th Cir. 1999) (“[T]he Privacy Act does not allow a court to alter records that accurately reflect an administrative decision, or the opinions behind that administrative decision.”); Milhous v. EEOC, No. 97-5242, 1998 WL 152784, at *1 (6th Cir. Mar. 24, 1998) (“The Privacy Act may not be used to challenge unfavorable agency decisions[.] It is intended solely to be used to correct factual or historical errors.”); Douglas v. Agric. Stabilization & Conservation Serv., 33 F.3d 784, 785 (7th Cir. 1994) (asserting that the “Privacy Act does not authorize relitigation of the substance of agency decisions” and that “the right response . . . is to correct the disposition under the Administrative Procedure Act”); Bailey v. VA, No. 94-55092, 1994 WL 417423, at *1 (9th Cir. Aug. 10, 1994) (finding that plaintiff may not use Privacy Act to collaterally attack grant or denial of benefits); Sugrue v. Derwinski, 26 F.3d 8, 11 (2d Cir. 1994) (finding that the Privacy Act may not be used “as a rhetorical cover to attack VA benefits determinations”); Geurin v. Army, No. 90-16783, 1992 WL 2781, at *2 (9th Cir. Jan. 6, 1992) (finding doctrine of res judicata bars relitigation of claims under Privacy Act that had been decided against plaintiff by United States Claims Court in prior action under 28 U.S.C. § 1491); Pellerin v. VA, 790 F.2d 1553, 1555 (11th Cir. 1986) (quoting Rogers v. Labor, 607 F. Supp. 697, 699 (N.D. Cal. 1985) that the Privacy Act “may not be employed as a skeleton key for reopening consideration of unfavorable federal agency decisions,” and dismissing amendment lawsuit challenging VA disability benefits determination on the ground that veterans benefit statute limits judicial review of VA’s determinations); Hutton v. VA, No. 1:12CV190, 2013 WL 1331191, at *2 (explaining that even if plaintiff’s Privacy Act claim were properly before the court, “[p]laintiff seeks to alter records that, under the facts alleged, accurately reflect the administrative decisions made years ago”); New-Howard v. Shinseki, No. 09-5350, 2012 WL 2362546, at *7 (E.D. Pa. June 21, 2012) (“Plaintiff’s placement in the position of Office Automation Clerk and her placement in the FERS system may have been substantively incorrect, to the extent that such placement occurred, the records in her file accurately reflect what occurred in August 2005. As a result, the proper procedure for Plaintiff to employ in order to correct the error is to pursue the matter before the MSPB.”); Hardy v. McHugh, 692 F. Supp. 2d 76, 80-81 (D.D.C. 2010) (rejecting claim to correct Army memorandum of reprimand that included “implication that [plaintiff] intentionally misrepresented his educational credentials” because “the Army’s judgment is based on accurate facts” and because plaintiff “presents the same facts that have been considered by various Army boards and asks [the court] to substitute [its] judgment for theirs”); Jackson v. Labor, No. 2:06-CV-02157, 2008 WL 539925, at *4 (E.D. Cal. Feb. 25, 2008) (ruling that

plaintiff may not bring amendment lawsuit under Privacy Act to re-litigate determination of Federal Employees' Compensation Act benefits); Davenport v. Harvey, No. 06-CV-02669, slip op. at 8 (S.D. Cal. May 3, 2007) (rejecting claim "seek[ing] to alter factual findings and conclusion made by the [DOD Office of Hearings and Appeals] [administrative judge] as part of Plaintiff's appeal of the denial of his security clearance"), aff'd in pertinent part, vacated in part, & remanded sub nom. Davenport v. McHugh, 372 F. App'x 820 (9th Cir. 2010); Lee v. Geren, 480 F. Supp. 2d 198, 209 (D.D.C. Mar. 29, 2007) (finding that plaintiff "is not seeking to correct any true errors in his records" but instead "is hoping that this Court will expunge all references in his records to an adverse personnel action that he could not challenge directly because the CSRA precludes such review"); Lechliter v. Army, No. 04-814, 2006 WL 462750, at *2-3 (D. Del. Feb. 27, 2006) ("To the extent that [plaintiff] is asking [the court] to alter the ultimate determination by the Department that he is not disabled, rather than to correct factual errors recited in his records, such relief is outside that provided by the Privacy Act."); Levant v. Roche, 384 F. Supp. 2d 262, 270 (D.D.C. 2005) (concluding that plaintiff's "true complaint is not about the accuracy of his records, but about the underlying decision [not to promote him to the rank of major general, which those records] reflect"); Byrnes v. MSPB, No. 04-742, 2005 WL 486156, at *2-3 (D.D.C. Mar. 2, 2005) (ruling that plaintiff could not collaterally attack "an inartfully drafted settlement agreement" terminating a lawsuit by seeking to amend agreement to include a provision requiring MSPB to "depublish" its prior decision); Bernard v. DOD, 362 F. Supp. 2d 272, 280-81 (D.D.C. 2005) (dismissing plaintiff's amendment claim because plaintiff did not "seek to correct a factual or historical error" but rather challenged agency's substantive judgments or decisions); Gowan v. Air Force, No. 90-94, slip op. at 26, 33 (D.N.M. Sept. 1, 1995) (commenting that "Privacy Act, unfortunately, may not be used as a collateral attack on the improper referral of charges [for court martial], nor may the Privacy Act be used as a method for the Court to oversee the activities of the armed services"), aff'd, 148 F.3d 1182 (10th Cir. 1998); Williams v. McCausland, 90 Civ. 7563, 1994 WL 18510, at *17 (S.D.N.Y. Jan. 18, 1994) (denying plaintiff's request to supplement record of his administrative proceeding before MSPB because request "constitutes an attempt to contest the MSPB's determination on the merits of his request for a stay of his removal"); Smith v. Conti Assurance Co., No. 91 C 0963, 1991 WL 164348, at *5 (N.D. Ill. Aug. 22, 1991) (finding that plaintiff cannot use Privacy Act to collaterally attack agency decision regarding her Federal Employees Health Benefit Act claim); Rowan v. USPS, No. 82-C-6550, 1984 U.S. Dist. LEXIS 17042, at *6 (N.D. Ill. May 2, 1984) (asserting that the Privacy Act is not "a means for all disgruntled governmental employees to have unflattering appraisals removed from their

personnel files or shaded according to their own whims or preferences”); Leib v. VA, 546 F. Supp. 758, 762 (D.D.C. 1982) (“The Privacy Act was not intended to be and should not be allowed to become a ‘backdoor mechanism’ to subvert the finality of agency determinations.” (internal citation omitted)); Lyon v. United States, 94 F.R.D. 69, 72 (W.D. Okla. 1982) (asserting that a Privacy Act claim cannot be “a backdoor mechanism to subvert authority bestowed upon the Secretary of Labor to handle employee compensation claims” and stating that the FECA “provides the exclusive method of presenting compensation claims resulting from on-the-job injuries of federal employees”); Bashaw v. Treasury, 468 F. Supp. 1195, 1196-97 (E.D. Wis. 1979) (citing OMB 1975 Guidelines with approval and holding that amendment remedy is “neither a necessary nor an appropriate vehicle for resolving the merits of the plaintiff’s [discrimination] claims”); Kennedy v. Andrus, 459 F. Supp. 240, 242 (D.D.C. 1978) (noting that OMB 1075 Guidelines “clearly forbid collateral attack in the case of final judicial or quasi-judicial actions” and observing that “the same considerations would seem to apply to agency personnel actions, such as the reprimand here, for collateral attack under the Privacy Act could undermine the effectiveness of agency grievance systems”), aff’d, 612 F.2d 586 (D.C. Cir. 1980) (unpublished table decision); cf. Subh v. Army, No. 1:10cv433, 2010 WL 4961613, at *4 (E.D. Va. Nov. 30, 2010) (rejecting plaintiff’s attempt “to rewrite history to pretend that he correctly answered ‘yes’ to question 22 [on Standard Form 86, the ‘Questionnaire for National Security Positions’] when in fact he falsely answered ‘no’” because “[t]he Privacy Act plainly does not exist to allow applicants to obtain such a ‘do-over’ of their security forms in the guise of an administrative ‘correction’”); Doe v. HHS, 871 F. Supp. 808, 814-15 (E.D. Pa. 1994) (“[T]he specific reporting provisions encompassed in the [Health Care Quality Improvement] Act supersede[] any claims [plaintiff] might have under the Privacy Act.”), aff’d, 66 F.3d 310 (3d Cir. 1995) (unpublished table decision).

Criminal court convictions and sentences are generally not subject to civil amendment court review under the Privacy Act. Federal prisoners frequently attempt to invoke the subsection (g)(1)(A) amendment remedy as a basis for a collateral attack on a conviction or the duration of a sentence. Just as in the damages context – discussed in the “5 U.S.C. § 552a(g)(1)(C) - Damages Lawsuits for Failure to Assure Fairness in Agency Determination” section, below – courts have frequently ruled that unless the conviction or sentence has been invalidated in a prior proceeding, the prisoner’s exclusive remedy is a writ of habeas corpus. See, e.g., Reeves v. BOP, 885 F. Supp. 2d 384, 389 (D.D.C. 2012) (“A civil action under the Privacy Act is not the proper means by which a federal prisoner may secure a reduction in the

duration of his confinement.”); Crompton v. Kent, No. 12-cv-757, 2012 WL 5903088, at *3 (W.D. Wis. Nov. 26, 2012) (holding that a prisoner’s claim to amend his presentence report cannot succeed because the individual defendants were immune and that BOP “cannot be ordered to amend plaintiff’s presentence report because it has no authority to take such an action”); King v. Johns, No. 4:10cv1835, 2010 WL 4065405, at *1 (N.D. Ohio Oct. 14, 2010) (“[A] complaint seeking relief under . . . § 552a is not a permissible alternative to a petition for writ of habeas corpus if the plaintiff essentially challenges the legality of his confinement.”); Truesdale v. DOJ, 731 F. Supp. 2d 3, 11 (D.D.C. 2010) (dismissing Privacy Act claims because a ruling in plaintiff’s favor would impact the duration of his confinement, and should be brought in a petition for a writ of habeas corpus “not by way of a suit brought under the Privacy Act”); Davis v. United States, No. 09-1961, 2010 WL 2011549, at *1 n.1 (D. Md. May 18, 2010) (“[T]o the extent Petitioner believes that his sentence should be modified, such claims may only be made in the context of a habeas petition.”); Brown v. BOP, 498 F. Supp. 2d 298, 303-04 (D.D.C. 2007) (“The Privacy Act is not the proper means by which a prisoner may collaterally attack his sentence absent a showing that his sentence has been invalidated in a prior proceeding.”); Forrester v. Parole Comm’n, 310 F. Supp. 2d 162, 168-70 (D.D.C. 2004) (concluding that reaching plaintiff’s Privacy Act claim seeking order to expunge information “would have a probabilistic impact on his confinement . . . and therefore plaintiff may only raise [such a claim] in a petition for a writ of habeas corpus”); Graham v. Hawk, 857 F. Supp. 38, 40-41 (W.D. Tenn. 1994) (“The Privacy Act is not a means of circumventing [habeas] exhaustion requirement.”), aff’d, 59 F.3d 170 (6th Cir. 1995) (unpublished table decision). Similarly, the D.C. Circuit has concluded that the Privacy Act amendment provisions do not allow for amendment of military records: “The proper means by which to seek a change to military records is through a proceeding before the . . . Board for Correction of Military Records,” not under the Privacy Act. Glick v. Army, No. 91-5213, 1992 WL 168004, at *1 (D.C. Cir. June 5, 1992) (per curiam); see also Cargill v. Marsh, 902 F.2d 1006, 1007-08 (D.C. Cir. 1990) (per curiam) (affirming dismissal of Privacy Act claim and concluding proper means to seek substantive change in military records is through proceeding before the Boards for Correction of Records); Walsh v. Hagee, 900 F. Supp. 2d 51, 60 (D.D.C. 2012) (“For [plaintiff] to obtain injunctive relief to amend his military record, he must proceed under 10 U.S.C. § 1552.”); Doe v. Navy, 764 F. Supp. 1324, 1327 (N.D. Ind. 1991) (“[P]laintiff is not free to choose to attempt amendment of his military records under the Privacy Act alone without resort to the records correction board remedy.”); cf. Hardy, 692 F. Supp. 2d at 80-81 (rejecting claim seeking correction of Army memorandum of reprimand including “implication that

[plaintiff] intentionally misrepresented his educational credentials” because “the Army’s judgment is based on accurate facts” and because plaintiff “presents the same facts that have been considered by various Army boards and asks [the court] to substitute [its] judgment for theirs”); Walker v. United States, No. 93-2728, 1998 WL 637360, at *14 (E.D. La. Sept. 16, 1998) (citing Cargill and finding plaintiff’s claim “unavailing” to extent that he “is attempting to use the Privacy Act as a vehicle for his collateral attack on the Army’s allegedly improper failure to correct his military records”), aff’d, 184 F.3d 816 (5th Cir. 1999) (unpublished table decision). But see Diederich v. Army, 878 F.2d 646, 647-48 (2d Cir. 1989) (holding that “Privacy Act claims were properly before the district court” and that plaintiff was not required to further exhaust administrative remedies before asserting claim for amendment of military records where his direct request to Army for correction had been stalled before appeals board for several months); see also Def. Priv. Bd., Advisory Opinions No. 4, Corrections of Military Records Under the Privacy Act, in Judge Advocate General’s School, U.S. Army, JA 235, Government Information Practices – Casebook, A-13 (March 2000), https://www.justice.gov/paoverview_ja-235 (affording review under Privacy Act for factual matters only but noting that challenges to judgmental decisions may be made to the Boards for Correction of Military or Naval Records).

Finally, several courts have ruled that statutes that provide other avenues of redress, such as the CSRA, can bar certain kinds of subsection (g)(1)(C) damages actions. These cases are discussed below under “5 U.S.C. § 552a(g)(1)(C) - Damages Lawsuits for Failure to Assure Fairness in Agency Determination.”

The courts are split as to whether records that are exempt from the Privacy Act’s access provision are also exempt from the Privacy Act’s amendment suits.

The Courts of Appeals for the Fifth, Seventh, and Ninth Circuits have concluded that records that are exempt from access under the Privacy Act are not subject to amendment suits. The Court of Appeals for the Fifth Circuit held that a plaintiff had no right to amend the record at issue even though that record was only “exempt from the access requirements of the Act.” Smith v. United States, 142 F. App’x 209, 210 (5th Cir. 2005) (per curiam) (emphasis added). In other words, the court explained, “the scope of accessibility and the scope of amendment under the Privacy Act are coextensive.” Id. The plaintiff in Smith had sought to amend a report that was “prepared in response to [his Federal Tort Claims Act] claim.” Id. The Fifth Circuit explained that because this report “was prepared in reasonable

anticipation of a civil suit or proceeding” within the meaning of the subsection (d)(5) exemption, “[t]he report is . . . also exempt from the amendment requirements of the Act.” Id. Thus, the court concluded, the amendment claim was “barred by exemption.” Id. Subsection (d)(5) is discussed below under “Ten Exemptions.”

The Smith court agreed with earlier cases in the Court of Appeals for the Ninth and Seventh Circuits. The Ninth Circuit held that “Congress intended to provide the remedies of amendment or expungement only for records that are accessible under the Privacy Act.” Baker v. Navy, 814 F.2d 1381, 1385 (9th Cir. 1987) (finding that plaintiff’s ability to access record under FOIA or because of personal knowledge of its existence, did not permit him to amend record because it was not contained in system of records as required for access by subsection (d)(1) of Privacy Act). Similarly, the Seventh Circuit concluded that “you cannot amend a document if you don’t have access to it.” Wentz v. DOJ, 772 F.2d 335, 338 (7th Cir. 1985) (alternative holding) (concluding that amendment was not appropriate because the record was exempt from access under subsection (d)(1), pursuant to subsection (j)(2)).

The Courts of Appeals for the District of Columbia, First, and Fourth Circuits also have concluded that courts do not have jurisdiction under subsection (g)(1)(A) to order the amendment of records addressed by the Civil Service Reform Act’s (CSRA) comprehensive remedial scheme. See Wills v. OPM, No. 93-2079, 1994 WL 22349, at *3-4 (4th Cir. Jan. 28, 1994) (alternative holding) (per curiam) (unpublished table decision) (finding jurisdiction was proper under CSRA where challenge to merits of statement on SF-50 was actually complaint regarding adverse employment decision); Vessella v. Air Force, No. 92-2195, 1993 WL 230172, at *2 (1st Cir. June 28, 1993) (citing Kleiman, infra, and holding that plaintiff could not “bypass the CSRA’s regulatory scheme” by bringing Privacy Act claim for same alleged impermissible adverse personnel practices that he challenged before MSPB, even though MSPB dismissed his claims as untimely); Kleiman v. Energy, 956 F.2d 335, 338 (D.C. Cir. 1992) (quoting Carducci v. Regan, 714 F.2d 171, 174 (D.C. Cir. 1983) and refusing to allow exhaustive remedial scheme of CSRA to be “impermissibly frustrated” by granting review of personnel decisions under the Privacy Act); see also Wonders v. McHugh, No. 1:12-CV-817, 2013 WL 1729928, at *6 (M.D. Ala. Apr. 4, 2013) (finding plaintiff’s claims about “personnel actions” fell within “CSRA’s general prohibition against prejudicial treatment” rather than under Privacy Act); Minshew v. Donley, 911 F. Supp. 2d 1043, 1067 (D. Nev. 2012) (explaining that CSRA preempts plaintiff’s Privacy Act claim: “[T]he CSRA is the exclusive means

for federal employees to challenge prohibited personnel practices, a federal employee may not resort to other statutes to effectively challenge, review, reverse, or otherwise collaterally attack a decision falling within the scope of the CSRA"); Lee v. Geren, 480 F. Supp. 2d 198, 206, 208 (D.D.C. 2007) (following "the course set by [Kleiman]" by "evaluat[ing] the merits of plaintiff's claims . . . in a way that does not do violence to the CSRA" but ultimately finding that "[t]here is simply nothing inaccurate about" plaintiff's records).

3. Remedies

The Privacy Act allows for broad injunctive remedies in amendment suits, including expungement.

The Act provides for broad injunctive remedies, contemplating "expungement [of inaccuracies] and not merely redress by supplement." R.R. v. Army, 482 F. Supp. 770, 774 (D.D.C. 1980); see also Smith v. Nixon, 807 F.2d 197, 204 (D.C. Cir. 1986); Hobson v. Wilson, 737 F.2d 1, 65-66 (D.C. Cir. 1984), overruled in part on other grounds, Leatherman v. Tarrant Cnty. Narcotics Intel. & Coord. Unit, 507 U.S. 163 (1993).

Once an agency offers to destroy a record in response to an expungement request, the lawsuit is at an end, and the agency cannot be compelled to affirmatively determine and announce that the challenged record violated the Act. See Reuber v. United States, 829 F.2d 133, 144-49 (D.C. Cir. 1987); see also Comm. in Solidarity v. Sessions, 929 F.2d 742, 745 n.2 (D.C. Cir. 1991); Metadure Corp. v. United States, 490 F. Supp. 1368, 1375 (S.D.N.Y. 1980). But see Doe v. U.S. Civil Serv. Comm'n, 483 F. Supp. 539, 551 (S.D.N.Y. 1980).

The expungement remedy often is sought in cases asserting constitutional claims in addition to Privacy Act claims, such as claims for violation of the Fourth Amendment's due process protections. As the District of Columbia Circuit Court of Appeals has stated, "Congress's provision of specific Privacy Act remedies does not bar" a plaintiff's equitable Constitutional claims. Abdelfattah v. DHS, 787 F.3d 524, 534 (D.C. Cir. 2015) (holding that "[w]e have repeatedly recognized a plaintiff may request expungement of agency records for both violations of the Privacy Act and the Constitution"); see Chastain v. Kelley, 510 F.2d 1232, 1235-38 (D.C. Cir. 1975); Doe v. Air Force, 812 F.2d 738, 740-41 (D.C. Cir. 1987) (explaining that expungement of records seized from plaintiff's Air Force barracks may be "available as a remedy if it is determined that the retained copies and information were

unconstitutionally obtained”); Fendler v. Parole Comm’n, 774 F.2d 975, 979 (9th Cir. 1985); Ezenwa v. Gallen, 906 F. Supp. 978, 986 (M.D. Pa. 1995); cf. Johnson v. Sessions, No. 92-201, 1992 WL 212408, at *2 (D.D.C. Aug. 19, 1992) (refusing to invoke equitable powers to expunge plaintiff’s arrest record because court did not have jurisdiction to order FBI to violate its own regulations which require FBI to wait for authorization from appropriate judicial authority before expunging arrest record); NTEU v. IRS, 601 F. Supp. 1268, 1273 (D.D.C. 1985) (“Although the [inherent equitable power to order the expungement of a record] is most frequently employed to vindicate express or implied constitutional or statutory rights . . . the remedy need not always be so limited.”).

However, when such equitable remedies are requested pursuant solely to the doctrine of ancillary jurisdiction – “which recognizes federal courts’ jurisdiction over some matters (otherwise beyond their competence) that are incidental to other matters” – the courts generally have not permitted equitable expungement. See Kokkonen v. Guardian Life Ins. Co. of Am., 511 U.S. 375, 378 (1994). Following Kokkonen, a number of circuits have found that Federal courts do not maintain “inherited” powers ancillary to its original action to hear requests for equitable expungement of records; jurisdiction must be grounded in the Constitution or by statute. United States v. Wahi, 850 F.3d 296, 302 (7th Cir. 2017); Doe v. United States, 833 F.3d 192, 199 (2d Cir. 2016); United States v. Field, 756 F.3d 911, 916 (6th Cir. 2014); United States v. Coloian, 480 F.3d 47, 52 (1st Cir. 2007); United States v. Meyer, 439 F.3d 855, 862 (8th Cir. 2006); United States v. Dunegan, 251 F.3d 477, 479 (3d Cir. 2001); United States v. Sumner, 226 F.3d 1005, 1014 (9th Cir. 2000).

B. 5 U.S.C. § 552a(g)(1)(B) - Access Lawsuits

“Whenever any agency . . . refuses to comply with an individual request under subsection (d)(1) of this section [the individual may bring a civil action against the agency].” 5 U.S.C. § 552a(g)(1)(B).

Comment:

Subsection (g)(1)(B) authorizes an individual to bring a civil suit against an agency that refuses to comply with the individual’s access request. Sovereign immunity is not a defense in such cases. See In re U.S. Office of Pers. Mgmt. Data Sec. Breach Litig., 928 F.3d 42, 61 (D.C. Cir. 2019) (noting that Privacy Act “provides . . . a waiver of sovereign immunity”); Braun v. USPS, No. 16-2079, 2017 WL 4325645, at *5 (D.D.C. Sept. 17, 2017) (concluding that Privacy Act

access lawsuit is not barred by sovereign immunity, because Act is statutory waiver of such immunity).

1. Exhaustion of Administrative Remedies

Requesters must exhaust administrative remedies before filing access suits under subsection (g)(1)(B); unlike amendment suits under subsection (g)(1)(A), the exhaustion requirement in access suits is not jurisdictional.

Just as under the FOIA, a requester must comply with agency procedures and exhaust all available administrative remedies – through pursuit of an access request to the agency and, if that request is denied, through an administrative appeal – prior to bringing a subsection (g)(1)(B) action.

The exhaustion requirement cannot be found in the language of the Privacy Act itself, and arises instead from jurisprudential exhaustion principles. Thus, it is not jurisdictional. Because “[t]he language in [subsections (d)(1) and (g)] does not expressly require exhaustion of particular administrative remedies,” there is no statutory requirement for exhaustion related to a request for access to records. Taylor v. Treasury, 127 F.3d 470, 476 (5th Cir. 1997). The Court of Appeals for the Fifth Circuit noted that, “[w]henver the Congress statutorily mandates that a claimant exhaust administrative remedies, the exhaustion requirement is jurisdictional because it is tantamount to a legislative investiture of exclusive original jurisdiction in the agency.” Id. at 475. However, in “the absence of a statutory requirement of exhaustion . . . the jurisprudential doctrine of exhaustion controls. . . . The jurisprudential exhaustion doctrine is not jurisdictional in nature.” Id. (citations omitted). The Fifth Circuit concluded that the plaintiff’s “failure to exhaust administrative remedies did not constitute a jurisdictional bar to assertion of his claim [for access to records, but] . . . application of the jurisprudential exhaustion doctrine in this case indicates that . . . [plaintiff’s] claims under the Privacy Act must be dismissed for failure to state a claim upon which relief can be granted.” Id. at 476-77.

The Courts of Appeals for the Third and Ninth Circuits also have recognized a jurisprudential exhaustion requirement in Privacy Act cases. The Court of Appeals for the Third Circuit followed Taylor and stated, “To the extent exhaustion of administrative remedies is required, it is not a jurisdictional prerequisite.” Wadhwa v. VA, 342 F. App’x 860, 862-63 (3d Cir. 2009) (per curiam) (citing Taylor, 127 F.3d at 475-76) (emphasis added). Rather, courts have required plaintiffs seeking access to records to exhaust administrative remedies pursuant to the “jurisprudential exhaustion

doctrine.” See, e.g., id. The Third Circuit “disagree[d] with the District Court’s conclusion that it lacks jurisdiction to entertain [plaintiff’s] claim [for access to records] under the Privacy Act because [plaintiff] failed to exhaust his administrative remedies.” 342 F. App’x at 862. See also Buckley v. Schaul, 135 F. App’x 960, 960 (9th Cir. 2005) (holding that “even in the absence of an explicit exhaustion requirement, a district court may in its discretion require such exhaustion”).

As noted above in the section entitled, “5 U.S.C. § 552a(g)(1)(A) - Amendment Lawsuits,” access lawsuits differ in this respect from amendment lawsuits. See also, e.g., Kvech v. Holder, No. 10-cv-545, 2011 WL 4369452, at *8 (D.D.C. Sept. 19, 2011) (“While the Privacy Act requires that plaintiffs first resort to administrative remedies for denials of requests to amend records, . . . the statute does not contain a similar requirement with respect to an access claim.”). Because subsection (d)(2) regarding amendment by its terms requires exhaustion, that requirement is jurisdictional in nature. See 5 U.S.C. § 552a(d)(2); see also Quinn v. Stone, 978 F.2d 126, 137-38 (3d Cir. 1992) (“These provisions entail a requirement that the plaintiff exhaust her administrative remedies before she can take advantage of [subsection (g)(1)(A)]” (citing Dickson v. OPM, 828 F.2d 32, 40-41 (D.C. Cir. 1987))). But see Singh v. DHS, No. 1:12cv00498, 2013 WL 1704296, at *10-12 (E.D. Cal. Apr. 19, 2013) (following Taylor, a Privacy Act access case, and finding exhaustion requirement for the plaintiff’s amendment claim as non-jurisdictional).

Plaintiffs’ access requests must conform to agency regulations to exhaust administrative remedies.

Nearly all courts have concluded that plaintiffs fail to exhaust administrative remedies if their access requests do not conform to agency regulations. See, e.g., Vaughn v. Danzig, 18 F. App’x 122, 125 (4th Cir. 2001) (per curiam) (affirming district court’s summary judgment for agency because plaintiff’s “telephonic request for the record before it was destroyed did not comply with the requirement for submitting a request under the Freedom of Information Act, Privacy Act, or Navy regulations implementing those statutes”); Taylor, 127 F.3d at 473-78 (upholding dismissal of plaintiff’s request because plaintiff’s “Privacy Act requests plainly did not comply with [agency] regulations because he did not list the systems that he wished to have searched, their location, and the business address of the systems officer”); Powell v. IRS, 317 F. Supp. 3d 266 (D.C.C. 2018) (concluding that plaintiff failed to exhaust all but one request because he did not comply with agency requirements to clearly mark request or to

state that request was pursuant to statute), reconsidered in nonpertinent part, Powell v. IRS, No. CV 17-278, 2018 WL 10196621, at *1 (D.D.C. Sept. 12, 2018); Powell v. IRS, 255 F. Supp. 3d 33, 42 (D.D.C. 2017) (dismissing same plaintiff's earlier suit because he referred only to FOIA in his initial request and failed to file any proper request under agency's Privacy Act regulations); Haley v. SSA, No. JKB-14-3775, 2015 WL 3745618 (D. Md. June 11, 2015) (dismissing complaint because plaintiff did not mail request to proper office or properly identify records requested); Canada v. Soc. Sec. of Worcester Mass., No. 14-40041-TSH, 2014 U.S. Dist. LEXIS 198790, at *4-5 (D. Mass. 2014) (concluding that plaintiff failed to state cause of action because he did not allege that he had asked for document in question under agency's Privacy Act regulations); Godaire v. Napolitano, No. 3:10cv01266, 2010 WL 6634572, at *7 (D. Conn. Nov. 17, 2010); Ioane v. Comm'r of IRS, No. 3:09-CV-00243, 2010 WL 2600689, at *4 (D. Nev. Mar. 11, 2010); Sterrett v. Navy, No. 09-CV-2083, 2010 WL 330086, at *3-4 (S.D. Cal. Jan. 20, 2010); Gadd v. United States, No. 4:08CV04229, 2010 WL 60953, at *12 (E.D. Ark. Jan. 5, 2010), aff'd, 392 F. App'x 503 (8th Cir. 2010); Ramstack v. Army, 607 F. Supp. 2d 94, 102-03 (D.D.C. 2009); Willis v. DOJ, 581 F. Supp. 2d 57, 69-70 (D.D.C. 2008); Mulhern v. Gates, 525 F. Supp. 2d 174, 187 (D.D.C. 2007); Brown v. DOJ, No. 02-2662, slip op. at 20-24 (N.D. Ala. June 21, 2005); MacLeod v. IRS, No. 99-1088, 2001 U.S. Dist. LEXIS 9327, at *3-4 (S.D. Cal. June 4, 2001); Broadrick v. Exec. Office of the President, 139 F. Supp. 2d 55, 61 (D.D.C. 2001), aff'd per curiam, No. 01-5178 (D.C. Cir. May 1, 2002); Scaife v. IRS, No. 02-1805, 2003 U.S. Dist. LEXIS 22661, at *8 (D.D.C. Nov. 20, 2003); Flowers v. Exec. Office of the President, 142 F. Supp. 2d 38, 44 (D.D.C. 2001); Walker v. Henderson, No. 98 C 3824, 1999 WL 39545, at *9 (N.D. Ill. Jan. 20, 1999), appeal voluntarily dismissed, No. 99-1615 (7th Cir. May 27, 1999); Reeves v. United States, No. 94-1291, 1994 WL 782235, at *2 (E.D. Cal. Nov. 16, 1994), aff'd, 108 F.3d 338 (9th Cir. 1997) (unpublished table decision); Taylor v. Def. Fin. & Accounting Servs., No. 2:12-2466, 2014 U.S. Dist. LEXIS 268, at *16-25 (E.D. Cal. Jan. 3, 2014); Fields v. IRS, No. 12-14753, 2013 WL 3353921, at *3 (E.D. Mich. July 3, 2013); Cross v. Potter, No. 3:09-CV-1293, 2013 WL 1149525, at *9 (N.D.N.Y. Mar. 19, 2013); Guzman v. United States, No. S-93-1949, slip op. at 3-5 (E.D. Cal. Oct. 5, 1994); Hass v. Air Force, 848 F. Supp. 926, 930 (D. Kan. 1994); Gergick v. Austin, No. 89-0838-CV-W-2, 1992 U.S. Dist. LEXIS 7338, at *13-16 (W.D. Mo. Apr. 29, 1992), aff'd, No. 92-3210 (8th Cir. July 9, 1993); Wood v. IRS, No. 1:90-CV-2614, 1991 U.S. Dist. LEXIS 19707, at *8 (N.D. Ga. July 26, 1991); Searcy v. SSA, No. 91-C-26 J, slip op. at 8-11 (D. Utah June 25, 1991) (magistrate's recommendation), adopted, (D. Utah Sept. 19, 1991), aff'd, No. 91-4181, 956 F.2d 278 (10th Cir. 1992) (unpublished table decision); Crooker v. Marshals Serv., 577 F. Supp. 1217, 1217-18 (D.D.C. 1983); Lilienthal v. Parks, 574 F. Supp. 14, 18 & n.7 (E.D.

Ark. 1983); Gibbs v. Rauch, No. 77-59, slip op. at 2-3 (E.D. Ky. Feb. 9, 1978); Larsen v. Hoffman, 444 F. Supp. 245, 256 (D.D.C. 1977); cf. Banks v. DOJ, 605 F. Supp. 2d 131, 139 (D.D.C. 2009) (concluding that plaintiff failed to exhaust administrative remedies with respect to instant request because he did not pay record duplication fees for earlier request); Nurse v. Sec’y of the Air Force, 231 F. Supp. 2d 323, 331 (D.D.C. 2002) (“[W]hile the FOIA requires that a request must ‘[reasonably] describe’ the records, Privacy Act requests require greater specificity.”); but see Clutter v. Perdue, No. H-18-310, 2019 WL 1589942, at *7 (S.D. Tex. Jan. 28, 2019) (allowing plaintiff’s claim to proceed without explicitly considering his compliance with agency requirements because he sufficiently pled that he submitted a FOIA/Privacy Act request for records but that the request was not acknowledged and that records were not produced).

In access suits, plaintiffs generally must file an administrative appeal to exhaust administrative remedies.

The courts also generally have dismissed a plaintiff’s complaint for failure to exhaust administrative remedies if the plaintiff did not file an administrative appeal to an agency’s denial of the access request. See Lopez v. NARA, 301 F. Supp. 3d 78, 90 (D.D.C. 2018) (dismissing plaintiff’s Privacy Act claim for failure to exhaust administrative remedies where plaintiff “never internally appealed NARA’s determination, and plaintiff never sent a proper request to CIA”); Kearns v. FAA, 312 F. Supp. 3d 97, 107 (D.D.C. 2018) (finding that because plaintiff “did not appeal the FAA’s determination regarding his November 2015 Privacy Act request, Kearns did not pursue the full extent of his administrative remedies”); Varad v. United States Dep’t of Treasury, No. 18-91338-RGS, 2018 WL 3849861, at *2 (D. Mass. Aug. 13, 2018) (dismissing plaintiff’s complaint because her access requests were submitted to agency less than 30 days ago, suggesting that requester had not yet filed or completed appeal); Barouch v. DOJ, 422 F. Supp. 2d 30, 67-68 (D.D.C. 2013); Yee v. Solis, No. C-08-4259, 2010 WL 1655816, at *14 (N.D. Cal. Apr. 22, 2010), aff’d on other grounds, No. 10-16376, 2012 WL 902895 (9th Cir. Mar. 19, 2012); Gadd, 2010 WL 60953, at *12; Bettweiser v. Lucas, No. 06-CIV-0142, 2007 WL 2601089, at *2 (D. Idaho Sept. 10, 2007); Clemmons v. DOJ, No. 06-00305, 2007 WL 1020796, at *5 (D.D.C. Mar. 30, 2007); Sussman v. DOJ, No. 03-3618, 2006 WL 2850608, at *5 (E.D.N.Y. Sept. 30, 2006); Glenn v. Rumsfeld, No. C 05-01787, 2006 WL 515626, at *6-7 (N.D. Cal. Feb. 28, 2006); Biondo v. Navy, 928 F. Supp. 626, 630-33 (D.S.C. 1995), aff’d, 86 F.3d 1148 (4th Cir. 1996) (unpublished table decision); Hass v. Air Force, 848 F. Supp. 926, 930 (D. Kan. 1994); cf. Ramstack, 607 F. Supp. 2d at 104 (holding defendant bears burden of proving affirmative defense of failure to exhaust

administrative remedies). But see Fischer v. FBI, No. 07-2037, 2008 WL 2248711, at *2 (D.D.C. May 29, 2008) (excusing failure to file administrative appeal where agency had previously remanded request on administrative appeal and requester apparently did not understand that he had to file second appeal after agency reprocessed the request); Mumme v. Labor, 150 F. Supp. 2d 162, 171 (D. Me. 2001) (refusing to “strictly apply formalistic procedural rules against [p]laintiff” because “[p]rocedural rules . . . cut both ways,” and it was not clear that agency’s response letter “included any written explanation of the partial grant of [p]laintiff’s appeal as required by [its] regulation”), aff’d, No. 01-2256 (1st Cir. June 12, 2002).

An agency’s failure to meet its own deadlines does not constructively exhaust an individual’s administrative remedies.

The Court of Appeals for the Fourth Circuit and several district courts have noted that an individual cannot “constructively exhaust” administrative remedies under the Privacy Act – i.e., deem that administrative remedies are exhausted where the agency failed to timely respond – because “the Privacy Act contains no equivalent to FOIA’s ‘constructive exhaustion’ provision [5 U.S.C. § 552(a)(6)(C)].” Pollack v. DOJ, 49 F.3d 115, 116 n.1, 118-19 (4th Cir. 1995) (indicating that only FOIA claim was properly before district court because “Privacy Act contains no equivalent to FOIA’s ‘constructive exhaustion’ provision which . . . enabled the district court to review his FOIA request”); see also Kearns v. FAA, 312 F. Supp. 3d at 107 (D.D.C. 2018) (concluding that although plaintiff argued that he “‘constructively exhausted’ his Privacy Act claims, . . . the law is clear that such a route to exhaustion is not available under the statute”); Gadd, 2010 WL 60953, at *12 (citing Pollack and dismissing access claim for failure to exhaust administrative remedies); Barouch v. DOJ, 962 F. Supp. 2d at 68 (stating that no equivalent constructive exhaustion provision exists under Privacy Act and finding “that plaintiff failed to exhaust his administrative remedies with respect to his [Privacy Act] request to EOUSA” and accordingly, court lacked subject matter jurisdiction); Sussman v. DOJ, No. 03-3618, 2006 WL 2850608, at *5 (E.D.N.Y. Sept. 30, 2006) (“The Privacy Act . . . does not allow for ‘constructive exhaustion,’ and prohibits a requester from filing an action without having obtained a response from the agency.”); Anderson v. USPS, 7 F. Supp. 2d 583, 586 n.3 (E.D. Pa. 1998) (citing Pollack for proposition that “Privacy Act contains no section equivalent to the ‘constructive exhaustion’ provision of the FOIA,” but alternatively finding that access suit must be dismissed for failure to exhaust administrative remedies), aff’d, 187 F.3d 625 (3d Cir. 1999) (unpublished table decision); cf. Johnson v. FBI, No. 94-1741, slip op. at 6 (D.D.C. Aug. 31, 1995) (citing Pollack but determining that

“since plaintiff has sought an action in equity, and has not exhausted his administrative remedies through administrative appeal . . . plaintiff is barred from seeking injunctive relief under the Privacy Act”).

An agency’s failure to comply with its own regulations, however, can undercut an exhaustion defense. See Jonsson v. IRS, No. 90-2519, 1992 WL 115607, at *1 (D.D.C. May 4, 1992); Haldane v. Comm’r, No. 90-654M, 1990 U.S. Dist. LEXIS 11612, at *4-6 (W.D. Wash. Aug. 23, 1990).

2. Standard and Scope of Review

Access suits are reviewed in the federal courts de novo.

The civil remedies subsection for access suits establishes parameters for such suits, including the standard of judicial review. In civil actions for access, courts “shall determine the matter de novo.” 5 U.S.C. § 552a(g)(3)(A). See Doe v. United States, 821 F.2d 694, 697-98 (D.C. Cir. 1987) (en banc); Barouch v. DOJ, 87 F. Supp. 3d 10, 32 (D.D.C. 2015). Courts may review records in camera to determine whether any of the exemptions set forth in subsection (k) apply. See 5 U.S.C. § 552a(g)(3)(A). Furthermore, in Privacy Act access cases, courts may rely on agency affidavits or declarations to enter summary judgment in favor of the government, e.g., an affidavit describing search terms and type of search performed to demonstrate that agency conducted an adequate search. Elgabrownny v. CIA, No. 17-CV-00066, 2019 WL 1440345 (D.D.C. Mar. 31, 2019) (citing Chambers v. Interior, 568 F. 3d 998, 1003 (D.C. Cir. 2009)). For more detailed discussions of these topics, see “Individual’s Right of Access” section above and “Ten Exemptions, Seven Specific Exemption Rules Agencies May Promulgate” section below.

Once an agency provides the requested records, any pending access claim is moot.

Several courts have recognized that jurisdiction to consider a Privacy Act access claim exists only if the government has failed to comply with a request for records; once a request is complied with and the responsive records have been disclosed, a Privacy Act access claim is moot. See Jackson v. Shinseki, 526 F. App’x 814, 817 (10th Cir. 2013) (affirming district court’s decision that plaintiff’s claim was moot because “defendants had ‘provided [appellant] with copies of all responsive documents in their possession,’ thus agency was ‘discharg[ed] of their obligations under the Privacy Act’”); Campbell v. SSA, 446 F. App’x 477, 480 (3d Cir. 2011); Yonemoto v. VA, 305 F. App’x 333, 334 (9th Cir. 2008); Lovell v. Alderete, 630 F.2d 428, 430 (5th Cir. 1980) (dismissing both FOIA and Privacy Act claims as moot where

“[e]ven though the information [plaintiff sought] was delivered late, [plaintiff] now has all of the information he requested”); Crummey v. SSA, 794 F. Supp. 2d 46, 61 (D.D.C. June 30, 2011), aff’d per curiam, No. 11-5231, 2012 WL 556317 (D.C. Cir. Feb. 6, 2012); Dickerson v. SSA, No. A-10-CA-795-SS, 2011 WL 1332426, at *4 (W.D. Tex. June 8, 2011); Sterrett, 2010 WL 330086, at *2-3; Jordan v. DOJ, No. 07-cv-02303, 2009 WL 2913223, at *26 (D. Colo. Sept. 8, 2009); Van Allen v. HUD, No. G-07-315, 2009 WL 1636303, at *1 (S.D. Tex. June 9, 2009); Falwell v. Exec. Office of the President, 158 F. Supp. 2d 734, 740 (W.D. Va. 2001); Mumme, 150 F. Supp. 2d at 171-72; Fisher v. FBI, 94 F. Supp. 2d 213, 216 (D. Conn. 2000) (finding that plaintiff’s claim was moot where agency provided material and that “[t]he fact that the records came after some delay is not necessarily tantamount to an improper denial of the records”); Jacobs v. Reno, No. 3:97-CV-2698-D, 1999 U.S. Dist. LEXIS 3104, at *14-15 (N.D. Tex. Mar. 11, 1999) (dismissing access claim as moot where plaintiff had received access to records and finding no eligibility for award of attorney fees and costs based on plaintiff’s assertion that his lawsuit may have caused agency to comply with Privacy Act when it would not otherwise have done so, “particularly when § 552a(d)(1) imposes no deadline for agency compliance and absent evidence of extended and unjustified delay”), aff’d, 208 F.3d 1006 (5th Cir. 2000) (unpublished table decision) Biondo, 928 F. Supp. at 631; Letscher v. IRS, No. 95-0077, 1995 WL 555476, at *1 (D.D.C. July 6, 1995); Polewsky v. SSA, No. 5:93-CV-200, slip op. at 9-10 (D. Vt. Mar. 31, 1995) (magistrate’s recommendation), adopted, (D. Vt. Apr. 13, 1995), aff’d, No. 95-6125, 1996 WL 110179, at *2 (2d Cir. Mar. 12, 1996); Smith v. Cont’l Assurance Co., No. 91 C 0963, 1991 WL 164348, at *3 (N.D. Ill. Aug. 22, 1991); cf. Riser v. State, No. 09-3273, 2010 WL 4284925, at *7 (S.D. Tex. Oct. 22, 2010) (dismissing claim “seek[ing] a declaratory judgment that the agencies’ earlier withholding of his records . . . was improper” as moot “because the documents have now been produced”); Yee, 2010 WL 1655816, at *14 (asserting that Privacy Act claim for access was moot where magistrate judge in prior order had found that agency complied with his order to produce the record at issue to plaintiff).

Some courts have required plaintiffs to allege that an agency’s failure to provide access was improper, not simply that the request was denied.

To maintain an access lawsuit under subsection (g)(1)(B), the plaintiff must allege not only that access was requested and denied, but also that the denial or failure to act on the request was improper. See Camper v. NSA, No. 1:18-cv-01794-PWG, 2019 WL 3841940, at *5 (D. Md. Aug. 15, 2019) (holding that plaintiff failed to allege what was improper about agency’s

stated legal grounds for denial, citing Singh v. DHS, No. 12-498-AWI, 2014 WL 67254, at *4 (E.D. Cal. Jan. 8, 2014), Biondo, 928 F. Supp. at 631 (D.S.C. 1995), and Bruan v. Agency, No. 15-18-H-DLC-JTJ, 2015 WL 12591720, at *1 (D. Mont. Oct. 30, 2015)); Fleischman v. Comm’r of Soc. Sec., No. 3:15-CV-897-J-PDB, 2016 WL 7474577 (M.D. Fla. Dec. 29, 2016); cf. Beach v. DHS, No. CV 08–00420–RGK, 2008 WL 11337801, at *2 (C.D. Cal. Sept. 2, 2008) (plaintiff sufficiently stated claim for relief under subsection (g)(1)(B) by alleging that agency refused to disclose documents after multiple requests).

Most courts have considered access to tax records under the Internal Revenue Code, rather than the Privacy Act.

The Court of Appeals for the District of Columbia Circuit has ruled that “the specific provisions of [26 U.S.C.] § 6103 rather than the general provisions of the Privacy Act govern the disclosure of . . . tax information” and that “individuals seeking ‘return information’ . . . must do so pursuant to § 6103 of the Internal Revenue Code, rather than the Privacy Act.” Lake v. Rubin, 162 F.3d 113, 115-16 (D.C. Cir. 1998). In reaching this conclusion, the D.C. Circuit looked to the legislative history of § 6103 and embraced an earlier ruling by the Court of Appeals for the Seventh Circuit, Cheek v. IRS, 703 F.2d 271, 272 (7th Cir. 1983) (per curiam), that similarly had held that § 6103 “displaces” the Privacy Act and shields tax return information from release to a first-party requester. See also Kendrick v. Wayne Cnty., No. 10-13752, 2011 WL 2580675, at *1-2 (E.D. Mich. June 29, 2011); Paige v. IRS, No. 1P-85-64-C, slip op. at 3-4 (S.D. Ind. Jan. 13, 1986); cf. Maxwell v. O’Neill, No. 00-01953, 2002 WL 31367754, at *4 (D.D.C. Sept. 12, 2002) (“while [section] 6103 may supersede the Privacy Act, it does not supersede the FOIA”), *aff’d*, No. 04-5082 (D.C. Cir. May 27, 2005). *But cf.* Sinicki v. Treasury, No. 97 CIV. 0901, 1998 WL 80188, at *3-5 (S.D.N.Y. Feb. 24, 1998) (finding Cheek unpersuasive in context of wrongful disclosure claim and denying motion to dismiss Privacy Act claim, stating that “the language, structure, purpose and legislative history of Section 6103 do not make manifest and clear a legislative intent to repeal the Privacy Act as it applies to tax return information”).

The Court of Appeals for the Ninth Circuit has interpreted 26 U.S.C. § 7852(e) to likewise prevent Privacy Act access to records pertaining to tax liability. Jacques v. IRS, 972 F.2d 1339 (unpublished disposition), 1992 WL 185449, at *2 (9th Cir. Aug. 5, 1992); O’Connor v. United States, No. 89-15321, slip op. at 5 (9th Cir. June 4, 1991); see also Prince v. Comm’r, No. 98-17183, 1999 WL 511185, at *1 (9th Cir. July 15, 1999) (concluding that district court lacked subject matter jurisdiction over claim for attorney fees in

Privacy Act suit for access to tax return records due to 26 U.S.C. § 7852(e)'s prohibition against application of subsection (g) of Privacy Act to determinations of tax liability); Hart v. United States, No. 00-2158, 2000 WL 1727737, at *1-2 (E.D. Pa. Sept. 27, 2000) (following Maxwell v. Rubin, infra, and dismissing access claim for lack of subject matter jurisdiction for records relating, "directly and indirectly, to tax disputes with the IRS concerning liability," because although § 7852(e) does not exempt the IRS from the access provision, it does exempt it from the civil remedy provision), aff'd, 275 F.3d 35 (3d Cir. 2001) (unpublished table decision); Weiss v. Sawyer, 28 F. Supp. 2d 1221, 1227-28 (W.D. Okla. 1997) (applying 26 U.S.C. § 7852 to prevent apparent access claim); cf. Baker v. Matson, No. 98 M 1675, 1998 U.S. Dist. LEXIS 21312, at *8-9 (D. Colo. Dec. 7, 1998) (ruling that court had no jurisdiction over Privacy Act access claim) (magistrate's recommendation), adopted, No. 98 M 1675, 1999 WL 521287 (D. Colo. Jan. 12, 1999). The Ninth Circuit's rationale differs from the rationale applied by the D.C. Circuit, however. Cf. Lake v. Rubin, 162 F.3d at 114-16 (affirming judgments of district court "not on the jurisdictional rationale contained in" opinions in the Ninth Circuit based on § 7852, which the D.C. Circuit questioned, but instead on the basis of 26 U.S.C. § 6103, which provides the exclusive means by which individuals may obtain their tax records); Wood v. IRS, No. 1:90-CV-2614, 1991 U.S. Dist. LEXIS 19707, at *1, 8 (N.D. Ga. July 29, 1991) (denying plaintiff summary judgment on its Privacy Act claim for access to tax records, based on plaintiff's failure to exhaust remedies, without addressing whether court had jurisdiction to review the claim in light of § 7852 or § 6103).

3. Remedies

Courts can order agencies to produce the requested records; monetary damages, however, are not available in access cases.

In access lawsuits, courts can enjoin the agency from withholding records and order their production to the individual. See 5 U.S.C. § 552a(g)(3)(A); Kursar v. Transportation Sec. Admin., 581 F. Supp. 2d 7, 19 (D.D.C. 2008) (citing Doe v. Stephens, 851 F.2d 1457, 1463 (D.C. Cir. 1988)); Dick v. Holder, 67 F. Supp. 3d 167, 187 (D.D.C. 2014) (citing, inter alia, Kursar).

Lastly, damages are not recoverable in an access case. See Benoist v. United States, No. 87-1028, slip op. at 3 (8th Cir. Nov. 4, 1987); Thurston v. United States, 810 F.2d 438, 447 (4th Cir. 1987); Kvech, 2011 WL 4369452, at *8 n.13; Brown v. DOJ, No. 02-2662, slip op. at 27 (D. Ala. June 21, 2005); Haddon v. Freeh, 31 F. Supp. 2d 16, 22 (D.D.C. 1998); Vennes v. IRS, No. 5-88-36, slip

op. at 6-7 (D. Minn. Oct. 14, 1988) (magistrate’s recommendation), adopted, (D. Minn. Feb. 14, 1989), aff’d, No. 89-5136MN, 890 F.2d 419 (8th Cir. 1989) (unpublished table decision); Bentson v. Comm’r, No. 83-048-GLO-WDB, slip op. at 2 (D. Ariz. Sept. 14, 1984); see also Quinn v. HHS, 838 F. Supp. 70, 76 (W.D.N.Y. 1993) (citing Thurston in dictum). But cf. Beattie v. Astrue, 845 F. Supp. 2d 184, 195 (D.D.C. 2012) (ruling that plaintiff “failed to make out a claim under the Privacy Act” because agency’s responses did not meet the intentional and willful standard); Robinson v. Watkins, No. 4:11cv89, 2011 WL 6029969, at *5 (E.D. Va. Oct. 13, 2011) (“The relief provided [under the Privacy Act] is that the plaintiff will be given access to the record, and for monetary damages if an agency’s persistent refusal to allow access is ‘intentional and willful.’”); Riser, 2010 WL 4284925, at *7 (“Plaintiff’s factual assertions about his repeated Privacy Act requests and the delay in receiving records are insufficient to raise an inference of willful or intentional withholding of records about him.”); Fischer v. DOJ, 723 F. Supp. 2d 104, 115 (D.D.C. 2010) (refusing to award damages on ground that agency “neither inappropriately withheld information nor acted in bad faith” where plaintiff sought damages pursuant to subsection (g)(1)(D) in connection with his access request).

C. 5 U.S.C. § 552a(g)(1)(C) - Damages Lawsuits for Failure to Assure Fairness in Agency Determination

“Whenever any agency . . . fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual . . . the individual may bring a civil action against the agency.” 5 U.S.C. § 552a(g)(1)(C).

Comment:

Subsection (g)(1)(C) allows individuals to sue an agency for failure to maintain records with such “accuracy, relevance, timeliness, and completeness” as is necessary to assure fairness in agency determinations.

This section provides a civil remedy against an agency that does not maintain its records in accordance with the requirements of section (e)(5) of the Privacy Act. The standard for maintaining records under this provision is identical to the standard under subsection (e)(5), which requires agencies to maintain records used in making determinations about individuals “with such accuracy,

relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination.” See, e.g., *Lettersworth v. FDIC*, 248 F.3d 386, 390 n.3 (5th Cir. 2001) (explaining that the “statutory obligation” imposed by subsection (e)(5) “is made enforceable by substantively identical language in subsection 552a(g)(1)(C)”); *Doe v. United States*, 821 F.2d 694, 698 n.10 (D.C. Cir. 1987) (en banc) (concluding that agency record met accuracy standard although subsection (e)(5) “uses the phrase ‘reasonably necessary to assure fairness’ whereas subsection (g)(1)(C) does not include the word ‘reasonably.’ We attribute no substantive significance, for the issue at hand, to the omission of the word ‘reasonably’ in § 552a(g)(1)(C).”); *Gard v. Dep’t of Educ.*, 789 F. Supp. 2d 96, 106 (D.D.C. 2011) (explaining that claim alleging violation of subsection (e)(5) “is entirely duplicative” of claim alleging violation of subsection (g)(1)(C) because “[c]laims predicated upon violations of Section 552a(e)(5) . . . must be brought under 552a(g)(1)(C).”).

The key element of the standard – the necessity ‘to assure fairness in any determination’ – calls for a balanced judgment, one inherently involving a reasonableness criterion. *Edison v. Army*, 672 F.2d 840, 843 (11th Cir. 1982) (concluding that although it “must be read in pari materia with subsection (e)(5),” “[i]f the court determines that the agency has done what is reasonable in assuring the accuracy of the information, no more is required.”).

Assuming that an individual meets the requirements for establishing an agency’s failure to maintain a record concerning an individual with “accuracy, relevance, timeliness, and completeness,” “actual damages” sustained by the individual, but in no case less than \$1000, are recoverable. See 5 U.S.C. § 552a(g)(4)(A). The meaning of “actual damages” and the \$1000 minimum recovery provision are discussed below under “Principles Applicable to Damages Lawsuits, Actual Damages.”

1. Exhaustion of Administrative Remedies

Most courts have concluded that plaintiffs are not required to exhaust administrative remedies to obtain damages under (g)(1)(C).

Most courts have concluded that exhaustion of administrative remedies is not a prerequisite to a civil action for damages under subsection (g)(1)(C). For example, in *Hewitt v. Grabicki*, 794 F.2d 1373, 1379 (9th Cir. 1986), the Ninth Circuit contrasted subsection “(g)(1)(A) (action for order to amend record permitted when agency review resulted in denial of request or agency refused to review)” with subsection “(g)(1)(C) (permits action where agency’s failure to maintain proper records results in adverse determination

against individual)” to conclude that “[e]xhaustion of administrative remedies is not a precondition to bringing an action for damages under the Privacy Act.” Phillips v. Widnall, No. 96-2099, 1997 WL 176394, at *2-3 (10th Cir. Apr. 14, 1997); Hubbard v. EPA, 809 F.2d 1, 7 (D.C. Cir. 1986), vacated in nonpertinent part & reh’g en banc granted (due to conflict within circuit), 809 F.2d 1 (D.C. Cir. 1986), resolved on reh’g en banc sub nom. Spagnola v. Mathis, 859 F.2d 223 (D.C. Cir. 1988); Nagel v. HEW, 725 F.2d 1438, 1441 & n.2 (D.C. Cir. 1984); Johnson v. Air Force, No. CV F 09-0281, 2010 WL 1780231, at *6 (E.D. Cal. Apr. 30, 2010) (citing Hewitt, aff’d on other grounds, 465 F. App’x 644 (9th Cir. 2012)); Reitz v. USDA, No. 08-4131, 2010 WL 786586, at *11 n.12 (D. Kan. Mar. 4, 2010); Murphy v. United States, 121 F. Supp. 2d 21, 28 (D.D.C. 2000), aff’d per curiam, 64 F. App’x 250 (D.C. Cir. 2003); M.K. v. Tenet, 99 F. Supp. 2d 12, 20 (D.D.C. 2000) (quoting Nagel); Gergick v. Austin, No. 89-0838-CV-W-2, 1992 U.S. Dist. LEXIS 7338, at *13-16 (W.D. Mo. Apr. 29, 1992), aff’d, No. 92-3210 (8th Cir. July 9, 1993).

A few other courts have found otherwise, however, requiring plaintiff to exhaust administrative remedies before bringing an (e)(5) claim under (g)(1)(C). Moore v. Potter, No. 3:04-CV-1057, 2006 WL 2092277, at *8 (M.D. Fla. July 26, 2006); see, e.g., Olivares v. NASA, 882 F. Supp. 1545, 1546, 1552 (D. Md. 1995) (concluding that plaintiff’s failure to exhaust administrative remedies precludes damages claim under subsection (e)(5)), aff’d, 103 F.3d 119 (4th Cir. 1996) (unpublished table decision); Graham v. Hawk, 857 F. Supp. 38, 40 (W.D. Tenn. 1994) (stating that “[e]ach paragraph of 5 U.S.C. § 552a(g) . . . requires as a prerequisite to any action that the agency refuse an individual’s request to take some corrective action regarding his file”), aff’d, 59 F.3d 170 (6th Cir. 1995) (unpublished table decision).

A provision of the Prison Litigation Reform Act of 1996 (“PLRA”), 42 U.S.C. § 1997e(a) (2018), requires inmates to exhaust administrative remedies prior to bringing an “action . . . with respect to prison conditions,” which may include accuracy of records and requests for correction. 42 U.S.C. § 1997e(a). However, when the inmate seeks remedies concerning accuracy pursuant to subsection (e)(5)/(g)(1)(C) and correction of records under (d)(2) in a system of records that maintains exemptions of (e)(5) and (d)(2), this provision of the PLRA has minimal practical effect. See Barnett v. United States, 195 F. Supp. 3d 4, 8 (D.D.C. 2016) (any claims for correction of alleged erroneous information contained in an inmate’s central file, including presentence reports, fails because BOP has exempted its Inmate Central Record System from Privacy Act’s (e)(5) accuracy and (d)(2) amendment requirements under (j)(2), 28 C.F.R. § 16.97(j)). But cf. McCulough v. BOP, No. 1:06-cv-00563, 2011 WL 3568800, at *3-4 (E.D. Cal. Aug. 12, 2011) (recommending

dismissal of claim that “BOP violated the Privacy Act through its maintenance of inaccurate records and use of those records as the basis for decisions that adversely affected Plaintiff” on ground that plaintiff failed to satisfy exhaustion requirement of PLRA) (magistrate’s recommendation), adopted, 2011 WL 4373939 (E.D. Cal. Sept. 19, 2011). For a discussion of the exhaustion requirement imposed by the PLRA on claims for damages brought by prisoners under subsection (g)(1)(D), see the discussion below under “5 U.S.C. § 552a(g)(1)(C) - Damages Lawsuits for Failure to Comply with Other Privacy Act Provisions.”

2. Elements of a Damages Claim

In a suit for damages under subsection (g)(1)(C), an individual has the burden of proving that: (1) he or she “has been aggrieved by an adverse determination”; (2) the agency “failed to maintain his or her records with the degree of accuracy necessary to assure fairness in the determination”; (3) the agency’s “reliance on the inaccurate records was the proximate cause of the adverse determination”; and (4) the agency “acted intentionally or willfully in failing to maintain accurate records.” Deters v. U.S. Parole Comm’n, 85 F.3d 655, 657 (D.C. Cir. 1996).

In most cases, courts have found that plaintiffs have not met one or more of these elements and, therefore, were not entitled to damages

a. First Element: Aggrieved by Adverse Determination

Considering the first requirement for a damages suit under subsection (g)(1)(C), the courts often have concluded that the plaintiff was not “aggrieved” or that the agency action at issue did not constitute an “adverse determination.” See, e.g., Bettersworth v. FDIC, 248 F.3d 386, 392-93 (5th Cir. 2001) (holding that Federal Reserve Bank letter informing company that its application was unlikely to be approved did not constitute “adverse determination” against plaintiff because there were “diverse grounds relied upon in the Reserve Bank’s letter,” entity applying was company, not plaintiff, and “informal oral or written statements made in the deliberative process about a particular administrative determination do not constitute the determination itself”); Jarrell v. Army Review Bd. Agency, No. 3:19-CV-00349, 2020 WL 2128612, at *3 (S.D. Ohio May 5, 2020), report and recommendation adopted sub nom. Jarrell v. Army Review Boards Agency, No. 3:19-CV-00349, 2020 WL 2909969 (S.D. Ohio June 3, 2020) (plaintiff did not establish that he was “aggrieved” by inaccuracy in brother’s record because under subsection

552a(g)(1)(C), “only ‘the individual’ with inaccurate records who has suffered an adverse determination may bring a § 552a(g)(1)(C) action”); Yusim v. SSA, 406 F. Supp. 3d 194, 196 (E.D.N.Y. 2018) (finding that SSA’s allegedly inaccurate listing of claimant’s application date for benefits did not violate his Privacy Act rights, where he did not claim that failure to maintain accurate records was done intentionally or willfully or that he suffered adverse determination); Melvin v. SSA, 126 F. Supp. 3d 584, 606 (E.D.N.C. 2015) (dismissing plaintiff’s (g)(1)(C) claim because there was “no adverse agency determination resulting from the SSA’s alleged failure to maintain the September 29, 2010, appeal letter” and no decision had been made by SSA with regard to plaintiff’s benefits); Scott v. Conley, 937 F. Supp. 2d 60, 78 (D.D.C. 2013) (dismissing plaintiff’s Privacy Act claim for failure to allege “some adverse effect,” because plaintiff “has not alleged facts to show that she has suffered or is suffering any adverse determination or effect because of BOP’s alleged failure to comply with the requirement that it collect only ‘relevant and necessary’ information”); Elliott v. BOP, 521 F. Supp. 2d 41, 56 (D.D.C. 2007) (“The fact that Plaintiff was kept at [a particular institution] during [the period during which plaintiff alleged that BOP relied upon inaccurate or incomplete medical records] does not mean that the BOP actually made a ‘determination’ to do so.”); Lee v. Geren, 480 F. Supp. 2d 198, 209-10 (D.D.C. Mar. 29, 2007) (concluding that “mere issuance of a notice of proposed termination does not constitute an ‘adverse determination’ under the Privacy Act” and that “[t]he only ‘adverse determination’ at issue in this case is plaintiff’s fourteen-day suspension,” where plaintiff received notice of proposed termination but was only suspended for two weeks); but see, e.g., Perry v. BOP, 371 F.3d 1304, 1305 (11th Cir. 2004) (relying on Ninth Circuit’s formulation of elements necessary for Privacy Act claim under (g)(1)(C) in Rose v. United States, 905 F.2d 1257, 1259 (9th Cir. 1990), and concluding plaintiffs had alleged necessary elements to state claim, vacating district’s court decision and remanding for district court to consider complaint under Privacy Act); Toolasprashad v. BOP, 286 F.3d 576, 583-86 (D.C. Cir. 2002) (holding that transfer of prisoner in alleged retaliation for exercise of his First Amendment rights constitutes assertion of “adverse determination” under Privacy Act, sufficient to “survive [agency’s] motion to dismiss”); Fleck v. VA OIG, No. CV 18-1452, 2020 WL 42842, at *6-8 (D.D.C. Jan. 3, 2020) (denying VA’s motion to dismiss where second agency’s decision not to hire plaintiff was adverse action, plaintiff sufficiently alleged factual inaccuracies in OIG report, and inaccuracies led to second agency’s failure to hire him).

b. Second Element: Failure to Maintain Accurate, Relevant, Timely and/or Complete Records

Similarly, courts rarely have concluded that an agency failed to maintain accurate records. See, e.g., Jones v. Luis, 372 F. App'x 967, 969-70 (11th Cir. 2010) (per curiam) (ruling that district court properly dismissed Privacy Act claim where plaintiff "does not allege any errors in the BOP's record keeping" but rather merely "alleges that [a BOP official] misused the information in the records to make an adverse determination against" plaintiff); Treadwell v. BOP, 32 F. App'x 519, 520-21 (10th Cir. 2002) (finding plaintiff's claim that BOP erroneously based his security classification in part on nonviolent juvenile robbery offense does not amount to violation of Privacy Act where plaintiff agreed that conviction accurately appeared on his record but disagreed with way BOP used that information); Williams v. BOP, No. 94-5098, 1994 WL 676801, at *1 (D.C. Cir. Oct. 21, 1994) (asserting appellant did not establish either that agency "maintained an inaccurate record or that it made a determination adverse to him in reliance on inaccurate information capable of verification, the statutory prerequisites to maintaining an action pursuant to the Privacy Act"); Hadley v. Moon, No. 94-1212, 1994 WL 582907, at *1-2 (10th Cir. Oct. 21, 1994) (finding plaintiff must allege actual detriment or adverse determination in order to maintain claim under Privacy Act); Ashbourne v. Hansberry, No. 12-cv-01153302, 2015 WL 11303198, at *7-9 (D.D.C. Nov. 25, 2015) (finding that plaintiff failed to allege claim under subsection (g)(1)(C) since plaintiff did not present evidence of a single inaccurate record relied upon by agency when reviewing misleading information provided by plaintiff during pre-employment process), aff'd, 703 F. App'x 3 (D.C. Cir. 2017); Doe v. Rogers, 139 F. Supp. 3d 120, 168 (D.D.C. 2015) (dismissing plaintiff's (g)(1)(C) claim because "only agency 'decision' that arguably meets this definition [of an adverse agency determination] is the Secretarial Review Decision, but, again, the plaintiffs have not identified any inaccurate agency report that the Secretary relied on to reach that decision"); Cross v. Potter, No. 3:09-CV-1293, 2013 WL 1149525, at *9 (N.D.N.Y. Mar. 19, 2013) (dismissing plaintiff's claim under § 552a(g)(1)(C) because "[t]he record of a criminal acquittal is not an inaccuracy within her record simply because [p]laintiff believes that the criminal charge was improperly brought against her"); Kvech v. Holder, No. 10-cv-545, 2011 WL 4369452, at *5-6 (D.D.C. Sept. 19, 2011) (although plaintiff "pled facts sufficient to show she was aggrieved by an adverse determination and the FBI acted intentionally," she "failed to plead facts which might establish" (1) "FBI failed to 'assure fairness' by maintaining inaccurate records; and (2) reliance on the inaccurate records was the

‘proximate cause’ of the adverse determination”); Feldman v. CIA, 797 F. Supp. 2d 29, 44-47 (D.D.C. 2011) (dismissing plaintiff’s (g)(1)(C) claim because plaintiff failed to set forth that agency failed to maintain records with degree necessary to assure fairness in CIA director’s determination, and because plaintiff primarily focused on disagreement with interpretation of legal issues rather than factual errors); Hollins v. Cross, No. 1:09cv75, 2010 WL 1439430, at *5 (N.D. W. Va. Mar. 17, 2010) (“[B]ecause the plaintiff has failed to show that his [presentence investigation report] is actually erroneous, he cannot show that the BOP’s use of that document to make . . . administrative decisions, has had an adverse effect on him.”); Ramirez v. DOJ, 594 F. Supp. 2d 58, 66-67 (D.D.C. 2009) (dismissing plaintiff’s (g)(1)(C) complaint because plaintiff failed to show the records held by defendants were inaccurate), aff’d per curiam on other grounds, No. 10-5016, 2010 WL 4340408 (D.C. Cir. Oct. 19, 2010); Doe v. DOJ, 660 F. Supp. 2d 31, 43 (D.D.C. 2009) (concluding that plaintiff “failed to show that there was an error in the records” by objecting only to “misinterpretation of [accurate] records by DOJ employees, for which there is no remedy under the Privacy Act”); De la Cruz-Jimenez v. DOJ, 566 F. Supp. 2d 7, 9-10 (D.D.C. 2008) (finding that plaintiff failed to establish the threshold requirement of an inaccurate record, thus dismissing plaintiff’s (g)(1)(C) claim); but see, e.g., Perry, 371 F.3d at 1305 (finding plaintiffs had alleged necessary elements to state claim, vacating district’s court decision and remanding for district court to consider complaint under Privacy Act); Fleck v. VA OIG, 2020 WL 42842, at *6-8 (denying VA’s motion to dismiss where second agency’s decision not to hire plaintiff was adverse action, plaintiff sufficiently alleged factual inaccuracies in OIG report, and inaccuracies led to second agency’s failure to hire him); Ashbourne v. Hansberry, 302 F. Supp. 3d 338, 347 (D.D.C. 2018) (finding that plaintiff properly pled in her complaint that defendant DHS failed to maintain accurate records when it intentionally and deliberately failed to verify facts in deciding to terminate plaintiff’s federal employment).

Most cases brought under (g)(1)(C) involve the “accuracy” standard, but the D.C. District Court allowed a case to proceed under the “relevance” component.

Although most litigation pursuant to sections (e)(5)/(g)(1)(C) of the Privacy Act arises from challenges to the accuracy component of the “accuracy, relevance, timeliness, and completeness” standard, the District Court for the District of Columbia has considered a claim alleging irrelevancy. In Gerlich v. DOJ, the court noted that “[m]ost ‘adverse determination’ claims hinge on inaccurate or incomplete records.” 659 F.

Supp. 2d 1, 15 (D.D.C. 2009), aff'd in part, rev'd in part, 711 F.3d 161, 163 (D.C. Cir. 2013). Here, however, the plaintiffs alleged that “irrelevant records (i.e., the records of their First Amendment activities) led to an adverse [hiring] determination against them.” Id. In denying the Department’s motion to dismiss, the court stated: “By the plain language of (g)(1)(C), relevance stands on equal footing with accuracy, timeliness and completeness as a basis for pursuing money damages for an adverse determination.” Id. at 15-16 (holding that summary judgment was inappropriately granted under subsections (e)(5) and (e)(7) claims and concluding “in light of the destruction of appellants’ records, that a permissive spoliation inference was warranted because the senior Department officials had a duty to preserve the annotated applications and internet printouts given that Department investigation and future litigation were reasonably foreseeable”). For a more complete discussion of Gerlich, see the discussion under “5 U.S.C. § 552a(e)(5) - Maintain Accurate, Relevant, Timely, and Complete Records” above.

c. Third element: Proximate Cause

Courts commonly have dismissed an individual’s (g)(1)(c) suit if that individual did not meet the third requirement for such claims, i.e., that the agency’s reliance on inaccurate records was the proximate cause of the adverse determination. See, e.g., Chambers v. Interior, 568 F.3d 998, 1007 (D.C. Cir. 2009) (dismissing plaintiff’s (g)(1)(C) claim because plaintiff failed to show specific adverse determination resulting from agency’s failure to maintain accurate records); Hutchinson v. CIA, 393 F.3d 226, 229-30 (D.C. Cir. 2005) (concluding that plaintiff failed to show that alleged inaccuracies proximately caused adverse determination because record demonstrates that she was dismissed for sustained poor performance spanning three years); Rogers v. BOP, 105 F. App’x 980, 983-84 (10th Cir. 2004) (plaintiff failed to state Privacy Act claim under (g)(1)(C) because he failed to show that inaccurate record caused his eligibility for parole, rather than his legal ineligibility); Gowan v. Air Force, 148 F.3d 1182, 1194 (10th Cir. 1998) (finding no adverse effect from Air Force’s informing Wyoming Bar of court-martial charges preferred against plaintiff where plaintiff himself later informed Wyoming Bar without knowing Air Force had already done so); Williams v. BOP, No. 94-5098, 1994 WL 676801, at *1 (D.C. Cir. Oct. 21, 1994) (asserting appellant did not establish either that agency “maintained an inaccurate record or that it made a determination adverse to him in reliance on inaccurate information capable of verification, the statutory prerequisites to maintaining an action pursuant to the Privacy Act”); Colley v. James,

254 F. Supp. 3d 45, 67 (D.D.C. 2017) (finding that plaintiffs did not establish that the Air Force violated Privacy Act by engaging in willful or intentional conduct because agency had corrected inaccurate information pertaining to their appeal and there was no indication that incorrect information had been relied upon as part of appeal); Gillman v. United States, No. 16-00001, 2017 WL 969180, at *4-5 (D. Hawaii March 13, 2017) (finding that plaintiff “failed to establish the existence of a genuine issue of material fact—namely, whether VA personnel acted intentionally or willfully in maintaining allegedly inaccurate medical records,” and failed to provide “evidence to show that the VA’s maintenance of allegedly inaccurate mental health records caused a required adverse determination or actual damages”); Ashbourne, 2015 WL 11303198, at *7-9 (finding that plaintiff failed to allege claim under subsection (g)(1)(C) where plaintiff did not present evidence of inaccurate record relied upon by agency when reviewing misleading information provided by plaintiff during pre-employment process); Doe v. Rogers, 139 F. Supp. 3d at 168 (dismissing plaintiff’s (g)(1)(C) claim because “only agency ‘decision’ that arguably meets this definition [of an adverse agency determination] is the Secretarial Review Decision, but, again, the plaintiffs have not identified any inaccurate agency report that the Secretary relied on to reach that decision”); Dick v. Holder, 67 F.Supp.3d 167, 183-186 (D.D.C. 2014) (notwithstanding that plaintiff’s claim (g)(1)(C) claim fails because alert FBI issued in response to statements made by plaintiff to agency personnel was exempt from Privacy Act’s maintenance requirements, dismissing claim because even if court accepted plaintiff’s security clearance suspension or mandatory fitness examination as adverse determinations, plaintiff failed to show alert was cause of adverse determinations); Singh v. DHS, No. 1:12-cv-00498, 2014 WL 67254, at *9-11 (E.D. Cal. Jan. 8, 2014) (dismissing plaintiff’s (g)(1)(C) and (g)(1)(D) claims because plaintiff did not allege “sufficient causal connection between the Government’s failure to document the alleged promise to [p]laintiff that he would not be deported in conjunction with his plea and the removal proceedings that were instituted as a result of his conviction”); Scott, 937 F. Supp. 2d at 78 (dismissing plaintiff’s Privacy Act claim for failure to allege “some adverse effect,” because plaintiff “has not alleged facts to show that she has suffered or is suffering any adverse determination or effect because of BOP’s alleged failure to comply with the requirement that it collect only ‘relevant and necessary’ information”); New-Howard v. Shinseki, No. 09-5350, 2012 WL 2362546, at *9 (E.D. Pa. June 21, 2012) (“Plaintiff presents absolutely no evidence of instances in which she was denied leave due to an absence of accrued leave” and “[a]s a consequence, Plaintiff can maintain no cause of action for damages on the basis of the

failure to maintain records regarding her leave.”); Radakovic v. OPM, No. 11-10706, 2012 WL 1900037, at *3 (D. Mass. May 23, 2012) (“Plaintiff does not allege at the time of the ‘adverse determination’ . . . [agency] had any information available” because letter explaining reasons for plaintiff’s separation from former employer was not provided to agency until “two years and one month after plaintiff’s termination” and therefore plaintiff, “as a matter of law, does not allege a § 552a(g)(1)(C) violation.”), aff’d, No. 12-1934 (1st Cir. Apr 10, 2013); Kvech, 2011 WL 4369452, at *5-6 (although plaintiff “pled facts sufficient to show she was aggrieved by an adverse determination and the FBI acted intentionally,” she “failed to plead facts which might establish” (1) “FBI failed to ‘assure fairness’ by maintaining inaccurate records; and (2) reliance on the inaccurate records was the ‘proximate cause’ of the adverse determination.”); Conley v. United States, No. 2:10-cv-444, 2011 WL 1256611, at *6-7 (S.D. Ohio Mar. 31, 2011) (“[A]ny possible recovery under [(g)(1)(C)] is precluded because [plaintiff] has failed to adequately plead that an adverse determination resulted from any of the [agency’s] alleged violations of the Privacy Act.”); Ramey v. Marshals Serv., 755 F. Supp. 2d 88, 96-97 (D.D.C. 2010) (finding that plaintiff did not “set forth specific facts showing a genuine issue for trial on the question of whether the U.S. Marshals relied on inaccurate information in ordering Plaintiff’s removal from the Twelfth Circuit Contract”); Reitz, 2010 WL 786586, at *11 (dismissing plaintiff’s (g)(1)(C) claim because plaintiff failed to show that mistake in Farm Service Agency’s records caused or led to the agency’s adverse determination); Krieger v. DOJ, 529 F. Supp. 2d 29, 49-50 (D.D.C. 2008) (explaining that even if former agency employee’s performance appraisal reports were missing from his file, he “has adduced no evidence that his missing [reports] were the proximate cause of his failure to obtain job offers”); Murphy v. United States, 167 F. Supp. 2d 94, 97-98 (D.D.C. 2001) (stating that although documents delayed plaintiff’s transfer and thus played a part in transfer process, plaintiff “has neither shown that they caused the transfer nor identified a genuine issue of fact that is material to the dispositive issue of causation”), aff’d per curiam, 64 F. App’x 250 (D.C. Cir. 2003); Schwartz v. DOJ, No. 94 CIV. 7476, 1995 WL 675462, at *7-8 (S.D.N.Y. Nov. 14, 1995) (finding alleged inaccuracy in presentence report “cannot have caused an adverse determination” where sentencing judge was made aware of error and stated that fact at issue was not material for sentencing, nor did any omission of additional facts in report result in plaintiff’s “not receiving a fair determination relating to his rights”), aff’d, 101 F.3d 686 (2d Cir. 1996) (unpublished table decision); Kellett v. United States, 856 F. Supp. 65, 70-71 (D.N.H. 1994) (concluding that factors plaintiff claimed were inaccurate were not proximate cause of agency

determination where those factors “were not substantially relied on in rendering the decision” and that where officials “did not substantially rely on the inaccurate information,” plaintiff did not “establish intentional or willful conduct”), aff’d sub nom. Kellett v. U.S. Bureau of Prisons, 66 F.3d 306 (1st Cir. 1995) (unpublished table decision); but see, e.g., Perry, 371 F.3d at 1305 (finding plaintiffs had alleged necessary elements to state claim, vacating district’s court decision and remanding for district court to consider complaint under Privacy Act); Fleck v. VA OIG, 2020 WL 42842, at *6-8 (denying VA’s motion to dismiss where second agency’s decision not to hire plaintiff was adverse action, plaintiff sufficiently alleged factual inaccuracies in OIG report, and inaccuracies led to second agency’s failure to hire him); Makowski v. United States, 27 F. Supp. 3d 901, 914-15 (N.D. Ill. 2014) (“[Plaintiff] has linked the alleged Privacy Act violation with his alleged damages by stating that ICE issued an unlawful detainer against him because of its reliance on DHS’s inaccurate records, the detainer disqualified [plaintiff] from boot camp, [plaintiff] was not processed into boot camp until his father retained an attorney’s assistance to prompt ICE to cancel the detainer, and the delay in processing into boot camp caused [plaintiff] to remain incarcerated from May to July 2011, preventing him from seeking employment.”).

d. Fourth Element: Intentional or Willful Conduct

Finally, plaintiffs rarely have established that an agency intentionally or willfully failed to maintain accurate records. See, e.g., Deters v. Parole Comm’n, 85 F.3d 655, 660 (D.C. Cir. 1996) (concluding that where Parole Commission informed plaintiff that it would consider his challenge and examine the accuracy of his records at parole hearing, no fact-finder could determine that agency “flagrantly disregarded” plaintiff’s Privacy Act rights and that “a violation (if any) could in no sense be deemed ‘patently egregious and unlawful.’”); Yusim, 406 F. Supp. 3d at 196 (finding that SSA’s allegedly inaccurate listing of claimant’s application date for benefits did not violate his Privacy Act rights, where he did not claim that failure to maintain accurate records was done intentionally or willfully or that he suffered adverse determination); Colley v. James, 254 F. Supp. 3d 45, 67 (D.D.C. 2017) (finding that plaintiffs did not establish that the Air Force violated Privacy Act by engaging in willful or intentional conduct because agency had corrected inaccurate information pertaining to their appeal and there was no indication that incorrect information had been relied upon as part of appeal); Ahuruonye v. Interior, 239 F. Supp. 3d 136, 143 (D.D.C. 2017) (finding that plaintiff “failed to meet his burden of demonstrating that the defendant intentionally or willfully failed to

maintain his 2014 Within Grade Increase Notice in the format requested”); Gillman v. United States, 2017 WL 969180, at *4-5 (finding that plaintiff “failed to establish the existence of a genuine issue of material fact – namely, whether VA personnel acted intentionally or willfully in maintaining allegedly inaccurate medical records,” and failed to provide “evidence to show that the VA’s maintenance of allegedly inaccurate mental health records caused a required adverse determination or actual damages”); Kellett, 856 F. Supp. at 70-71 (concluding that factors plaintiff claimed were inaccurate were not proximate cause of agency determination where those factors “were not substantially relied on in rendering the decision” and that where officials “did not substantially rely on the inaccurate information,” plaintiff did not “establish intentional or willful conduct”); but see Ashbourne v. Hansberry, 302 F. Supp. 3d at 347 (finding that plaintiff properly pled in her complaint that defendant DHS failed to maintain accurate records when it intentionally and deliberately failed to verify facts in deciding to terminate plaintiff’s federal employment). For additional discussion of the “intentional or willful” standard under 5 U.S.C. § 552a(g)(4) for damages actions, see discussion below under “Principles Applicable to Damages Lawsuits, Intentional or Willful Standard.”

3. Standard and Scope of Review

Courts review (g)(1)(C) lawsuits under the standards set out in that section, not de novo.

Unlike amendment lawsuits under subsection (g)(1)(A), courts do not review subsection (g)(1)(C) actions under a de novo standard. Compare 5 U.S.C. § 552a(g)(2) with id. § 552a(g)(4). Instead, the courts determine whether the standards for “accuracy, relevance, timeliness, and completeness” set forth in subsection (g)(1)(C) have been met. See White v. OPM, 787 F.2d 660, 663 (D.C. Cir. 1986) (“In § 552a(g)(1)(C) . . . suits for damages, however, de novo review is not called for. Rather, the reviewing court is to inquire whether the standard articulated in § 552a(g)(1)(C) has been met.”); see also Sellers v. BOP, 959 F.2d 307, 312-13 (D.C. Cir. 1992); Nolan v. DOJ, No. 89-A-2035, 1991 WL 134803, at *3 (D. Colo. July 17, 1991), appeal dismissed in pertinent part on procedural grounds, 973 F.2d 843 (10th Cir. 1992); Reitz, 2010 WL 786586, at *10; see also Doe v. United States, 821 F.2d 694, 712 (D.C. Cir. 1987) (en banc) (Mikva, J., joined by Robinson and Edwards, JJ., dissenting).

Plaintiffs cannot use subsection (g)(1)(C) lawsuits to collaterally attack agency determinations.

Just as in the amendment context (see “5 U.S.C. § 552a(g)(1)(A) - Amendment Lawsuits” discussion above), many courts have expressed disfavor toward litigants who attempt to invoke the subsection (g)(1)(C) damages remedy as a basis for collateral attacks on judicial and quasi-judicial agency determinations, such as those denying benefit and or detrimental employment decisions. See, e.g., Taylor v. Def. Fin. & Accounting Servs., No. 2:12-2466, 2014 U.S. Dist. LEXIS 268, at *25 (E.D. Cal. Jan. 3, 2014) (finding that plaintiff cannot use claim under (g)(1)(C) and (g)(1)(D) to reopen determinations that plaintiff owed an overpay debt); Middlebrooks v. Mabus, No. 1:11cv46, 2011 WL 4478686, at *5 (E.D. Va. Sept. 23, 2011) (“Even if these claims were not untimely, . . . plaintiff’s challenge to the accuracy of her record is a veiled attempt to relitigate her discrimination claim, which is . . . beyond the scope of the [Privacy] Act” because “[t]he Act is a vehicle for correcting facts in agency records if those facts are erroneously recorded but not for altering records that reflect an administrative decision or assessments.”); Feldman, 797 F. Supp. 2d at 47 (dismissing Privacy Act claim because “plaintiff’s inaccuracy claims, at their core, attempt to attack the judgment of a federal official, rather than to correct a factual or historical error in an official record that proximately caused an adverse determination”); Doe v. DOJ, 660 F. Supp. 2d at 42-43 (“[P]laintiff’s arguments that defendants lacked a basis to terminate him because his job did not require a security clearance or because they failed to follow the correct procedures . . . or that DOJ gave too much weight to his psychologist’s . . . letter are impermissible attacks on DOJ’s personnel decisions and administrative actions.” (citations omitted)); Allmon v. BOP, 605 F. Supp. 2d 1, 7 (D.D.C. 2009) (ruling that prisoner may not “us[e] [a] Privacy Act suit as a means to effect his transfer to a less-secure facility”); Ray v. DHS, No. H-07-2967, 2008 WL 3263550, at *10-11 (S.D. Tex. Aug. 7, 2008) (“To the extent that [plaintiff’s] section 552a(g)(1)(C) claim seeks review of the TSA’s decision to suspend him indefinitely without pay based on his failure to disclose his previous offenses,” it must be dismissed because “[t]he Privacy Act . . . does not authorize relitigation of the substance of agency decisions.”); Brown v. Prob. Office, No. 03-872, 2005 WL 2284207, at *3 (E.D. Tex. Aug. 15, 2005) (magistrate’s recommendation) (rejecting plaintiff’s claim as essentially a “challeng[e] to the application of the classification guidelines, not the accuracy or completeness of the information”), adopted, No. 03-872 (E.D. Tex. Sept. 9, 2005); Compro-Tax v. IRS, No. H-98-2471, 1999 U.S. Dist. LEXIS 5972, at *11-12 (S.D. Tex. Apr. 9, 1999) (magistrate’s recommendation) (finding no intentional or willful

agency action, and stating that “Privacy Act may not be used to collaterally attack a final agency decision as ‘inaccurate,’ or ‘incomplete’ merely because the individual contests the decision”), adopted, No. H-98-2471, 1999 WL 501014 (S.D. Tex. May 12, 1999); Douglas v. Farmers Home Admin., No. 91-1969, 1992 U.S. Dist. LEXIS 9159, at *2-3 (D.D.C. June 26, 1992) (applying principles of White v. U.S. Civil Serv. Comm’n, 589 F.2d 713 (D.C. Cir. 1978) (per curiam) (holding that (g)(1)(A) plaintiff was not entitled to bring Privacy Act damages action for allegedly inaccurate appraisal of his property where he had not sought judicial review under APA)); Castella v. Long, 701 F. Supp. 578, 584-85 (N.D. Tex. 1988) (holding “collateral attack on correctness of the finding supporting the discharge decision” is improper under Act), aff’d, 862 F.2d 872 (5th Cir. 1988) (unpublished table decision); Holmberg v. United States, No. 85-2052, slip op. at 2-3 (D.D.C. Dec. 10, 1985) (stating that Privacy Act “cannot be used to attack the outcome of adjudicatory-type proceedings by alleging that the underlying record was erroneous”); cf. Bhatia, 2011 WL 1298763, at *4-5 (dismissing as “unripe” plaintiff’s “attempt[] to collaterally attack the validity of the criminal indictment . . . under the guise of Privacy Act claims” because “[t]he validity or invalidity of the criminal charges contained in the indictment cannot be determined until the criminal action is finally resolved”), aff’d, 507 F. App’x 649 (9th Cir. 2013). The OMB 1975 Guidelines, 40 Fed. Reg. at 28,969, https://www.justice.gov/paoverview_omb-75, also address this issue.

Similarly, subsection (g)(1)(C) lawsuits filed to attack a criminal conviction or sentence are not cognizable.

Federal prisoners frequently attempt to invoke the subsection (g)(1)(C) damages remedy as a basis for a collateral attack on a conviction or the duration of a sentence. The Court of Appeals for the D.C. Circuit has explained that “such a claim is not cognizable” unless the conviction or sentence “has been invalidated in a prior proceeding.” White v. Prob. Office, 148 F.3d 1124, 1125-26 (D.C. Cir. 1998) (per curiam). In White, the D.C. Circuit held that a Privacy Act claim for damages could not be brought to “collaterally to attack” a federal prisoner’s sentence, stating that: “Because a judgment in favor of [plaintiff] on his challenge to the legal conclusions in his presentence report would necessarily imply the invalidity of his sentence, which has not been invalidated in a prior proceeding, his complaint for damages under the Privacy Act must be dismissed.” Id. at 1125-26. See also, e.g., Aguiar v. DEA, 334 F. Supp. 3d 130, 146 (D.D.C. 2018) (finding plaintiff’s claims relating to accuracy of his GPS data not cognizable under Privacy Act because such claims were being used to collaterally attack his conviction and sentence); Lewis v. Parole Comm’n, 770 F. Supp. 2d 246,

249-51 (D.D.C. 2011) (dismissing claim that agency's reliance on allegedly inaccurate information adversely affected plaintiff in parole hearings because "it is 'probabilistic' that the plaintiff's claim, if successful, would result in a decreased sentence or a more favorable parole decision" and such claims must be brought in habeas); Cargill v. Prob. Office for the Middle Dist. of N.C., No. 10-0388, 2010 WL 917010, at *1 (D.D.C. Mar. 9, 2010) (citing White v. Prob. Office and stating that "plaintiff cannot maintain his Privacy Act claim for damages based on the premise that his sentence is unlawful unless he can also show that his sentence was invalidated by an appropriate court"); Skinner v. BOP, 584 F.3d 1093, 1098, 1101 (D.C. Cir. 2009) (explaining that federal inmate's subsection (g)(1)(C) claim "is barred unless and until he successfully challenges the disciplinary hearing on which it is based through an action in habeas corpus"); Corley v. Parole Comm'n, 709 F. Supp. 2d 1, 5 (D.D.C. 2009) ("To the extent that this Privacy Act case is a disguised collateral attack on the plaintiff's conviction and sentence by denying that an indictment ever issued or that a conviction was ever obtained . . . this court must dismiss the case."); Brown v. BOP, 498 F. Supp. 2d. 298, 303-04 (D.D.C. 2007) ("The Privacy Act is not the proper means by which a prisoner may collaterally attack his sentence absent a showing that his sentence has been invalidated in a prior proceeding."); Wattleton v. Lappin, 94 F. App'x 844, 845 (D.C. Cir. 2004) (per curiam) ("[S]uccess on [the] Privacy Act claim would, at a minimum, have a 'probabilistic impact' on the duration of [the prisoner's] custody, [because] appellant is required to proceed by way of a habeas petition."); Doyon v. DOJ, 304 F. Supp. 2d 32, 35 (D.D.C. 2004) ("A challenge to the professional judgment of [BOP] officials in assessing points for purposes of establishing a prisoner's custody classification is not properly mounted by means of a Privacy Act suit."); Razzoli v. BOP, 230 F.3d 371, 373, 376 (D.C. Cir. 2000) (holding that "habeas is indeed exclusive even when a non-habeas claim would have a merely probabilistic impact on the duration of custody" and, therefore, finding "not cognizable" prisoner's claim that agency violated Privacy Act by relying on inaccurate information in postponing his eligibility for parole); Thomas v. Parole Comm'n, No. 94-0174, 1994 WL 487139, at *6 (D.D.C. Sept. 7, 1994) (stating that plaintiff should not be allowed to use Privacy Act "to collaterally attack the contents of his presentence report," as he "originally had the opportunity to challenge the accuracy . . . before the judge who sentenced him").

Other courts outside the D.C. Circuit also have rejected these types of claims on similar grounds. *See, e.g., Whitley v. Hunt*, 158 F.3d 882, 889-90 (5th Cir. 1998) (affirming district court's conclusion that there was "no factual or legal basis" for claim that "prison officials abused their discretion by relying upon

the sentence imposed against Whitley to determine his classification”; “Whitley is essentially claiming that his sentence itself was incorrectly entered. That is an issue that should have been resolved on direct appeal from his criminal conviction”; Hurley v. BOP, No. 95-1696, 1995 U.S. App. LEXIS 30148, at *4 (1st Cir. Oct. 24, 1995) (stating that any alleged inaccuracy in plaintiff’s presentence report, which agency relied on, “should have been brought to the attention of the district court at sentencing; or, at the very least, on appeal from his conviction and sentence”); Wingo v. Farley, No. 4:12-CV-2072, 2013 WL 2151638, at *3 (N.D. Ohio May 16, 2013) (explaining that “Privacy Act is not the proper vehicle to challenge an agency’s opinions or judgments. Rather, the Act ‘is intended to remedy factual or historical errors, and is not a vehicle for addressing the judgments of federal officials . . . reflected in records maintained by federal agencies.’”); Eubanks v. United States, No. 2:09cv126, 2010 WL 1141436, at *2 (N.D. W. Va. Jan. 12, 2010) (magistrate’s recommendation) (asserting that claim “seeking damages for the alleged miscalculation of [plaintiff’s] sentence should be dismissed” because his “sentence calculation has never been invalidated”), adopted, 2010 WL 1141437 (N.D. W. Va. Mar. 22, 2010), aff’d per curiam, 405 F. App’x 796 (4th Cir. 2010); Blanton v. Schultz, No. 105CV0001, 2005 WL 3507969, at *3 (E.D. Cal. Dec. 21, 2005) (finding that prisoner’s argument that BOP is using “false information” to assign prisoner less favorable custody and security classifications “is nothing more than an attempt to resurrect an otherwise improper [petition for writ of habeas corpus]”).

Courts often have found Privacy Act damages claims under subsection (g)(1)(C) precluded by other statutes.

As in the amendment context, 26 U.S.C. § 7852(e) (2018) (a provision of the Internal Revenue Code) also displaces the Privacy Act’s damages remedy for inaccurate records in matters concerning tax liability. *See, e.g., Risk v. United States*, No. 07-60025, 2007 WL 9701106, at * 2 (finding that “plaintiffs’ reliance on the Privacy Act of 1974 is also misplaced since the Internal Revenue Code explicitly states that [(g)(1)(C)] is inapplicable in tax matters” (citing to 26 U.S.C. § 7852(e)); *see also Ford v. United States*, No. 91-36319, 1992 WL 387154, at *2 (9th Cir. Dec. 24, 1992); McMillen v. Treasury, 960 F.2d 187, 188 (1st Cir. 1991); Swartz v. IRS, No. 05-72215, 2006 WL 1374472, at *2 (May 18, 2006); Sherwood v. United States, No. 96-2223, 1996 WL 732512, at *9 (N.D. Cal. Dec. 9, 1996).

In Hubbard v. EPA, the leading D.C. Circuit case concerning the causation requirement of subsection (g)(1)(C), the D.C. Circuit’s finding of a lack of causation was heavily influenced by the Civil Service Reform Act’s (CSRA)

jurisdictional bar to district court review of government personnel practices. See 809 F.2d at 5. Although the D.C. Circuit stopped short of holding that the CSRA's comprehensive remedial scheme constitutes a jurisdictional bar to a subsection (g)(1)(C) action, it noted that "it would be anomalous to construe the pre-existing Privacy Act to grant the district court power to do indirectly that which Congress precluded directly: 'the Privacy Act was not intended to shield [federal] employees from the vicissitudes of federal personnel management decisions.'" Id. (quoting Albright v. United States, 732 F.2d 181, 190 (D.C. Cir. 1984)); cf. Biondo v. Navy, No. 2:92-0184-18, slip op. at 21-23 (D.S.C. June 29, 1993) (finding, based upon Hubbard, "that the 'collateral attack' argument complements the causation requirement of the Privacy Act"). The concurring opinion in Hubbard argued, however, that "[n]othing in the wording or legislative history of either Act" supports the majority's "suggestion that serious consideration of a Privacy Act claim in the context of a federal personnel dispute somehow creates a potential conflict with the" (CSRA). 809 F.2d at 12-13 (Wald, J., concurring) (citing Molerio v. FBI, 749 F.2d 815, 826 (D.C. Cir. 1984), Albright, 732 F.2d at 188, and Borrell v. U.S. Int'l Comm'n Agency, 682 F.2d 981, 992-93 (D.C. Cir. 1982)). That opinion also noted that circuit court precedents since the passage of the CSRA have, "without a hint of the majority's caution, reviewed the Privacy Act claims of federal employees or applicants embroiled in personnel disputes." Id.

Although Hubbard merely applied a strict causation test where a government personnel determination was being challenged, several more cases have gone further and construed the CSRA's comprehensive remedial scheme to constitute a jurisdictional bar to subsection (g)(1)(C) damages lawsuits challenging federal employment determinations. See Yu v. VA, 528 F. App'x 181, 184 (3d Cir. 2013) (affirming district court decision that VA's actions that took place after plaintiff's termination "are personnel decisions because they 'occurred only as result of the employment relationship' [plaintiff] had with the VA," and therefore, preclude Privacy Act damages claims); Doe v. FDIC, 545 F. App'x 6, 8 (2d Cir. 2013) (stating that because "Doe's Privacy Act claims fall within the definition of a 'prohibited personnel action,' the CSRA dictates that Doe may not pursue her claims in federal court"); Orsay v. DOJ, 289 F.3d 1125, 1128-31 (9th Cir. 2002); Phillips v. Widnall, No. 96-2099, 1997 WL 176394, at *3 (10th Cir. Apr. 14, 1997) (citing Henderson v. SSA, infra, to hold that claim concerning alleged inaccuracies and omissions in appellant's employment file that formed basis of her claim for damages to remedy loss of promotion and other benefits of employment "is not a recognizable claim under the Privacy Act," as "CSRA provides the exclusive remedial scheme for review of [appellant's] claims

OVERVIEW OF THE PRIVACY ACT

related to her position”); Vessella v. Air Force, No. 92-2195, 1993 WL 230172, at *2 (1st Cir. June 28, 1993) (citing Hubbard and Henderson v. SSA, for the proposition that the Privacy Act “cannot be used . . . to frustrate the exclusive, comprehensive scheme provided by the CSRA”); Houlihan v. OPM, 909 F.2d 383, 384-85 (9th Cir. 1990) (per curiam); Henderson v. SSA, 908 F.2d 559, 560-61 (10th Cir. 1990), aff’g 716 F. Supp. 15, 16-17 (D. Kan. 1989)); Minshew v. Donley, 911 F. Supp. 2d 1043, 1067-68 (D. Nev. 2012) (explaining that CSRA preempts plaintiff’s Privacy Act claim because plaintiff “effectively seeks to achieve through a Privacy Act claim an interpretation of the settlement agreement [between plaintiff] and the Air Force which resolved the appeal of her removal pending before the MSPB . . . [plaintiff] thus must bring her claim before the MSPB, not this Court”); Doe v. FDIC, No. 11 Civ. 307, 2012 WL 612461, at *5 (S.D.N.Y. Feb. 27, 2012) (“To the extent [plaintiff] has alleged that the disclosures underlying her Privacy Act claims were personnel actions taken in response to her reporting violations of banking laws and regulations, the Court finds that these claims are precluded by the CSRA.”); Lim v. United States, No. 10-2574, 2011 WL 2650889, at *8 (D. Md. July 5, 2011) (“[W]hile labeled as a Privacy Act violation, [plaintiff] is ultimately challenging the basis for his discharge, a personnel decision which cannot be challenged outside the framework of the CSRA.”); Pippinger v. Sec’y of the Treasury, No. 95-CV-017, 1996 U.S. Dist. LEXIS 5485, at *15 (D. Wyo. Apr. 10, 1996) (citing Henderson and stating that to extent plaintiff challenges accuracy of his personnel records, court does not have jurisdiction “to review errors in judgment that occur during the course of an employment/personnel decision where the CSRA precludes such review”), aff’d sub nom. Pippinger v. Rubin, 129 F.3d 519 (10th Cir. 1997); Barhorst v. Marsh, 765 F. Supp. 995, 999 (E.D. Mo. 1991); Barkley v. USPS, 745 F. Supp. 892, 893-94 (W.D.N.Y. 1990); McDowell v. Cheney, 718 F. Supp. 1531, 1543 (M.D. Ga. 1989); Tuesburg v. HUD, 652 F. Supp. 1044, 1049 (E.D. Mo. 1987); Edwards v. Baker, No. 83-2642, slip op. at 4-6 (D.D.C. July 16, 1986) (rejecting plaintiff’s Privacy Act challenge to an “employee performance appraisal system” on the grounds that “plaintiffs may not use that Act as an alternative route for obtaining judicial review of alleged violations of the CSRA”).

Courts in other cases have declined to go that far. *See, e.g., Doe v. FBI*, 718 F. Supp. 90, 100-01 n.14 (D.D.C. 1989) (rejecting contention that CSRA limited subsection (g)(1)(C) action), aff’d in part, rev’d in part & remanded, on other grounds, 936 F.2d 1346 (D.C. Cir. 1991); *see also Halus v. Army*, No. 87-4133, 1990 WL 121507, at *5 n.8 (E.D. Pa. Aug. 15, 1990) (finding that the “court may determine whether a Privacy Act violation caused the plaintiff damage (here, the loss of his job)”); Hay v. Sec’y of the Army, 739 F.

Supp. 609, 612-13 (S.D. Ga. 1990) (quoting Rogers v. Labor, 607 F. Supp. 697, 699 (N.D. Cal 1985), and Hewitt v. Grabicki, 794 F.2d at 1379) (acknowledging that “Privacy Act ‘may not be employed as a skeleton key for reopening consideration of unfavorable federal agency decisions,’” but allowing Privacy Act claim to proceed because, where “agency acted in an ‘intentional or willful’ manner in failing to maintain accurate records, district court may award actual damages sustained by the individual as a result of an adverse determination based upon such records”).

To date, the D.C. Circuit has declined to rule that the CSRA bars a Privacy Act claim for damages. See Kleiman v. Energy, 956 F.2d 335, 337-39 & n.5 (D.C. Cir. 1992) (holding that Privacy Act did not afford relief where plaintiff did not contest that record accurately reflected his assigned job title, but rather challenged his position classification – personnel decision judicially unreviewable under the CSRA – but noting that nothing in opinion “should be taken to cast doubt on Hubbard’s statement that ‘the Privacy Act permits a federal job applicant to recover damages for an adverse personnel action actually caused by an inaccurate or incomplete record” (quoting Hubbard, 809 F.2d at 5)); Holly v. HHS, No. 88-5372, 1990 WL 13096, at *1 (D.C. Cir. Feb. 7, 1990) (declining to decide whether CSRA in all events precludes Privacy Act claim challenging federal employment determination; instead applying doctrine of “issue preclusion” to bar individual “from relitigating an agency’s maintenance of the challenged records” because arbitrator had previously found that no “[agency] manager acted arbitrarily, capriciously or unreasonably in determining [that plaintiff] was not qualified”); Ahuruonye v. Interior, 312 F. Supp. 3d 1, 14-15 (D.D.C. 2018) (acknowledging that Privacy Act should not be used to circumvent CSRA, but finding that Privacy Act permits federal job applicant or employee to recover damages for adverse personnel action actually caused by inaccurate or incomplete record); Gard v. Dep’t of Educ., 789 F. Supp. 2d 96, 106 (D.D.C. 2011) (citing and quoting Hubbard, but finding that plaintiff’s “claims must fail to the extent that he has not produced any evidence supporting a reasonable inference that a Privacy Act violation itself actually caused the adverse events of which he complains”); Peter B. v. CIA, 620 F. Supp. 2d 58, 76 (D.D.C. 2009) (explaining that if plaintiff “seeks to correct factually inaccurate records,” then his claim “would not be precluded by the CSRA,” but concluding that “[i]t is premature to determine whether [plaintiff] seeks to [do this], or if [plaintiff] disagrees with the [agency’s] judgments contained in his records”); Lee v. Geren, 480 F. Supp. 2d at 210-12 (following Hubbard and Kleiman and concluding that allegedly inaccurate documents produced during investigation of plaintiff did not

actually cause his suspension but rather “merely memorialized” that determination and thus “had no independent effect of their own”); Doe v. Goss, No. 04-2122, 2007 WL 106523, at *8-9 (D.D.C. Jan. 12, 2007) (citing Hubbard and finding that CSRA did not preclude plaintiff’s accuracy claim or his “information-gathering” claim because plaintiff alleged actual causation with respect to both claims). But see Holly v. HHS, No. 89-0137, slip op. at 1 (D.D.C. Aug. 9, 1991) (citing Kleiman for proposition that court lacks subject matter jurisdiction in Privacy Act damages action in which plaintiff challenges personnel action governed by CSRA), aff’d, 968 F.2d 92 (D.C. Cir. 1992) (unpublished table decision).

The Court of Appeals for the Ninth Circuit considered the interplay between the Privacy Act and a statute that broadly precludes judicial review of VA disability benefit decisions – 38 U.S.C. § 211(a) (later repealed, now see 38 U.S.C. § 511 (2018)) – and concluded that it barred a subsection (g)(1)(C) damages action. Rosen v. Walters, 719 F.2d 1422, 1424-25 (9th Cir. 1983). In Rosen, the plaintiff contended that the VA deliberately destroyed medical records pertinent to his disability claim, thereby preventing him from presenting all the evidence in his favor. Id. at 1424. The Ninth Circuit ruled that such a damages claim would “necessarily run counter to the purposes of § 211(a)” because it would require a determination as to whether “but for the missing records, Rosen should have been awarded disability benefits.” Id. at 1425. Further, it declined to find that the Privacy Act “repealed by implication” 38 U.S.C. § 211(a). Id.; see also Demoruelle v. VA, No. 16-00562, 2017 WL 2836989, at *5 (D. Hawaii June 30, 2017) (dismissing plaintiff’s accuracy claims since court is precluded from having jurisdiction over claims that seek review of VA’s benefit decisions pursuant to 38 U.S.C. § 511(a) and consistent with Veterans for Common Sense v. Shinseki, 678 F.3d 1013 (9th Cir. 2012)); Thomas v. Principi, 265 F. Supp. 2d 35, 39-40 (D.D.C. 2003) (holding claim for failure to maintain accurate and complete records was barred by former 38 U.S.C. § 511 “because the injuries that allegedly resulted from defendants’ failure to maintain [plaintiff’s] records all ultimately concern the adverse benefits determination made by the [VA]”), aff’d in pertinent part, rev’d in part, 394 F.3d 970 (D.C. Cir. 2005); R.R. v. Army, 482 F. Supp. 770, 775-76 (D.D.C. 1980) (rejecting damages claim for lack of causation and noting that “[w]hat plaintiff apparently seeks to accomplish is to circumvent the statutory provisions making the VA’s determinations of benefits final and not subject to judicial review”); cf. Kaswan v. VA, No. 81-3805, 1988 WL 98334, at *12 (E.D.N.Y. Sept. 15, 1988) (stating that Privacy Act is “not available to collaterally attack factual and legal decisions to grant or deny veterans benefits”), aff’d, 875 F.2d 856 (2d Cir. 1989) (unpublished table decision); Leib v. VA, 546 F. Supp. 758, 761-62

(D.D.C. 1982) (“The Privacy Act was not intended to be and should not be allowed to become a ‘backdoor mechanism’ to subvert the finality of agency determinations.” (quoting Lyon v. United States, 94 F.R.D. 69, 72 (W.D. Okla. 1982))). Relying on Rosen, the District Court for the District of Idaho similarly held that the statutory scheme regarding the awarding of retirement benefits and “Congress’s intent that OPM, MSPB and the Federal Circuit review decisions regarding the denial of disability retirement benefits” prohibited it from reviewing Privacy Act damages claim where plaintiff alleged that VA’s failure to maintain file resulted in his being denied disability retirement benefits by OPM. Braun v. Brown, No. CV 97-0063-S, slip op. at 7-11 (D. Idaho June 22, 1998).

Several courts have held that the provision of the Federal Employees’ Compensation Act (FECA), 5 U.S.C. § 8116(c) (2018), that provides that the liability of the United States under FECA with respect to the injury of an employee is exclusive, operates to preclude a cause of action under the Privacy Act, and deprives the court of subject matter jurisdiction. *See, e.g., Vogrin v. ATF*, No. 598CV117, 2001 WL 777427, at *7-8 (N.D. W. Va. Mar. 30, 2001), *aff’d per curiam*, No. 01-1491 (4th Cir. July 3, 2001). The court ruled that FECA’s exclusivity provision “precludes a suit under the Privacy Act even if FECA does not provide benefits for all of the injuries that [the plaintiff] claims.” *Id.* at *7; *see also Scott v. USPS*, No. 05-0002, 2006 WL 2787832, at *3-4 (D.D.C. Sept. 26, 2006) (explaining that “even though [plaintiff] was ultimately denied compensation under FECA based on a lack of competent medical evidence” and establishing that agency’s disclosure of records caused her alleged emotional injury, “that is immaterial to the issue of the Court’s jurisdiction”); Lyon v. United States, 94 F.R.D. 69, 72 (W.D. Okla. 1982) (finding Privacy Act claim cannot be “a backdoor mechanism to subvert authority bestowed upon the Secretary of Labor to handle employee compensation claims”; stating FECA “provides the exclusive method of presenting compensation claims resulting from on-the-job injuries of federal employees”); *cf. Jackson v. Labor*, No. 2:06-CV-02157, 2008 WL 539925, at *4 (E.D. Cal. Feb. 25, 2008) (ruling that plaintiff may not bring amendment lawsuit under Privacy Act to re-litigate determination of FECA benefits); Weber v. Henderson, 33 F. App’x 610, 612 (3d Cir. 2002) (holding that Privacy Act claim was barred by res judicata where plaintiff could have raised Privacy Act claim in prior suit when he brought claim against same defendants as cause of action under FECA).

The D.C. District Court has found that a Privacy Act claim is not precluded by the exclusivity of relief under Title VII of the Civil Rights Act.

The District Court for the District of Columbia concluded, however that a Privacy Act claim was not precluded by the exclusivity of relief under Title VII of the Civil Rights Act of 1964, 42 U.S.C. § 2000e (2018). See Velikonja v. Mueller, 315 F. Supp. 2d 66, 77 (D.D.C. 2004) (noting that agency “failed to cite any cases in which a Privacy Act claim is precluded by Title VII” and that “the court is not aware of any”), subsequent opinion, 362 F. Supp. 2d 1, 13-19 (D.D.C. 2004) (finding no inaccuracies, adverse determination, or intentional or willful conduct), aff’d in part & rev’d in part sub nom. Velikonja v. Gonzales, 466 F.3d 122 (D.C. Cir. 2006) (affirming on ground of finding of no inaccuracies, adverse determination, or intentional or willful conduct).

The courts have split as to whether the (g)(1)(C) standards apply only to the receiving agency or to any agency.

In Perry v. FBI, 759 F.2d 1271, 1275-76 (7th Cir. 1985), reh’g en banc granted on other grounds, 769 F.2d 450 (7th Cir. 1985), the Court of Appeals for the Seventh Circuit, without discussing subsection (g)(1)(C), adopted a comparatively narrower construction of subsection (e)(5), holding that “when one federal agency sends records to another agency to be used by the latter in making a decision about someone, the responsibility for ensuring that the information is accurate, relevant, timely, and complete lies with the receiving agency – the agency making ‘the determination’ about the person in question – not the sending agency.”

Subsequently, however, in Dickson v. OPM, 828 F.2d 32, 36-40 (D.C. Cir. 1987), the D.C. Circuit held that a subsection (g)(1)(C) damages lawsuit is proper against any agency maintaining a record violating the standard of fairness mandated by the Act, regardless of whether that agency is the one making the adverse determination. See also Blazy v. Tenet, 979 F. Supp. 10, 19 (D.D.C. 1997) (“The adverse determination need not be made by the agency that actually maintains the record so long as it flowed from the inaccurate record.” (citing Dickson)), summary affirmance granted, No. 97-5330, 1998 WL 315583 (D.C. Cir. May 12, 1998); Doe v. U.S. Civil Serv. Comm’n, 483 F. Supp. 539, 556 (S.D.N.Y. 1980) (applying subsection (e)(5) to agency whose records were used by another agency in making determination about individual); R.R. v. Army, 482 F. Supp. at 773 (applying subsection (e)(5) to agency whose records were used by another agency in making determination about individual). In so holding, the D.C. Circuit

noted that “the structure of the Act makes it abundantly clear that [sub]section (g) civil remedy actions operate independently of the obligations imposed on agency recordkeeping pursuant to [sub]section (e)(5).” Dickson, 828 F.2d at 38. In Dickson, the D.C. Circuit distinguished Perry on the grounds that “[a]ppellant is not proceeding under [sub]section (e)(5), Perry does not discuss [sub]section (g)(1)(C), and the construction of (e)(5) does not migrate by logic or statutory mandate to a separate [sub]section on civil remedies.” 828 F.2d at 38; see also Doe v. FBI, 718 F. Supp. at 95 n.15 (noting conflict in cases but finding that Dickson’s holding obviated need “to enter that thicket”).

D. 5 U.S.C. § 552a(g)(1)(D) - Damages Lawsuits for Failure to Comply with Other Privacy Act Provisions

“Whenever any agency . . . fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual . . . the individual may bring a civil action.” 5 U.S.C. § 552a(g)(1)(D).

Comment:

In addition to damages under subsection (g)(1)(C)’s “accuracy, relevance, timeliness, and completeness” standard, subsection (g)(1)(D) provides a “catch-all” remedies provisions that allows lawsuits for actual damages against an agency for failure to comply with “any other provision” of the Privacy Act, if there is an “adverse effect” on the individual.

1. Exhaustion of Administrative Remedy

Individuals are not required to exhaust administrative remedies before filing suit under subsection (g)(1)(D).

Exhaustion of administrative remedies is not a prerequisite to a civil action for damages under subsection (g)(1)(D). Diederich v. Army, 878 F.2d 646, 648 (2d Cir. 1989); Nagel v. HEW, 725 F.2d 1438, 1441 & n.2 (D.C. Cir. 1984); McKoy v. Spencer, No. 16-1313, 2019 WL 400615, at *4 -5 (D.D.C. Jan. 31, 2019) (finding that while claim to amend record does require exhaustion of administrative remedies, damages claim stemming from improper disclosure of personnel records to third parties does not); Gergick v. Austin, No. 89-0838-CV-W-2, 1992 U.S. Dist. LEXIS 7338, at *13-16 (W.D. Mo. Apr. 29, 1992), aff’d, No. 92-3210 (8th Cir. July 9, 1993); Pope v. Bond, 641 F. Supp. 489, 500 (D.D.C. 1986). But see Graham v. Hawk, 857 F. Supp. 38, 40 (W.D.

Tenn. 1994) (stating that “[e]ach paragraph of 5 U.S.C. § 552a(g) . . . requires as a prerequisite to any action that the agency refuse an individual’s request to take some corrective action regarding his file”), aff’d, 59 F.3d 170 (6th Cir. 1995) (unpublished table decision).

The Prison Litigation Reform Act imposes additional procedural requirements on prisoners, however.

While “exhaustion is normally not required for damages actions under the Privacy Act,” note that 42 U.S.C. § 1997e(a) (2018), a provision of the Prison Litigation Reform Act of 1996 (“PLRA”), “imposes additional procedural requirements with respect to prisoners.” Reid v. BOP, No. 04-1845, 2005 WL 1699425, at *3 (D.D.C. July 20, 2005). Specifically, § 1997e(a) provides that “[n]o action shall be brought with respect to prison conditions under [any Federal law] by a prisoner confined in any jail, prison, or other correctional facility until such administrative remedies as are available are exhausted.” 42 U.S.C. § 1997e(a). The Supreme Court “has read the exhaustion requirements [of § 1997e(a)] broadly to include ‘all inmate suits about prison life, whether they involve general circumstances or particular episodes, and whether they allege excessive force or some other wrong.’” Reid, 2005 WL 1699425, at *3 (quoting Porter v. Nussle, 534 U.S. 516, 532 (2002)). In McGee v. BOP, for example, the prisoner sued the BOP alleging unlawful disclosure. 118 F. App’x 471, 474 (10th Cir. 2004). The Court of Appeals for the Tenth Circuit concluded that the prisoner “failed to exhaust his administrative remedies with respect to his Privacy Act claim” pursuant to § 1997e(a). Id. at 475; see also Smith v. B A Blackmon Warden FCI Marianna, No. 5:18CV40, 2019 WL 3047081, at *6-7 (N.D. Fla. May 21, 2019) (magistrate recommendation) (finding prisoner’s claim under Privacy Act “must be a separate (non-habeas) filing subject to the PLRA, filing fee and other provisions”) adopted, 2019 WL 3037921 (N.D. Fla. 2019); Lugo-Vazquez v. Grondolsky, No. 08-986, 2010 WL 2287556, at *2-3 (D.N.J. June 2, 2010) (granting summary judgment to agency on Privacy Act claim because plaintiff failed to exhaust administrative remedies under § 1997e(a)); cf. Lee v. DOJ, 235 F.R.D. 274, 289-91 (W.D. Pa. 2006) (concluding that PLRA did not apply to allegation that “pertain[ed] to the disclosure of the [record] to a private bank, not to the means by which it was obtained,” because allegation “did not relate to prison life”).

2. Elements of a Subsection (g)(1)(D) Claim

In a suit for damages under subsection (g)(1)(D), an individual has the burden of proving that: (1) the information at issue is covered by the Privacy

Act's provisions; (2) the agency violated a provision of the Privacy Act not covered by the other civil remedies provisions; (3) the violation had an "adverse effect" on the plaintiff that was a "causal nexus" between the violation and the adverse effect; and (4) the violation was "willful or intentional." See, e.g., Quinn v. Stone, 978 F.2d 126, 131 (3d Cir. 1992); Pierce v. Air Force, 512 F.3d 184, 186 (5th Cir. 2007). The third element of this cause of action, which is composed of two parts – "adverse effects" and "causation" – is discussed in detail, below. As referenced below, analysis of the remaining elements can be found in other sections of this Overview.

a. First Element: Information Covered by Privacy Act

Information is generally covered by the Privacy Act if it is a "record" maintained in a "system of records." See Quinn, 978 F.2d at 132 (concluding that information disclosed -- hunting roster and time card -- was information covered by Privacy Act because it "contained an identifying particular (the plaintiff's name) and was maintained within a system of records"). Certain records, however, may be subject to the Privacy Act's provisions, even if not maintained in a system of records. See, e.g., McCready v. Nicholson, 465 F.3d 1 (D.C. Cir. 2006). These issues are discussed in more detail above under the "Definitions" section.

b. Second Element: Catch-All Remedy Provision

Subsection (g)(1)(D) acts as a "catch-all remedy provision applicable if the agency 'fails to comply with any other provision' of the Privacy Act." E.g., Fazaga v. FBI, 965 F.3d 1015, 1063 (9th Cir. 2020) (claim based on an alleged violation of subsection (e)(7)); Sussman v. Marshals Serv., 494 F.3d 1106 (D.C. Cir. 2007) (claimed based on an alleged violation of subsection (b)). Plaintiffs must demonstrate that an agency's action violated a Privacy Act provision not otherwise captured in subsections (g)(1)(A), (g)(1)(B), or (g)(1)(C) in order to successfully raise a claim under subsection (g)(1)(D).

c. Third Element: Adverse Effect had Causal Nexus to Violation

i. Adverse Effects

A complaint is subject to dismissal for failure to state a subsection (g)(1)(D) damages claim if no "adverse effect" is alleged. See, e.g., Doe v. Chao, 540 U.S. 614, 624 (2004) ("'[A]dverse effect' acts as a term of art identifying a potential plaintiff who satisfies the injury-in-fact and causation requirements of Article III standing, and who may

consequently bring a civil action without suffering dismissal for want of standing to sue.”); Hunt v. VA, 739 F.3d 706, 707 (D.C. Cir. 2014) (“The district court lacked subject matter jurisdiction over appellant’s Privacy Act claims for damages because the claims are based on the assertion ‘that the VA’s failure to maintain accurate and complete records adversely affected a veteran’s benefits determinations.’”); Hernandez v. Johnson, 514 F. App’x 492, 500 (5th Cir. 2013) (holding that “although [appellant] complained of damages dating back to 2008, he also indicated in his deposition that he was not aware of any of the disclosures until either 2010 or 2011,” and thus, “no reasonable jury could find that the adverse effects [appellant] suffered were caused by these disclosures”); Shearson v. DHS, 638 F.3d 498, 505-06 (6th Cir. 2011) (“[Plaintiff’s] request to pursue a claim under § 552a(e)(4) was properly denied because she failed to allege or show the requisite ‘adverse effect’ from Defendants’ alleged failure to provide notice specifically regarding the [system of records] at an earlier date.”); McCready v. Nicholson, 465 F.3d 1 (D.C. Cir. 2006) (remanding case for district court to determine whether plaintiff suffered “adverse effect” by being denied bonus); Quinn, 978 F.2d at 135 (“[T]he adverse effect requirement of (g)(1)(D) is, in effect, a standing requirement.”); Taylor v. FAA, 351 F. Supp. 3d 97, 103-4 (D.D.C. 2018) (finding no adverse effect from mere improper maintenance of Plaintiff’s name, address, and email address by the FAA); Wright v. United States, No. 4:17-CV-02101, 2018 WL 4854037, at *8 (N.D. Ala. Oct. 5, 2018) (dismissing Privacy Act claim as not satisfying standing requirements where no particularized injury regarding plaintiff’s own data being lost was alleged); Young v. Tryon, No. 12-CV-6251CJS, 2015 WL 309431, at *17 (W.D.N.Y. Jan. 23, 2015) (magistrate recommendation) (noting lack of actual damages where complaint only alleged disclosure of medical information caused plaintiff to be “very uncomfortable discussing his medical issues”) adopted, 2015 WL 554807 (Feb. 11, 2015); Dick v. Holder, 67 F. Supp. 3d 167, 182-3 (D.D.C. 2014) (finding agent failed to provide allegations plausibly suggesting causal link between disclosure warning and claimed adverse effects); Fletcher v. DOJ, 17 F. Supp. 3d 89, 95-96 (D.D.C. 2014) (stating in dicta that “[b]ecause the requested court documents might be available from the [court] where they originated [] plaintiff cannot show an adverse effect from the agency’s destruction of the copies of the same records”); Reed v. Navy, 910 F. Supp. 2d 32, 45 (D.D.C. 2012) (finding that disclosures did not cause plaintiff to be constructively discharged because “the causal link between the disclosures and plaintiff’s separation from [his employer] is broken by intervening events”); Mata v. McHugh, No. 10-cv-838, 2012

WL 2376285, at *6 (W.D. Tex. June 22, 2012) (granting summary judgment on Privacy Act claim where plaintiff failed to plead specific actual damages from disclosure of resume); Raley v. Astrue, No. 2:11cv555, 2012 WL 2368609, at *7 (M.D. Ala. June 21, 2012) (“Plaintiff presents no evidence to establish that receiving someone else’s information did in fact adversely affect her.”); Hurt v. D.C. Court Servs. & Offender Supervision Agency, 827 F. Supp. 2d 16, 21 (D.D.C. 2011) (concluding that plaintiff did not show that alleged improper disclosure . . . resulted in his homelessness because “decision for him to leave [his] residence . . . was made before the alleged disclosure); Philippeaux v. United States, No. 10 Civ. 6143, 2011 WL 4472064, at *9 (S.D.N.Y. Sept. 27, 2011) (holding that plaintiff failed to allege that “any pertinent records have been removed” and, “[a]s a result, . . . he fails to adequately show that he was adversely affected by any disclosure”); Bhatia v. Office of the U.S. Attorney, N. Dist. of Cal., No. C 09-5581, 2011 WL 1298763, at *4 (N.D. Cal. Mar. 29, 2011) (finding that plaintiff who was “wrongly indicted” lacked standing because he “cannot show, at this juncture, that he was injured by the return of the criminal indictment” because “those charges are currently pending”); Mauldin v. Napolitano, No. 10-12826, 2011 WL 3113104, at *3 (E.D. Mich. July 26, 2011); Conley v. United States, No. 2:10-cv-444, 2011 WL 1256611, at *7 (S.D. Ohio Mar. 31, 2011); Shope v. Navy, No. 1:CV-09-2400, 2010 WL 2766638, at *3 (M.D. Pa. July 13, 2010); Sieverding v. DOJ, 693 F. Supp. 2d 93, 106 (D.D.C. 2010), aff’d per curiam, No. 10-5149, 2010 WL 4340348 (D.C. Cir. Oct. 19, 2010); Ciralsky v. CIA, 689 F. Supp. 2d 141, 155-56 (D.D.C. 2010); Sutera v. TSA, 708 F. Supp. 2d 304, 318-19 (E.D.N.Y. 2010); Goodwin v. Johnson, No. 8:10CV40, 2010 WL 1500872, at *3 (D. Neb. Apr. 14, 2010); Doe v. DOJ, 660 F. Supp. 2d 31, 49 (D.D.C. 2009); Baker v. United States, No. 5:05-221, 2006 WL 1635634, at *4 (E.D. Ky. June 8, 2006) (finding that plaintiff failed to allege any adverse effect resulting from disclosure to press of reasons for his medical discharge); Robinett v. State Farm Mut. Auto. Ins. Co., No. 02-0842, 2002 WL 31498992, at *4 (E.D. La. Nov. 7, 2002) (stating that “[e]ven if [agency’s] communication did not technically satisfy the notice requirement of [subsection (e)(8)], plaintiff was not adversely affected by a failure to receive notice after the records were disclosed,” because “plaintiff had no legal basis to prevent [agency] from releasing his records” and in fact knew of possible release and tried to prevent it), aff’d per curiam, 83 F. App’x 638 (5th Cir. 2003); Fort Hall Landowners Alliance, Inc. v. BIA, No. CV-99-00052-E, slip op. at 12 (D. Idaho Mar. 29, 2001); Hass v. Air Force, 848 F. Supp. 926, 932 (D. Kan. 1994); Swenson v. USPS, No. S-87-1282, 1994 U.S. Dist. LEXIS 16524, at *30

(E.D. Cal. Mar. 10, 1994); Green v. USPS, No. 88-0539, 1989 U.S. Dist. LEXIS 6846, at *6-8 (S.D.N.Y. June 19, 1989); Tracy v. SSA, No. 88-C-570-S, slip op. at 4-5 (W.D. Wis. Sept. 23, 1988); Crichton v. Cmty. Servs. Admin., 567 F. Supp. 322, 324 (S.D.N.Y. 1983) (finding mere maintenance of allegedly “secret file” insufficient to warrant damages where no showing of adverse effect); Church v. United States, 2 Gov’t Disclosure Serv. (P-H) ¶ 81,350, at 81,911 (D. Md. Jan. 5, 1981) (finding no adverse effect from failure to provide subsection (e)(3) notice); Harper v. United States, 423 F. Supp. 192, 196-97 (D.S.C. 1976); cf. Ashbourne v. Hansberry, 302 F. Supp. 3d 338, 347-48 (D.D.C. 2018) (finding plaintiff adequately pled adverse effect from purported falsification of her personnel records and then the use of those records to publicly terminate her); Babatu v. Dallas VA Med. Ctr., No. 3:11-CV-00533, 2014 WL 626515, at *9 (N.D. Tex. Feb. 18, 2014) (finding that plaintiff presented genuine disputes of material fact as to whether plaintiff was adversely affected due to “pecuniary loss in the form of lost work-study wages as a result of the disclosure of his information”); Banks v. Butler, No. 5:08CV336, 2010 WL 4537902, at *6 (S.D. Miss. Sept. 23, 2010) (magistrate’s recommendation) (asserting statements about plaintiff by staff members were “at most – innocuous statements of opinion, rather than disclosures of records and create no real adverse effect”), adopted, 2010 WL 4537909 (S.D. Miss. Nov. 2, 2010); Nunez v. Lindsay, No. 3:CV005-1763, 2007 WL 517754, at *1-2 (M.D. Pa. Feb. 12, 2007) (concluding that inmate lacked standing to bring Privacy Act claim against BOP based on prison’s “practice of photographing friends and family who chose to visit” him because “[a]ny invasion of privacy interests concerns the visitors, not the inmates”); Clark v. BOP, 407 F. Supp. 2d 127, 129-131 (D.D.C. 2005) (concluding that disclosure of inmate’s medical records to second inmate so that he could decipher word on first inmate’s chart presented triable issue of whether first inmate’s HIV status was disclosed, but dismissing claim because “plaintiff has not shown that the disclosure caused him to suffer an adverse effect or to sustain actual damages”).

“Adverse effects” include nonpecuniary and nonphysical harm as well as monetary loss.

An “adverse effect” includes not only monetary damages, but also nonpecuniary and nonphysical harm, such as mental distress, embarrassment, or emotional trauma. See, e.g., Speaker v. HHS Ctrs. for Disease Control & Prevention, 623 F.3d 1371, 1382-83 (11th Cir. 2010); Doe v. Chao, 306 F.3d 170, 187 (4th Cir. 2002) (Michael, J.,

dissenting) (“The majority and I . . . also agree that emotional distress can qualify as an adverse effect.”), aff’d, 540 U.S. 614 (2004); Quinn, 978 F.2d at 135-36; Englerius v. VA, 837 F.2d 895, 897 (9th Cir. 1988); Albright v. United States, 732 F.2d 181, 186 (D.C. Cir. 1984); Usher v. Sec’y of HHS, 721 F.2d 854, 856 (1st Cir. 1983); Parks v. IRS, 618 F.2d 677, 682-83 & n.2 (10th Cir. 1980); Kvech v. Holder, No. 10-cv-545, 2011 WL 4369452, at *4 (D.D.C. Sept. 19, 2011); Rice v. United States, 245 F.R.D. 3, 5-6 (D.D.C. 2007); Lechlitter v. Army, No. 04-814, 2006 WL 462750, at *5 (D. Del. Feb. 27, 2006); Schmidt v. VA, 218 F.R.D. 619, 632 (E.D. Wis. 2003); Romero-Vargas v. Shalala, 907 F. Supp. 1128, 1134 (N.D. Ohio 1995); cf. Tarullo v. Def. Contract Audit Agency, 600 F. Supp. 2d 352, 359 (D. Conn. 2009) (dismissing case where “the disclosures of [plaintiff’s] [social security number] had [no] adverse effect on [him] other than the displeasure he felt because these disclosures were against his wishes”); Clark v. BOP, 407 F. Supp. 2d 127, 131 (D.D.C. 2005) (“Nothing in the record . . . connects the alleged adverse effect, i.e., plaintiff’s maltreatment, with the disclosure at issue.”); Doyon v. DOJ, 304 F. Supp. 2d 32, 35 (D.D.C. 2004) (“[A]ssum[ing] without deciding that [BOP’s] decision ‘to restrict [plaintiff] from a transfer and many Institutional programs’ . . . is an adverse determination,” but finding the claim to have been rendered moot.). But see Ferguson v. Alderson Federal Prison Camp, No. 1:18-00180, 2018 WL 7820739, at *6 (S.D. W.Va., Oct. 18, 2018) (finding conclusory statement of adverse effect from alleged loss of outside medical records by prison resulting in “wounded feelings” and “mental anguish” failed to allege any actual damage or adverse consequence); Risch v. Henderson, 128 F. Supp. 2d 437, 441 (E.D. Mich. 1999) (stating that even assuming that there had been a violation of the Privacy Act for the maintenance of alleged “secret files,” because plaintiff claimed only “extreme mental anguish and mental concern and worry,” she had “failed to demonstrate [an] ‘adverse effect’”), aff’d sub nom. Risch v. USPS, 244 F.3d 510 (6th Cir. 2001).

For a novel interpretation of “adverse effect,” see Bagwell v. Brannon, No. 82-8711, slip op. at 5-6 (11th Cir. Feb. 22, 1984), in which the Court of Appeals for the Eleventh Circuit found that no “adverse effect” was caused by the government’s disclosure of an employee’s personnel file during cross-examination while defending against the employee’s tort lawsuit, because the “employee created the risk that pertinent but embarrassing aspects of his work record would be publicized” and “disclosure was consistent with the purpose for which the information was originally collected.”

“Adverse effect” is a separate element from “actual damages.”

The threshold showing of “adverse effect,” which typically is not difficult for a plaintiff to satisfy, should carefully be distinguished from the conceptually separate requirement of “actual damages,” discussed below. *See, e.g., Fort Hall Landowners Alliance, Inc. v. BIA*, 407 F. Supp. 2d 1220, 1225 (D. Idaho 2006) (explaining that “[i]t is important not to confuse this standing requirement with the entirely separate element that requires proof of actual damages” and that “to satisfy the Privacy Act’s adverse effect and causation requirements, plaintiffs need not show actual damages from the disclosure, but must merely satisfy the traditional ‘injury-in-fact and causation requirements of Article III’”). As one district court has explained, “[t]he requirement of an ‘adverse effect’ requires more” than a “statement of ‘damages’ [that] merely summarizes the alleged violations of law.” *Foncello v. Army*, No. 04-604, 2005 WL 2994011, at *4 (D. Conn. Nov. 7, 2005).

The distinct nature of these two elements is demonstrated by the Supreme Court’s review in *FAA v. Cooper*, 132 S. Ct. 1441 (2012), of an opinion by the Court of Appeals for the Ninth Circuit, *Cooper v. FAA*, 622 F.3d 1016 (9th Cir. 2010). In *Cooper* the Ninth Circuit, in construing the Privacy Act to allow for the recovery of nonpecuniary damages, reasoned that because “mental distress or emotional harm is sufficient to constitute an adverse effect,” a construction of the Act that allowed a plaintiff to establish standing for an injury that results in nonpecuniary harm, but that would not allow the plaintiff to seek actual damages for such a nonpecuniary injury would “frustrate the intent of Congress.” *Id.* at 1021. The Ninth Circuit majority further stated that “[i]n contrast, our opinion is true to the overall objective of the Act, allowing a plaintiff who demonstrates a nonpecuniary adverse effect to have the opportunity to recover nonpecuniary damages.” *Id.* However, on writ of certiorari a majority of the Supreme Court reversed the Ninth Circuit’s opinion and held that the Privacy Act does not authorize damages for nonpecuniary injuries such as mental or emotional distress. The Supreme Court did not consider the separate issue of “adverse effect” in its ruling. *See FAA v. Cooper*, 132 S. Ct. at 1453; *see also, Fazaga v. FBI*, 916 F.3d 1202, 1249 (9th Cir. 2019) (finding only damages and not injunctive relief available for Privacy Act violations of the catch-all provision at § 552a(g)(1)(D)); *Coleman v. U.S.*, 912 F.3d 824, 836 (5th Cir. 2019) (affirming summary judgment on Privacy Act claim against plaintiff who did not offer any evidence of actual harm other than her own unsubstantiated allegations of

emotional trauma); Richardson v. Bd. of Governors of Fed. Reserve Sys., 288 F. Supp. 3d 231, 236-37 (D.D.C. 2018) (finding claim that plaintiff suffered “adverse and harmful effects” insufficient where effects included “mental distress, emotional trauma, embarrassment, humiliation” that are not authorized under Privacy Act and where alleged “lost or jeopardized present and future financial opportunities” were not supported by sufficient facts to sustain claim of actual damages).

ii. Causation

A showing of causation – that the violation caused an adverse effect, and that the violation caused “actual damages,” as discussed below – is also required. See, e.g., Beaven v. DOJ, 622 F. 3d 540, 558 (6th Cir. 2010); Sweeney v. Chertoff, 178 F. App’x 354, 357-58 (5th Cir. 2006); Mandel v. OPM, 79 F. App’x 479, 481-82 (2d Cir. 2003), aff’g 244 F. Supp. 2d 146, 153 (E.D.N.Y. 2003); Orekoya v. Mooney, 330 F.3d 1, 10 (1st Cir. 2003); Quinn, 978 F.2d at 135; Hewitt v. Grabicki, 794 F.2d 1373, 1379 (9th Cir. 1986); Albright, 732 F.2d at 186-87; Edison v. Army, 672 F.2d 840, 842, 845 (11th Cir. 1982); Lugo v. DOJ, 214 F. Supp. 3d. 32, 41 (D.D.C. 2016); Iqbal v. DOJ, No. 3:11-cv-369, 2013 U.S. Dist. LEXIS 138793, at *15 (M.D. Fla. Sept. 26, 2013); Colgan v. Mabus, No. 11cv2278, 2013 U.S. Dist. LEXIS 129215, at *7-8 (S.D. Cal. Sept. 10, 2013); Su v. NASA, No. 5:09-cv-02838, 2013 WL 1663608, at *6-7 (N.D. Cal. Apr. 17, 2013); Reed, 910 F. Supp. 2d at 45-46; Grant v. United States, No. 2:11-cv-00360, 2012 WL 5289309, at *8-9 (E.D. Cal. Oct. 23, 2012); York v. McHugh, 698 F. Supp. 2d 101, 108 (D.D.C. 2010); Mitchell v. VA, No. 1:07-cv-1015-TCB, 2008 WL 11432084, at *3 (N.D. Ga. June 12, 2008); Thompson v. State, 400 F. Supp. 2d 1, 14 (D.D.C. 2005); Harmer v. Perry, No. 95-4197, 1998 WL 229637, at *3 (E.D. Pa. Apr. 28, 1998), aff’d, No. 98-1532 (3d Cir. Jan. 29, 1999); Swenson, No. S-87-1282, 1994 U.S. Dist. LEXIS 16524, at *30 (E.D. Cal. Mar. 10, 1994); Connelly v. Comptroller of the Currency, No. H-84-3783, slip op. at 4 (S.D. Tex. June 3, 1991); Rodgers v. Army, 676 F. Supp. 858, 862 (N.D. Ill. 1988); Tuesburg v. HUD, 652 F. Supp. 1044, 1048 (E.D. Mo. 1987); Ely v. DOJ, 610 F. Supp. 942, 946 (N.D. Ill. 1985), aff’d, 792 F.2d 142 (7th Cir. 1986) (unpublished table decision). But see Rickles v. Marsh, No. 3:88-100, slip op. at 8-9 (N.D. Ga. Jan. 10, 1990) (awarding minimum damages even in absence of causation).

It also has been held that “[f]or there to be a causal link between the injury and the violation of the Act, the injury necessarily must be distinct and independent from the violation of the Act itself.” Schmidt

v. VA, 218 F.R.D. at 632; *see also* Doe v. Chao, 306 F.3d at 186 (Michaels, J., dissenting) (“The causal prong makes it especially clear that an adverse effect must be something distinct from the intentional and willful violation itself. For if a violation of the Privacy Act was sufficient to constitute an adverse effect, there could be no question of whether the violation caused the adverse effect, and hence the causal prong would be superfluous.”); Quinn, 978 F.2d at 135 (stating that in addition to establishing an adverse effect sufficient to confer standing, “plaintiff must also allege a causal connection between the agency violation and the adverse effect”); *cf.* Doe v. Chao, 540 U.S. 614, 627 (2004) (“The ‘entitle[ment] to recovery’ necessary to qualify for the \$1,000 minimum is not shown merely by an intentional or willful violation of the Act producing some adverse effect.”). *But cf.* Romero-Vargas v. Shalala, 907 F. Supp. 1128, 1134-35 (N.D. Ohio 1995) (stating, prior to Supreme Court’s decision in Doe v. Chao, that “emotional distress caused by the fact that the plaintiff’s privacy has been violated is itself an adverse effect, and that statutory damages can be awarded without an independent showing of adverse effects”; stating further in memorandum on motion to alter or amend judgment that “[i]t is eminently reasonable to infer that plaintiffs suffered mental distress by the fact of knowing their personal information had been disclosed”).

d. Fourth Element: Intentional or Willful Standard

In addition, an agency must be found to have acted in an “intentional or willful” manner in order for a damages action to succeed. *See* 5 U.S.C. § 552a(g)(4). This standard is discussed below under “Civil Remedies, Principles Applicable to Damages Lawsuits, Intentional or Willful Standard.”

3. Standard and Scope of Review

Certain statutes preempt the Privacy Act’s remedies for alleged violations of the Privacy Act’s disclosure provisions.

The issue of the Privacy Act’s applicability to disclosures of tax information has been analyzed by the Court of Appeals for the District of Columbia Circuit in Gardner v. United States, 213 F.3d 735 (D.C. Cir. 2000), *aff’d*, No. 96-1467, 1999 U.S. Dist. LEXIS 2195, at *14-17 (D.D.C. Jan. 29, 1999). In Gardner, the D.C. Circuit concluded that the Internal Revenue Code preempts the Privacy Act for remedies for disclosures of tax information, holding that 26 U.S.C. § 6103 is “the exclusive remedy for a taxpayer

claiming unlawful disclosure of his or her tax returns and tax information.” 213 F.3d at 741-42. Similarly, although not going quite as far, the Court of Appeals for the Fifth Circuit had previously held that “[26 U.S.C.] § 6103 is a more detailed statute that should preempt the more general remedies of the Privacy Act, at least where . . . those remedies are in conflict.” Hobbs v. United States, 209 F.3d 408, 412 (5th Cir. 2000) (finding § 6103 and the Privacy Act to be “in conflict” where disclosure fell within one of the exceptions in § 6103, and holding that “[t]o the extent that the Privacy Act would recognize a cause of action for unauthorized disclosure of tax return information even where § 6103 would provide an exception for the particular disclosure, § 6103 trumps the Privacy Act”). Other courts, too, have found the provisions of the tax code to be exclusive as to wrongful disclosures of tax information. See Ross v. United States, 460 F. Supp. 2d 139, 151 (D.D.C. 2006) (“[Section] 6103 is the exclusive remedy for a taxpayer claiming unlawful disclosure of his or her tax returns and information.”); Schwartz v. Kempf, No. 4:02-cv-198, 2004 U.S. Dist. LEXIS 2238, at *10-12 (W.D. Mich. Jan. 22, 2004) (citing Gardner and finding the provisions of the Privacy Act to be “trumped by the more specific provisions of the Internal Revenue Code found in 26 U.S.C. § 6103”); Berridge v. Heiser, 993 F. Supp. 1136, 1144-45 (S.D. Ohio 1997) (holding that 26 U.S.C. § 7431(a)(1), which provides a mechanism for the award of civil damages for unauthorized disclosure of tax return information (as defined in 26 U.S.C. § 6103), is the “exclusive remedy by which [plaintiff] may bring a cause of action for improper disclosure of return information”); Gov’t Nat’l Mortgage, Ass’n v. Lunsford, No. 95-273, 1996 U.S. Dist. LEXIS 1591, at *8 (E.D. Ky. Feb. 2, 1996) (dismissing Privacy Act claim for wrongful disclosure (presumably brought under subsection (g)(1)(D)) and stating that “26 U.S.C. § 7852(e) precludes the maintenance of Privacy Act damages remedies in matters concerning federal tax liabilities”).

Nevertheless, the Courts of Appeals for the Fourth and the Eighth Circuits, as well as the United States Tax Court, have readily applied the Privacy Act as well as the provisions of the tax code to disclosures of tax return information, with no discussion of the issue of preemption. See, e.g., Scrimgeour v. IRS, 149 F.3d 318, 325-26 (4th Cir. 1998) (affirming denial of damages and finding that the agency had not acted with gross negligence under 26 U.S.C. § 7431 or greater than gross negligence under the Privacy Act for wrongful disclosure claims resting upon identical factual allegations); Taylor v. United States, 106 F.3d 833, 835-37 (8th Cir. 1997) (affirming finding that disclosures did not violate 26 U.S.C. § 6103 or Privacy Act); Stone v. Comm’r of IRS, No. 3812-97, 1998 WL 547043, at *3 (T.C. Aug. 31, 1998) (finding that disclosures did not violate either 26 U.S.C.

§ 6103 or Privacy Act). In addition, one district court specifically considered the issue and arrived at the conclusion that the Privacy Act's remedies are available for the wrongful disclosure of tax return information. Sinicki v. Treasury, No. 97 CIV. 0901, 1998 WL 80188, at *3-5 (S.D.N.Y. Feb. 24, 1998) (denying motion to dismiss Privacy Act wrongful disclosure claim and stating that "the language, structure, purpose and legislative history of Section 6103 do not make manifest and clear a legislative intent to repeal the Privacy Act as it applies to tax return information").

Several district courts have held that various sections of the Internal Revenue Code prevent their exercise of subject matter jurisdiction over Privacy Act claims brought under subsection (g)(1)(D) for alleged violations of other provisions of the Privacy Act. See Welborn v. IRS, 218 F. Supp. 3d 64, 81 (D.D.C. 2016) (citing 26 U.S.C. §§ 6103(a), 7431 as preempting failure to safeguard and unauthorized disclosure claims under Privacy Act); Diamond v. IRS, No. CV 13-8042-GHK, 2014 WL 7883613, at *9, 115 A.F.T.R.2d 2015-319 (C.D. Cal. Nov. 14, 2014) (magistrate recommendation) (citing 26 U.S.C. § 6103 as superseding a Privacy Act claim for unauthorized disclosure of tax return), adopted, 2015 WL 64805, 115 A.F.T.R.2d 2015-328, 2015-1 USTCP 50,162 (C.D. Cal. Jan. 5, 2015); Schwartz v. Kempf, 2004 U.S. Dist. LEXIS 2238, at *10-12 (citing 26 U.S.C. § 7852(e), stating that "provisions of the Privacy Act do not apply, either directly or indirectly, to assessing the possibility of a tax liability," where plaintiffs alleged that IRS violated Privacy Act by contacting persons regarding plaintiffs' tax situation); Berridge v. Heiser, 993 F. Supp. 1136, 1145 (S.D. Ohio 1997) (holding that 26 U.S.C. § 7852(e) prevented it from exercising jurisdiction over plaintiff's Privacy Act claims under subsections (e)(2), (e)(5), and (e)(6) related to tax liability); Estate of Myers v. United States, 842 F. Supp. 1297, 1302-04 (E.D. Wash. 1993) (dismissing Privacy Act subsection (g)(1)(D) damages claim and applying § 7852(e)'s jurisdictional bar to preclude subject matter jurisdiction to consider action against IRS for alleged violation of subsection (e)(3) concerning summons issued to assist in determination of foreign tax liability); cf. Smilde v. Richardson, Comm'r, No. 97-568, 1997 U.S. Dist. LEXIS 15050, at *6-7 (D. Minn. Aug. 28, 1997) (relying on limitation of Privacy Act applicability pursuant to sections 6103 and 7852(e), and finding that "Privacy Act does not support subject matter jurisdiction" to enjoin IRS from contracting out processing of tax returns), aff'd per curiam, 141 F.3d 1170 (8th Cir. 1998) (unpublished table decision); Trimble v. United States, No. 92-74219, 1993 WL 288295, at *1 (E.D. Mich. May 18, 1993) (citing 26 U.S.C. § 7852(e) for Privacy Act's inapplicability and dismissing unspecified Privacy Act claim), aff'd, 28 F.3d 1214 (6th Cir. 1994) (unpublished table decision).

Note also that some courts have held that the exclusivity provision of the Federal Employees' Compensation Act, 5 U.S.C. § 8116(c) (2018), precludes a cause of action under the Privacy Act. See, e.g., Smith v. Nicholson, 287 F. App'x 402, 403-05 (5th Cir. 2008) (per curiam) (discussing where Labor Secretary denied plaintiff's FECA claim alleging that VA injured him by disclosing his records "not for lack of coverage, but for insufficient proof," holding that "such a denial is conclusive as to FECA coverage"; "the Secretary found FECA applicable" and "[t]hat decision precludes any further action on [plaintiff's] Privacy Act claim"); Richards v. CIA, 837 F. Supp. 2d 574, 579-580 (E.D. Va. 2011) (dismissing Privacy Act claim because "[t]he disclosures and the subsequent harm came exclusively in the context of [plaintiff's] employment at the CIA" and stating that "absent a determination by the Secretary of Labor that FECA does not cover [plaintiff's] Privacy Act claim, this Court has no jurisdiction to entertain the Privacy Act claim"); Carte v. United States, No. 2:07-0515, 2010 WL 3259420, at *7-8 (S.D. W. Va. Aug. 18, 2010) (concluding that "whether viewed as being precluded by a merits based DOL decision or a decision of lesser quantum leaving open the substantial question of whether [plaintiff's] injuries, if any, were sustained while performing his duties, section 8116(c) bars a Privacy Act claim from being pursued in this action," where plaintiff attempted to recover for injury allegedly caused by agency's disclosure of his medical information by filing both FECA claim and Privacy Act claim); Vogrin v. ATF, No. 598CV117, 2001 WL 777427, at *7-8 (N.D. W. Va. Mar. 30, 2001) (ruling that FECA's exclusivity provision "precludes a suit under the Privacy Act even if FECA does not provide benefits for all of the injuries that [the plaintiff] claims"), aff'd per curiam, 15 F. App'x 72 (4th Cir. 2001).

Similarly, it has been held that the Civil Service Reform Act deprives a court of subject matter jurisdiction over a Privacy Act claim brought under subsection (g)(1)(D). See Henderson v. Air Force, No. 06-323, 2008 WL 4542761, at *2-3 (D. Ariz. Oct. 10, 2008), aff'd, 370 F. App'x 807 (9th Cir. 2010). This issue is discussed more fully above in the section titled, "5 U.S.C. § 552a(g)(1)(C) - Damages Lawsuits for Failure to Assure Fairness in Agency Determinations."

Subsection (g)(1)(D) suits cannot be used to collaterally attack agency determinations.

Consistent with case law under subsection (g)(1)(C), the District Court for the District of Columbia has stated that a plaintiff “cannot rely on any arguable violation of the Privacy Act” under (g)(1)(D) – in that case an alleged wrongful disclosure – to “collaterally attack” an agency personnel decision. Hanna v. Herman, 121 F. Supp. 2d 113, 123-24 (D.D.C. 2000) (finding that MSPB did not err in refusing to address plaintiff’s Privacy Act argument, but, “assuming arguendo that [he] preserved [it],” discussing merits of plaintiff’s “Privacy Act defense to the demotion”), summary affirmance granted sub nom. Hanna v. Chao, No. 00-5433 (D.C. Cir. Apr. 11, 2001); Hinson-Gribble v. OPM, No. 5:16-CV-70-FL, 2017 WL 9480265, at *5 (E.D.N.C. July 11, 2017) (dismissing Privacy Act claim to extent that plaintiff seeks to obtain relief from substantive decisions made with respect to various benefits she contends are due her); Melvin v. VA, F. Supp. 3d 350, 357 (D.D.C. 2014) (finding Privacy Act provisions for amending records not designed to permit collateral attack upon that which has already been subject of a judicial or quasi-judicial action). See also Cross, No. 3:09-CV-1293, 2013 WL 1149525, at *10 (N.D.N.Y. Mar. 19, 2013) (dismissing plaintiff’s damages claim for wrongful disclosure relating to her termination from United States Postal Service because she “does not articulate the disclosure of any specific information contained in a system of records”); Doe v. DOJ, 660 F. Supp. 2d at 50-51 (concluding that plaintiff’s subsection (b)/(g)(1)(D) claim against MSPB for refusing to allow him to proceed under pseudonym was “collateral attack” of that decision because plaintiff’s claim “attempts to achieve the same forbidden objective” as prototypical collateral attacks – “relitigating issues already decided by the ALJ”).

E. Principles Applicable to Damages Lawsuits

“In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of . . . actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000.” 5 U.S.C. § 552a(g)(4).

1. Intentional or Willful Standard

Comment:

Damages suits under the Privacy Act require that the agency acted in an “intentional or willful” manner.

In order for there to be any liability in a subsection (g)(1)(C) or (g)(1)(D) damages lawsuit, the agency must have acted in an “intentional or willful” manner. 5 U.S.C. § 552a(g)(4). The words “intentional” and “willful” in subsection (g)(4) do not have their vernacular meanings; instead, they are “terms of art.” White v. OPM, 840 F.2d 85, 87 (D.C. Cir. 1988) (per curiam); see also Convertino v. DOJ, 769 F. Supp. 2d 139, 145-46 (D.D.C. 2011) (noting that “[s]tandards of intentionality and willfulness are anything but rare in the law” but explaining that “the Privacy Act’s intent or willfulness requirement is peculiar to the Act and must not be confused with less exacting standards parading under the same name from other common law or statutory sources” (citing White)), rev’d and remanded on other grounds, 684 F.3d 93 (D.C. Cir. 2012). The Act’s legislative history indicates that this unique standard is “[o]n a continuum between negligence and the very high standard of willful, arbitrary, or capricious conduct,” and that it “is viewed as only somewhat greater than gross negligence.” 120 Cong. Rec. 40,406, reprinted in Source Book at 862, https://www.justice.gov/opcl/paoverview_sourcebook.

While not requiring premeditated malice, see Parks v. IRS, 618 F.2d 677, 683 (10th Cir. 1980), cases analyzing subsection (g)(4) have held that, to meet the “intentional or willful” standard, the agency’s actions must be:

- So patently egregious and unlawful that anyone undertaking the conduct should have known it was unlawful. E.g., Maydak v. United States, 630 F.3d 166, 179-83 (D.C. Cir. 2010); Sussman v. Marshals Serv., 494 F.3d 1106, 1122 (D.C. Cir. 2007); Laningham v. Navy, 813 F.2d 1236, 1242-43 (D.C. Cir. 1987) (per curiam); Albright v. United States, 732 F.2d 181, 189 (D.C. Cir. 1984); Wisdom v. HUD, 713 F.2d 422, 424-25 (8th Cir. 1983);
- Somewhat greater than gross negligence. E.g., Coleman v. United States, 12 F.3d 824, 836-837 (5th Cir. 2019); Maydak, 630 F.3d at 179-83; Beaven v. DOJ, 622 F.3d 540, 547-53 (6th Cir. 2010); Powers v. Parole Comm’n, 296 F. App’x 86, 87 (D.C. Cir. 2008); Scrimgeour v. IRS, 149 F.3d 318, 326 (4th Cir. 1998); Rose v. United States, 905 F.2d

OVERVIEW OF THE PRIVACY ACT

1257, 1260 (9th Cir. 1990); Britt v. Naval Investig. Service, 886 F.2d 544, 551 (3d Cir.1989); Andrews v. VA, 838 F.2d 418, 424-25 (10th Cir. 1988); Bruce v. United States, 621 F.2d 914, 917 (8th Cir. 1980);

- In flagrant disregard of an individual's rights under the Privacy Act. E.g., Lewis v. Mossbrooks, 788 F. App'x 455, 458 (9th Cir. 2019); Maydak, 630 F.3d at 179-83; Pippinger v. Rubin, 129 F.3d 519, 530 (10th Cir. 1997); Deters v. Parole Comm'n, 85 F.3d 655, 660 (D.C. Cir. 1996); Kellett v. BOP, 66 F.3d 306 (1st Cir. 1995) (per curiam) (unpublished table decision); Covert v. Harrington, 876 F.2d 751, 756-57 (9th Cir. 1989); or
- Without grounds for believing the agency's actions to be lawful. E.g., Maydak, 630 F.3d at 179-83; Kellett, 66 F.3d at *3; Covert, 876 F.2d at 756-57; Albright, 732 F.2d at 189-90.

Negligence violations are insufficient to meet the "intentional or willful" standard.

A mere negligent or inadvertent violation of the Privacy Act is not enough to clear this formidable "intentional or willful" barrier for a plaintiff seeking damages. See, e.g., Lewis v. Mossbrooks, 788 F. App'x at 458 (concluding that plaintiff's complaint did not suggest that in failing to remove flag in his record, any VA employee "'flagrantly disregard[ed]' Lewis' privacy rights or acted 'without grounds for believing [their action] to be lawful,' rather than negligently." (citations omitted)); Campbell v. SSA, 446 F. App'x 477, 479, 481 (3d Cir. 2011) (upholding district court conclusion that "there was no record evidence to support an assertion of willful or intentional conduct" where district court found that plaintiff's "assertion that his wife discovered some documents in her SSA file that should have been in his file, if true, established nothing more than negligence"); Maydak, 630 F.3d at 179-83 (holding that BOP did not intentionally or willfully commit Privacy Act violations because, among other reasons, records "were used only for legitimate law enforcement purposes" and notwithstanding court's "critical discussion of the review and retention policies" in prior opinions, "BOP officials were still never placed on clear notice that their practices violated the Act"); Wilkerson v. Shinseki, 606 F.3d 1256, 1268 (10th Cir. 2010) (finding standard not met where VA physician accessed plaintiff's medical records because physician testified that "he thought he could access the record so long as he had a 'need to know'" and "given that [plaintiff's] health records were relevant to whether he could continue working at the VA, [that] belief was reasonable"); Scrimgeour, 149 F.3d at 326 (finding plaintiff did not

“demonstrate the higher standard of culpability required for recovery under the Privacy Act” where court had already determined that IRS’s release of his tax returns did not meet lower standard of gross negligence under provision of Internal Revenue Code); Deters, 85 F.3d at 660 (finding that Parole Commission did not “‘flagrantly disregard’” plaintiff’s privacy when it supplemented his file with rebuttal quantity of drugs attributed to him in presentence investigation report (PSI) and offered inmate hearing concerning accuracy of disputed report and concluding that “[e]ven if the Commission inadvertently or negligently violated [plaintiff’s] Privacy Act rights by not examining the accuracy of the PSI before preparing a preliminary assessment . . . such a violation (if any) could in no sense be deemed ‘patently egregious and unlawful’” (quoting Albright and Laningham, *infra*)); Dowd v. IRS, 776 F.2d 1083, 1084 (2d Cir. 1985) (per curiam) (holding “mere administrative error” in negligently destroying files was not predicate for liability); Chapman v. NASA, 736 F.2d 238, 242-43 (5th Cir. 1984) (per curiam) (holding standard not met where agency “reasonably could have thought” untimely filing of evaluations was proper; “before our previous opinion ‘timely’ had no precise legal meaning in this circuit”); Wisdom v. HUD, 713 F.2d 422, 424-25 (8th Cir. 1983) (finding no willful violation of Act where good faith release of loan default records is pursuant to unchallenged “Handbook”); Perry v. Block, 684 F.2d 121, 129 (D.C. Cir. 1982) (finding delayed disclosure of documents through administrative oversight was not intentional or willful); Bruce v. United States, 621 F.2d 914, 917 (8th Cir. 1980) (finding standard not met where agency relied on regulations permitting disclosure of records pursuant to subpoena, as there were “at that time no regulations or other authority to the contrary”); Brown v. Esper, No. 1:17-cv-02004-RM-STV 2019 WL 6893019 at *9 (Dec. 18, 2019) (“The fact that DHA employees were able to locate files pertaining to Plaintiff on the shared drive is not indicative of flagrant or egregious conduct rising to [willful or intentional conduct]. Nor does the fact that DHA employees received training on the Privacy Act mean that every alleged violation is intentional or willful.”); Yusim v. Office of Acting Commissioner of SSA, 406 F. Supp. 3d 194, 196 (E.D.N.Y. 2018) (finding defendant’s alleged “ignorance” insufficient to meet intentional or willful standard); Chesser v. FBI, No. 1:13cv129 (LO/IDD), 2017 WL 663348, at *6 (E.D. Va. Feb. 17, 2017) (finding that because defendant’s “letter informing plaintiff of the disclosure establishes that defendants believed their disclosure was legal pursuant to § 552a(b)(8),” plaintiff could not establish that defendants’ disclosure was intentional or willful); Hills v. Liberty Mut. Ins., No. 14–CV–0328S, 2015 WL 1243337 (W.D.N.Y. Mar. 18, 2015) (“[T]o the extent, if any, that Plaintiff asserts that SSA employees should have discerned the true limited scope of the consent before disclosing Plaintiff’s

information, this allegation amounts to at best mere negligence or administrative error, which is insufficient to state a claim under the Privacy Act.”); Taylor v. Def. Fin. & Accounting Servs., No. 2:12-2466, 2014 WL 28820, at *9 (E.D. Cal. Jan. 3, 2014) (granting defendant’s summary judgment motion and finding that while “res ipsa loquitur is a viable theory of negligence, it cannot be used to prove intentional or willful conduct”); Williams v. United States, No. 12-00375, 2013 WL 3288306, at *11-15 (D. Haw. June 28, 2013) (finding that agency attempt[] to comply with [plaintiff’s] authorization” demonstrated intent to comply with Privacy Act and agency’s “attempts to remedy or mitigate the effects of the disclosure also show lack of willful or intentional agency action”); Reed v. Navy, 910 F. Supp. 2d 32, 44-45 (D.D.C. 2012) (explaining that even if agency employee “made any disclosures that crossed the line, the evidence does not support a conclusion that [agency employee] acted with ‘flagrant disregard’ for the Act”); Grant v. United States, No. 2:11-cv-00360, 2012 WL 5289309, at *10 (E.D. Cal. Oct. 23, 2012) (explaining that disclosure was not willful or intentional but inadvertent because “[b]efore sending out the . . . claim package, [defendant] redacted several mentions of plaintiff’s [medical] condition from the records in the claim package, but missed a few other references to plaintiff’s [medical condition], as well as certain references to certain medications that, unbeknownst to [defendant] at the time, were used to treat [plaintiff’s medical condition].”); McIntyre v. Fulwood, 892 F. Supp. 2d 209, 218 (D.D.C. 2012) (finding defendant’s actions were not intentional or willful because “[t]he Commission ceased reliance on the erroneous information, and has articulated a rational basis for its decision to deny Plaintiff parole”); Tungjunyatham v. Johanns, No. 1:06-cv-1764, 2009 WL 3823920, at *23 (E.D. Cal. Nov. 13, 2009) (finding standard not met “[i]n light of the two representatives’ established practice of communicating by [fax] in such a fashion” where agency representative faxed to office of plaintiff’s EEO representative records concerning plaintiff while latter representative was out of town and, as a result, “numerous agency employees had the chance to see the documents”), *aff’d*, Tungjunyatham v. Johanns, 500 F. App’x 686, 689 (9th Cir. 2012); Walker v. Gambrell, 647 F. Supp. 2d 529, 537-38 (D. Md. July 16, 2009) (alternative holding) (finding standard not met where plaintiff missed work due to miscarriage, her husband called agency to inform office of reason for plaintiff’s absence, employee who received call reacted in disruptive manner, and agency official sent e-mail to staff regarding miscarriage to inform it of reason for disruption; “disclosure may show negligence or a lack of tact and sensitivity; however, evidence of negligence is not sufficient to show that the agency acted willfully or intentionally”); Baptiste v. BOP, 585 F. Supp. 2d 133, 135 (D.D.C. 2008) (concluding that ICE’s failure to confirm receipt of faxed notice regarding

plaintiff's citizenship is no worse than negligence); Mulhern v. Gates, 525 F. Supp. 2d 174, 185-86 (D.D.C. 2007) (holding inadvertent disclosure "while attempting to assist plaintiff" not sufficient to satisfy standard); Elliott v. BOP, 521 F. Supp. 2d 41, 48 (D.D.C. 2007) (finding standard not met where BOP based plaintiff's designation on inaccurate presentence report because "BOP was [not] aware of any potential inaccuracy in [that] report"), abrogated on other grounds, Williams v. United States District Court, District of Columbia, 806 F. Supp. 2d 44, 48 (D.D.C. 2011); Thompson v. State, 400 F. Supp. 2d 1, 12-13 (D.D.C. 2005) (finding standard not met in subsection (e)(2) claim where agency "assumed that it would be appropriate to correspond with [plaintiff's doctor] about [plaintiff's] medical condition" because "it was plaintiff's doctor who made the first contact with the [agency], offering unsolicited medical information on plaintiff's behalf"); Wiley v. VA, 176 F. Supp. 2d 747, 756-57 (E.D. Mich. 2001) (stating that even if agency violated Privacy Act by disclosing VA claims file to employer pursuant to broadly written release, agency's actions were not "beyond grossly negligent," as "reasonable minds clearly could differ on the scope of the release," and thus agency's reliance on it "cannot be deemed wholly groundless"); Porter v. USPS, No. CV595-30, slip op. at 10, 13, 21-22 (S.D. Ga. July 24, 1997) (concluding that Postal Service acted with "mere negligence" when it disclosed letter from plaintiff's attorney written as response to plaintiff's proposed termination to two union officials with belief that they had "a right and duty to know the disciplinary affairs of a fellow postal worker" even though plaintiff had not filed grievance through union and "had specifically instructed the management that he did not want anyone from the [union] representing his interests"), aff'd, 166 F.3d 352 (11th Cir. 1998) (unpublished table decision); Smith v. BOP, No. 94-1798, 1996 WL 43556, at *2 (D.D.C. Jan. 31, 1996) (finding standard not met where adverse determination had been rectified; the fact that certain forms were corrected immediately, even though another form may not have been, "indicates that BOP officials did not intend to maintain plaintiff's records incorrectly"); Baitey v. VA, No. 8:CV89-706, slip op. at 8 (D. Neb. June 21, 1995) (finding standard not met where plaintiff failed to prove that VA acted in "flagrant or reckless disregard of [plaintiff's] rights under the Privacy Act" when it disclosed his medical records in response to incomplete and unsigned medical authorization); Olivares v. NASA, 882 F. Supp. 1545, 1549-50 (D. Md. 1995) (finding NASA's actions in contacting educational institutions to verify and correct discrepancies in plaintiff's record, even assuming initial consent to contact those institutions was limited, were not even negligent and do not "come close" to meeting standard), aff'd, 103 F.3d 119 (4th Cir. 1996) (unpublished table decision); Stephens v. TVA, 754 F. Supp. 579, 582 (E.D. Tenn. 1990) (finding no damages where "some

authority” existed for proposition that retrieval not initially and directly from system of records was not “disclosure,” and agency attempted to sanitize disclosed records); Blanton v. DOJ, No. 82-0452, slip op. at 6-8 (D.D.C. Feb. 17, 1984) (finding unauthorized “leak” of record not intentional or willful agency conduct); Krohn v. DOJ, No. 78-1536, slip op. at 3-7 (D.D.C. Nov. 29, 1984) (finding standard not met where agency relied in good faith on previously unchallenged routine use to publicly file records with court); Daniels v. St. Louis VA Reg'l Office, 561 F. Supp. 250, 252 (E.D. Mo. 1983) (finding mere delay in disclosure due in part to plaintiff’s failure to pay fees was not intentional or willful); Doe v. GSA, 544 F. Supp. 530, 541-42 (D. Md. 1982) (finding disclosure not “wholly unreasonable” where “some kind of consent” given for release of psychiatric records and where agency employees believed that release was authorized under GSA’s interpretation of its own guidelines, even though court concluded that such interpretation was erroneous).

In a number of other cases, courts have found that the plaintiff did not meet the “intentional or willful standard” without deciding whether the agency had violated the Privacy Act.

In addition to cases in which the court held that a mere negligent or inadvertent violation of the Privacy Act was insufficient to meet the “intentional or willful standard,” additional cases have concluded that plaintiffs have failed to meet this high standard for a variety of other reasons. *See, e.g., Jacobs v. BOP*, No. 12-5129, 2012 WL 6603085, at *1 (D.C. Cir. Dec. 17, 2012) (holding that “appellant has failed to demonstrate the Bureau violated the Act in an intentional or willful manner”); Luster v. Vilsack, 667 F.3d 1089, 1098 (10th Cir. 2011) (“[G]iven the lack of any authority in support of [plaintiff’s] contention that it is a violation of the Privacy Act to transmit confidential materials (all but one of which was covered by a transmittal cover sheet) to an unsecured fax machine, we agree with the district court that [plaintiff] has not demonstrated that any actual disclosure by [defendant] was willful and intentional.”); Puerta v. HHS, No. 99-55497, 2000 WL 863974, at *3 (9th Cir. June 28, 2000) (finding where agency, upon advice of its general counsel’s office, disclosed documents in response to grand jury subpoena, agency “may have intentionally produced [the] documents, but it does not necessarily follow that [it] intentionally violated . . . the Privacy Act”); Nathanson v. FDIC, No. 95-1604, 1996 U.S. App. LEXIS 3111, at *3-6 (1st Cir. Feb. 22, 1996) (per curiam) (affirming on grounds that disclosure was not intentional and willful because routine use “afforded reasonable grounds for belie[f] that [agency employee’s] conduct was lawful”); Scullion v. VA, No. 87-2405, slip op. at 4-8 (7th Cir. June 22,

1988) (holding no damages where agency relied upon apparently valid and unrevoked written consent to disclose records); Moskiewicz v. USDA, 791 F.2d 561, 564 (7th Cir. 1986) (noting that “elements of recklessness often have been a key characteristic incorporated into a definition of willful and intentional conduct”); Edison v. Army, 672 F.2d 840, 846 (11th Cir. 1982) (stating failure to prove agency acted “unreasonably” in maintaining records precludes finding intentional or willful conduct); Ahuruonye v. Interior, 2017 U.S. Dist. LEXIS 33207 (D.D.C. Mar. 8, 2017) (finding plaintiff had failed to demonstrate that defendant acted intentionally or willfully because plaintiff relied “exclusively upon speculative and conclusory statements”); Hurt v. D.C. Court Servs. & Offender Supervision Agency, 827 F. Supp. 2d 16, 21 (D.D.C. 2011) (finding standard not met where agency officials “believed that under [agency] policy they could disclose public information, such as the plaintiff’s conviction, to a third party without running afoul of the Privacy Act”); Alexander v. FBI, 691 F. Supp. 2d 182, 191 (D.D.C. 2010) (finding standard not met where agency disclosed records in response to “facially ordinary requests submitted according to unchallenged procedures that had been in place for thirty years” and “pursuant to its unchallenged regulations”), aff’d per curiam on other grounds, 456 F. App’x 1 (D.C. Cir. 2011); Trice v. Parole Comm’n, 530 F. Supp. 2d 213, 215 (D.D.C. 2008) (“Although plaintiff disagreed with the victim’s version of the circumstances surrounding the assault, he was able to provide his version of events at the revocation hearing. Plaintiff therefore cannot demonstrate to a reasonable fact finder that the Commission acted with the requisite level of intent [by considering only plaintiff’s version.”); Armstrong v. BOP, 976 F. Supp. 17, 22 (D.D.C. 1997) (finding standard not met where BOP refused to amend prison records to incorporate favorable information from inmate’s prior incarceration in accordance with BOP guidelines), summary affirmance granted, Armstrong v. BOP, No. 97-5208, 1998 WL 65543, at *1 (D.C. Cir. Jan. 30, 1998); Harris v. USDA, No. 3:92CV-283-H, slip op. at 1-2, 4-5 (W.D. Ky. May 14, 1996) (finding standard not met where agency acted pursuant to Correspondence Management Handbook in maintaining supporting documentation for plaintiff’s 1975 suspension), aff’d, 124 F.3d 197 (6th Cir. 1997) (unpublished table decision); Sterling v. United States, 826 F. Supp. 570, 572 (D.D.C. 1993) (finding standard not met where agency’s “efforts both before and after the release of information . . . indicate a sensitivity to the potential harm the release might cause and represent attempts to avert that harm”), summary affirmance granted, No. 93-5264 (D.C. Cir. Mar. 11, 1994); cf. Iqbal v. DOJ, No. 3:11-cv-369-J-37, 2013 WL 3903642, at *5 (M.D. Fla. Sept. 26, 2013) (“[T]he Court previously held that Plaintiff could satisfy his burden to allege intentional and willful conduct by making allegations consistent with Rule 9(b). . . . Plaintiff has

sufficiently met this standard.”); Stokes v. Barnhart, 257 F. Supp. 2d 288, 299-300 (D. Me. 2003) (citing Andrews, 838 F.2d at 424-25, and Albright, 732 F.2d at 189, and allowing plaintiff to amend complaint because agency employee’s belief “that her conduct violated any law or regulation... is not, and cannot be, determinative”).

For claims based on alleged violations of subsection 552a(b), several courts have required plaintiffs to identify the individual who disclosed the information in order to establish that the disclosure was “intentional or willful.”

In the context of a claim for disclosure in violation of subsection 552a(b), several courts have ruled that a plaintiff cannot show intentional or willful conduct without identifying the individual or individuals who disclosed the information. See, e.g., Convertino v. DOJ, 769 F. Supp. 2d 139, 146 (D.D.C. 2011) (“To meet the Privacy Act’s high standard for a showing of willfulness or intentionality, [plaintiff] must know the leaker’s identity. . . . [L]acking any evidence of the leaker’s identity, no reasonable fact-finder could find that DOJ acted willfully or intentionally with regard to any leak in this case.”), rev’d and remanded on other grounds, 684 F.3d 93 (D.C. Cir. 2012) (reversing district court’s summary judgment and ruling that district court committed abuse of discretion in denying appellant’s motion to stay summary judgment to allow for further discovery to determine leaker’s identity); Paige v. DEA, 818 F. Supp. 2d 4, 14 (D.D.C. 2010) (“In order to prove that [agency] acted willfully and intentionally, it is essential that Plaintiff identify the source of the disclosure.”), aff’d, 665 F.3d 1355 (D.C. Cir. 2012); Convertino v. DOJ, No. 07-cv-13842, 2008 WL 4104347, at *7 (E.D. Mich. Aug. 28, 2008) (“To establish that the DOJ committed a willful or intentional violation, [plaintiff] must present evidence of the disclosing person’s state of mind, which requires him to identify and question those who perpetrated the allegedly improper disclosure.”); cf. Lee v. DOJ, 413 F.3d 53, 55, 60 (D.C. Cir. 2005) (upholding district court order “holding [journalists] in contempt of court for refusing to answer questions regarding confidential sources” because “[i]f [plaintiff] cannot show the identities of the leakers, [plaintiff’s] ability to show the other elements of the Privacy Act claim, such as willfulness and intent, will be compromised”); Hatfill v. Gonzales, 505 F. Supp. 2d 33, 43 (D.D.C. 2007) (granting motion to compel reporters to disclose identity of individuals who disclosed information protected by Privacy Act because “the identity of DOJ and FBI sources will be an integral component of the plaintiff’s attempt to prove the requisite agency mens rea”).

Several district courts have allowed cases to proceed because the plaintiff sufficiently alleged intentional or willful conduct.

Several district court decisions have found “intentional or willful” violations of the statute, or have otherwise allowed cases to proceed after finding that plaintiffs presented sufficient facts regarding an agency’s alleged intentional or willful conduct. See, e.g., Ashbourne v. Hansberry, 302 F. Supp. 3d 338, 347-48 (D.D.C. Mar. 27, 2018) (“Accepting Ms. Ashbourne’s factual allegations as true and drawing all reasonable inferences in her favor, it is plausible that the DHS defendants are liable for a violation of . . . the Privacy Act.”); Kelley v. FBI, 67 F. Supp. 3d 240, 258 (D.D.C. 2014) (finding plaintiff “set forth sufficient facts about the alleged disclosure of information about plaintiffs to the media to overcome the low threshold at the motion to dismiss stage and create an inference of intentional and willful misconduct that allows” plaintiff’s first claim to proceed); Babatu v. Dallas VA Med. Ctr., No. 3:11-CV-00533, 2014 WL 626515, at *12 (N.D. Tex. Feb. 18, 2014) (considering “scope of employment . . . to the extent that it may be probative of whether [agency employee] acted intentionally or willfully in accessing and disclosing [plaintiff’s] information in [agency’s] database” and concluding that “an employee’s conduct, as well as the agency’s conduct, is relevant to the determination of whether a violation was intentional or willful”); Makowski v. United States, 27 F. Supp. 3d 901, 913 (N.D. Ill. 2014) (finding that plaintiff “has sufficiently pleaded facts to support his claim that DHS willfully violated its duty under the Privacy Act to maintain accurate records” in light of fact that agency did not update plaintiff’s citizenship status after being put on notice “not only that its record pertaining to [plaintiff’s] citizenship status was inaccurate, but also that this inaccuracy had the potential to contribute to an adverse immigration enforcement determination regarding [plaintiff] – as it did with the issuance of the 2009 detainer”); Minshew v. Donley, 911 F. Supp. 2d 1043, 1072 (D. Nev. 2012) (denying agency’s motion, as “[a] reasonable jury thus could find the [agency] acted in flagrant disregard of [plaintiff’s] rights by making an unsolicited disclosure of information contained within [plaintiff’s] OPF” to contractor “despite the fact that [contractor] did not request the information and indeed objected to the [agency’s] attempt to interfere with [plaintiff’s] placement”); Feldman v. CIA, 797 F. Supp. 2d 29, 40 (D.D.C. 2011) (finding that “plaintiff has adequately alleged intentional or willful conduct at this stage of the litigation” and denying agency’s motion to dismiss); McCullough v. BOP, No. 1:06-cv-00563, 2010 WL 5136133, at *6-7 (E.D. Cal. Dec. 6, 2010) (magistrate’s recommendation) (“Plaintiff’s allegation that [BOP] employees falsified reports and his central file and used those records to convict him of a rule violation is sufficient to state a cognizable claim

against [BOP].”), adopted, 2010 WL 5476701 (E.D. Cal. Dec. 29, 2010); Tolbert-Smith v. Chu, 714 F. Supp. 2d 37, 43-44 (D.D.C. 2010) (declining to dismiss allegation that agency employee “placed records referring and relating to [plaintiff’s] disability on a server accessible by other federal employees and members of the public . . . to retaliate against her for filing an administrative complaint”); Doe v. Goss, No. 04-2122, 2007 WL 106523, at *12 (D.D.C. Jan. 12, 2007) (“If proven, Defendants’ calculated recording of false information pursuant to these allegedly sham investigations would certainly meet Deters’ definition of a willful or intentional conduct.”); Carlson v. GSA, No. 04-C-7937, 2006 WL 3409150, at *5 (N.D. Ill. Nov. 21, 2006) (discussing e-mail sent by agency employee’s supervisor to other agency personnel and to individuals outside agency regarding plaintiff’s termination settlement agreement, which included “unnecessary details concerning [employee’s] personal information” and which supervisor encouraged recipients to disseminate); Doe v. Herman, No. 297-CV-00043, 1999 WL 1000212, at *1, *13-14 (finding unnecessary the disclosure of claimant’s social security number on multi-captioned hearing form to twenty other claimants, coal companies, and insurance companies); Tomasello v. Rubin, No. 93-1326, slip op. at 17-19 (D.D.C. Aug. 19, 1997) (concerning disclosure to “60 Minutes” and all 4,500 ATF employees of details concerning plaintiff’s EEO complaint), aff’d on other grounds, 167 F.3d 612 (D.C. Cir. 1999); Porter, No. CV595-30, slip op. at 10, 13, 22-23 (S.D. Ga. July 24, 1997) (concerning disclosure by Postmaster to USPS personnel who had no “need to know” of plaintiff’s two-week suspension for impersonating a postal inspector); Romero-Vargas v. Shalala, 907 F. Supp. 1128, 1133-34 (N.D. Ohio 1995) (finding telephonic verification or non-verification of plaintiffs’ social security numbers provided by agency to their employers in violation of regulations and agency employee manual); Swenson v. USPS, No. S-87-1282, 1994 U.S. Dist. LEXIS 16524, at *33-45 (E.D. Cal. Mar. 10, 1994) (discussing disclosure to Members of Congress, who were seeking to assist constituent with complaint regarding rural mail delivery, of irrelevant information concerning plaintiff’s EEO complaints and grievances); Connelly v. Comptroller of the Currency, No. H-84-3783, slip op. at 25-27 (S.D. Tex. June 3, 1991) (addressing violation of subsection (e)(5) by disapproving of plaintiff’s appointment as president of new bank without first obtaining evaluations of prominent bankers who knew plaintiff); MacDonald v. VA, No. 87-544-CIV-T-15A, slip op. at 4, 7 (M.D. Fla. July 28, 1989) (discussing disclosure of “counseling memorandum” to plaintiff’s employer “with malicious intent and with the purpose to injure Plaintiff”); Fitzpatrick v. IRS, 1 Gov’t Disclosure Serv. (P-H) ¶ 80,232, at 80,580 (N.D. Ga. Aug. 22, 1980) (discussing disclosure to plaintiff’s co-workers and former co-worker that he had retired for “mental” reasons,

even though purpose of disclosure was to “quell[] rumors and gossip”), aff’d in part, vacated & remanded in part, on other grounds, 655 F.2d 327 (11th Cir. 1982).

At least two courts of appeals, the Sixth and Ninth Circuits, have found intentional or willful Privacy Act violations.

At least two courts of appeals have found “intentional or willful” violations of the statute – the Court of Appeals for the Sixth Circuit and the Court of Appeals for the Ninth Circuit. See Beaven v. DOJ, 622 F.3d 540, 547-53 (6th Cir. 2010); Louis v. Labor, 19 F. App’x 487, 488-89 (9th Cir. 2001); Wilborn v. HHS, 49 F.3d 597, 602-03 (9th Cir. 1995); Covert v. Harrington, 876 F.2d 751, 756-57 (9th Cir. 1989); cf. Oja v. Army Corps of Eng’rs, 440 F.3d 1122, 1136 (9th Cir. 2006) (concluding that “it was clear . . . that the [agency’s] disclosures were intentional or willful” where agency posted information about former employee on its Web site, but dismissing claim as untimely).

In Beaven, a group of BOP employees sued the agency for unlawful disclosure after a BOP investigator left an “employee roster” containing “sensitive personal information” on a desk in an area to which prisoners had access. See 622 F.3d at 544-45. The district court had “found that [the investigator’s] course of conduct resulted in a disclosure under the Privacy Act . . . and that his actions were ‘intentional or willful’ within the meaning of § 552a(g)(4), although his final act of leaving the folder unsecured was ‘inadvertent.’” 622 F.3d at 547; see also v. DOJ, No. 03-84, 2007 WL 1032301, at *2, 14-17 (E.D. Ky. Mar. 30, 2007)). The Court of Appeals for the Sixth Circuit framed the “main issue” as “whether the requirement under § 552a(g)(4) that the district court find that ‘the agency acted in a manner which was intentional or willful’ requires the court to find that the final act that resulted in the disclosure was ‘intentional or willful’ or whether the court may find that the entire course of conduct that resulted in the disclosure was ‘intentional or willful.’” Beaven, 622 F.3d at 547. In holding the latter to be correct, the Sixth Circuit pointed out that “[n]o court has specifically interpreted § 552a(g)(4) in the light this panel must address” but observed, after reviewing the case law, that courts “determining whether a Privacy Act violation occurred have not differentiated between the final act and the course of action that results in the final act, but rather courts generally look to the entire course of conduct in context.” Id. at 548-50. The Sixth Circuit went on to conclude that “the facts in the instant case support[] the district court’s conclusion” and that the district court “did not commit clear error in finding that [the investigator’s] course of conduct was ‘willful.’” Id. at 552. The court noted that the investigator had “carried the

folder, which he knew contain[ed] confidential and sensitive information, into an inmate-accessible work area for the purpose of carrying out his own investigative work should he need to call a . . . computer administrator at home. Yet the roster [in the folder] not only listed the home telephone numbers of . . . computer administrators but also included detailed private and personal information related to all [of the prison facility] employees”; and that the roster was not marked “[Limited Official Use]-Sensitive,” as required by a BOP Program Statement, among other violations of BOP policy. Id. The Court stated that the investigator’s “need for some of the information . . . did not provide a legitimate basis for him to have the entire contents of the folder with him at the time” and that his “course of conduct that resulted in his leaving the unmarked folder in an inmate-accessible area . . . could properly be viewed as ‘the intentional or willful failure of the agency to abide by the Act.’” Id. at 552-53. See also Downie v. City of Middleburg Hts., 301 F.3d 688, 697-99 (6th Cir. 2002) (citing Toolasprashad, infra, and stating that “[w]hile the Privacy Act does not provide a separate damages remedy for the intentional or willful creation, maintenance, or dissemination of false records in retaliation for an individual’s First Amendment rights, we believe that retaliation on any basis clearly constitutes intentional or willful action”).

In Louis, the plaintiff had sought reconsideration of the denial of his claim for Federal Employees Compensation benefits by the Department of Labor. See 19 F. App’x at 488. In denying the plaintiff’s request for reconsideration, the Department indicated that it had considered the entirety of its prior decision, including a portion of that prior decision that impermissibly relied on a memorandum that had been the subject of prior litigation by the plaintiff. See id.; see also Louis v. Labor, No. C99-5195, slip op. at 1-2 (W.D. Wash. Oct. 15, 1999), aff’d in part, rev’d in part & remanded, Louis v. Labor, 19 F. App’x 487 (9th Cir. 2001); Louis v. Labor, No. C97-5521 (W.D. Wash. Feb. 27, 1998) (magistrate’s recommendation), adopted, (W.D. Wash. Mar. 23, 1998); Louis v. VA, No. C95-5606 (W.D. Wash. Oct. 31, 1996). Yet, the district court in a prior action had ordered that the agency “destroy all but one known copy of the document” and that it “maintain that single copy in a sealed envelope to be revealed to no person, agency, or entity.” Louis v. Labor, No. C97-5521, slip op. at 3 (W.D. Wash. Feb. 27, 1998). The Ninth Circuit ruled that the Department of Labor violated the Privacy Act when it failed “to maintain its records in such a way as to indicate to the claims examiner that it could not rely on [that memorandum] in reviewing Louis’ request for reconsideration.” 19 F. App’x at 489. The court stated that the agency’s “disregard of both the district court’s prior decision rendering reliance on [the memorandum] impermissible and its own assurance that it

would annotate the memo in its files ‘to reflect that it is not to be considered in any future action related to Dr. Louis’ claim’ constitutes a willful failure on the part of the government to abide by its obligations, and proximately resulted in the government’s refusal to reconsider its earlier decision, thereby adversely affecting [plaintiff].” Id.

In Wilborn, an attorney who had been employed by the Department of Health and Human Services sought Privacy Act damages for an Administrative Law Judge’s disclosure of adverse personnel information about him in an opinion 49 F.3d at 599-602. The court ruled that the “uncontroverted facts plainly establish that the ALJ disclosed the information . . . without any ground for believing it to be lawful and in flagrant disregard of the rights of Wilborn under the Privacy Act.” Id. at 602. The Ninth Circuit noted that not only was the ALJ personally familiar with the Privacy Act and had advised his staff concerning the Act’s disclosure prohibition, but further, that the ALJ had been informed by an agency attorney that the language at issue was “inappropriate and should not be included in the decision.” Id. Particularly troubling in this case was the additional fact that all information pertaining to the adverse personnel record was required to be, and in fact had been, removed from the system of records by the ALJ as a result of a grievance action filed by the plaintiff. Id.

In Covert, the Ninth Circuit ruled that the Department of Energy Inspector General’s routine use disclosure of prosecutive reports, showing possible criminal fraud, to the Justice Department violated subsection (e)(3)(C) because, at the time of their original collection by another component of the agency, portions of those reports – consisting of personnel security questionnaires submitted by the plaintiffs – did not provide actual notice of the routine use. 876 F.2d 751, 754-57 (9th Cir. 1989). The Ninth Circuit held that the failure to comply with subsection (e)(3)(C) was “greater than grossly negligent” even though the Inspector General was relying on statutes, regulations, and disclosure practices that appeared to permit disclosure, and no prior court had ever suggested that noncompliance with subsection (e)(3)(C) would render a subsequent subsection (b)(3) routine use disclosure improper. Compare id. at 756-57, with Chapman, 736 F.2d at 243, Wisdom, 713 F.2d at 424-25, and Bruce, 621 F.2d at 917.

The D.C. Circuit has found that plaintiffs submitted sufficient evidence to establish that complaint alleging “willful or intentional” data breach could proceed.

The Court of Appeals for the District of Columbia Circuit has not gone as far as the Sixth and Ninth Circuits in finding an “intentional or willful”

violation of the statute. It did find, however, that the plaintiff had submitted sufficient evidence that a motion to dismiss was not appropriate. See In re OPM Data Security Breach, 928 F.3d 42, 63–64 (D.C. Cir. 2019) (finding Plaintiff’s complaint “clears that hurdle by plausibly and with specificity alleging that OPM was willfully indifferent to the risk that acutely sensitive private information was at substantial risk of being hacked”); Toolasprashad v. BOP, 286 F.3d 576, 584 (D.C. Cir. 2002) (remanding case where district court had found that record would not support finding of intentional and willful action, and stating that, “[i]f proven, retaliatory fabrication of prison records would certainly meet [our] definition [as articulated in Deters] of a willful or intentional Privacy Act violation”).

Although only a few courts have addressed the issue, they have split over whether the Privacy Act limits recovery of damages under state law or the Federal Tort Claims Act for negligent disclosure.

The Court of Appeals for the Third Circuit has held that the Privacy Act – with its stringent “greater than gross negligence” standard for liability – does not indicate a congressional intent to limit an individual’s right under state law to recover damages caused by the merely negligent disclosure of a psychiatric report. See O’Donnell v. United States, 891 F.2d 1079, 1083-87 (3d Cir. 1989) (Federal Tort Claims Act (“FTCA” case). But see Hager v. United States, No. 86-3555, slip op. at 7-8 (N.D. Ohio Oct. 20, 1987) (finding Privacy Act preempts FTCA action alleging wrongful disclosure); cf. Doe v. DiGenova, 642 F. Supp. 624, 629-30, 632 (D.D.C. 1986) (holding state law/FTCA claim preempted by Veterans’ Records Statute, 38 U.S.C. §§ 3301-3302 (renumbered as 38 U.S.C. §§ 5701-5702 (2018))), aff’d in pertinent part, rev’d in part & remanded sub nom. Doe v. Stephens, 851 F.2d 1457 (D.C. Cir. 1988).

2. Actual Damages

“In any suit brought under the provisions of subsection (g)(1)(C) or (D) . . . in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual [for] actual damages sustained by the individual . . . but in no case shall a person entitled to recovery receive less than the sum of \$1,000.” 5 U.S.C. § 552a(g)(4)(A).

Comment:

The Supreme Court has held that plaintiffs must show actual damages to be “entitled to recovery” of the \$1,000 minimum.

In issuing its first purely Privacy Act decision in the history of the Act, the Supreme Court considered a decision by the Court of Appeals for the Fourth Circuit in which a divided panel held that in order to be entitled to a statutory minimum damages award for violation of the Privacy Act, a complainant must prove actual damages. Doe v. Chao, 540 U.S. 614 (2004), aff’d Doe v. Chao, 306 F.3d 170, 177-79 (4th Cir. 2002). Recognizing that the Fourth Circuit’s opinion in Doe v. Chao “conflicted with the views of other Circuits,” the Supreme Court granted certiorari. 540 U.S. at 618 (citing Orekoya v. Mooney, 330 F.3d 1, 7-8 (1st Cir. 2003); Wilborn v. HHS, 49 F.3d 597, 603 (9th Cir. 1995); Waters v. Thornburgh, 888 F.2d 870, 872 (D.C. Cir. 1989); Johnson v. IRS, 700 F.2d 971, 977, and n.12 (5th Cir. 1983); Fitzpatrick v. IRS, 665 F.2d 327, 330-31 (11th Cir. 1982) (awarding statutory minimum \$1,000 damages, but denying recovery beyond the statutory minimum because “appellant proved only that he suffered a general mental injury”). The majority conducted “a straightforward textual analysis,” looked to the Privacy Act’s legislative history, and ultimately, in a 6 to 3 decision, concluded that the Fourth Circuit’s view was correct. Id. at 620-29. The Court held that to meet the “entitle[ment] to recovery” language of subsection (g)(4)(A) to qualify for the \$1,000 minimum, showing “merely . . . an intentional or willful violation of the Act producing some adverse effect” is insufficient; “[the statute guarantees \$1,000 only to plaintiffs who have suffered some actual damages.” Id. at 627; deLeon v. Wilkie, No. CV 19-1250 (JEB), 2020 WL 210089, at *8 (D.D.C. Jan. 14, 2020) (finding plaintiff did not suffer actual damages where his complaint was “devoid of allegations that either incident — *i.e.*, the disclosure of his personnel records or of his pending disciplinary action — caused him to suffer any actual damages”); Clutter v. Perdue, No. H-18-310, 2019 WL 1589942, at *8 (S.D. Tex. Jan. 28, 2019) (dismissing subsection (g)(1)(D) claim for failure to plead in detail actual damages from unspecified Privacy Act violation); Taylor v. FAA, 351 F. Supp. 3d 97, 105-06 (D.D.C. 2018) (finding that because plaintiff’s complaint “made no allegation whatsoever of pecuniary or economic harm caused by the alleged Privacy Act violation, the court is foreclosed from granting the \$1,000 statutory award he seeks”); Otero v. DOJ, 292 F. Supp. 3d 245, 253-54 (D.D.C. 2018), aff’d sub nom. Otero v. DOJ, No. 18-5080, 2019 WL 4565497 (D.C. Cir. Sept. 4, 2019) (granting agency summary judgment where court “identifies no support for an award of damages – actual or otherwise – arising from a purported violation of the Privacy Act”);

Chichackli v. Kerry, 203 F. Supp. 3d 48, 57-58 (D.D.C. 2016) (dismissing Privacy Act claim, in part, by finding plaintiff failed to demonstrate “concrete and quantifiable damages” when pleading that several fraudulent bank accounts were established in his name, fraudulent income tax returns were filed under his social security number, and credit cards were issued using his personal information where actual sum of damages was “still undiscovered” and damages were “in an amount unknown at this time”); Welborn v. IRS, 218 F. Supp. 3d 64, 82-83 (D.D.C. 2016) (dismissing Privacy Act damages claim due to failure to plead actual damages where plaintiff class alleged false tax returns were filed, future e-filing of taxes was prohibited, lost time was spent dealing with ramifications of fraud, and there was heightened risk of further identity theft); Pinkney v. VA, No. 1:07-CV-00142, 2008 WL 4272749, at *5-6 (S.D. Ohio Sept. 11, 2008) (stating that “the Supreme Court in Doe v. Chao carefully reviewed the statutory language and legislative history and held that the minimum guarantee goes only to victims who prove some actual damages”). As a result, the court abrogated any prior case law that suggests that anything less than actual damages is sufficient to entitle an individual to an award of the statutory minimum \$1,000 damages.

The District of Columbia Circuit Court of Appeals has considered in detail whether plaintiff’s incurred costs constitute “actual damages.” The Court of Appeals, in In re OPM Data Sec. Breach Litig., reversed the district court’s decision dismissing a case involving a data breach that resulted in the disclosure of the sensitive information of more than 20 million government employees. 928 F.3d 42 (D.C. Cir. 2019). The court concluded that numerous expenses that plaintiffs had alleged in its complaint incurred as a result of the breach constituted actual damages, including legal fees to close fraudulent accounts, unauthorized charges on a utility bill, credit protection and/or credit repair services, new credit card accounts fraudulently opened in plaintiffs’ names, loans taken out in plaintiffs’ names that became delinquent, false tax returns filed using plaintiffs’ information that led to delays in receiving federal and state tax refunds and the forgone time value of that money, and the time plaintiffs’ took off work to resolve the fraudulent tax return filing and to close a fraudulently opened account. Id. at 64-66. Thus, the court determined that the plaintiffs adequately alleged actual damages.

After years of differing opinions in the circuits, in 2004, the United States Supreme Court limited “actual damages” to pecuniary or monetary damages, abrogating earlier cases that had found to the contrary.

Although Doe v. Chao settled the issue of whether actual damages are required to recover either the statutory minimum or damages beyond the minimum, and that actual damages include out-of-pocket expenses, the Supreme Court did not rule explicitly on the issue of whether nonpecuniary damages for mental injury – such as emotional trauma, anger, fear, or fright – satisfy the definition of actual damages. Doe v. Chao, 540 U.S. at 627 n.12 (noting division among Courts of Appeals on “the precise definition of actual damages,” and stating “[t]hat issue is not before us, however”). Until the Supreme Court answered this question eight years later in FAA v. Cooper, 566 U.S. 284 (2012), discussed below, lower courts were divided on the issue. Compare, e.g., Jacobs v. Nat’l Drug Intelligence Ctr., 548 F.3d 375, 378 (5th Cir. 2008), Johnson v. IRS, 700 F.2d at 974-80 (finding nonpecuniary damages recoverable), and Parks v. IRS, 618 F.2d 677, 682-83, 685 (10th Cir. 1980) (stating that plaintiffs had “alleged viable claims for damages” where only alleged adverse effect was “psychological harm”), with Fanin v. VA, 572 F.3d 868, 872 (11th Cir. 2009) (following Fitzpatrick in requiring pecuniary losses), cert. denied sub nom. Perkins v. VA, 130 S. Ct. 1755 (2010), Hudson v. Reno, 130 F.3d 1193, 1207 n.11 (6th Cir. 1997) (citing plaintiff’s failure to show “actual damages” as additional basis for affirming district court decision and stating that “the weight of authority suggests that actual damages under the Privacy Act do not include recovery for ‘mental injuries, loss of reputation, embarrassment or other non-quantifiable injuries’” (citing Fitzpatrick)), DiMura v. FBI, 823 F. Supp. 45, 47-48 (D. Mass. 1993) (finding that “‘actual damages’ does not include emotional damages”). See generally Doe v. Chao, 306 F.3d at 181-82 (finding that plaintiff had “utterly failed to produce evidence sufficient to permit a rational trier of fact to conclude that he suffered any ‘actual damages,’” and thus stating that “we need not reach the issue of whether the term ‘actual damages’ as used in the Act encompasses damages for non-pecuniary emotional distress” where plaintiff “did not produce any evidence of tangible consequences stemming from his alleged angst over the disclosure of his [social security number]” to corroborate his “conclusory allegations” of emotional distress); id. at 198 n.13 (Michael, J., dissenting) (stating that “the majority’s holding commits this circuit to the position that the term ‘actual damages’ includes at least emotional distress that would qualify as ‘demonstrable’ under [Price v. City of Charlotte, 93 F.3d 1241 (4th Cir. 1996)]”).

In Cooper, the Supreme Court settled this confusion by interpreting actual damages to be “limited to proven pecuniary or economic harm.” 566 U.S. at 299. The plaintiff in Cooper had alleged that the agency’s “unlawful disclosure . . . of his confidential medical information, including his HIV status, had caused him ‘humiliation, embarrassment, mental anguish, fear of social ostracism, and other severe emotional distress,’” but he “did not allege any pecuniary or economic loss.” Id. at 289. In framing the issue, the Court stated: “Because respondent seeks to recover monetary compensation from the Government for mental and emotional harm, we must decide whether the civil remedies provision of the Privacy Act waives the Government’s sovereign immunity with respect to such a recovery.” Id. at 291. The Court explained that any ambiguities in the scope of the waiver must be construed “in favor of the sovereign.” Id. In reaching its conclusion, the Court first observed that “‘actual damages’ is a legal term of art” that has a “chameleon-like quality” because its “precise meaning . . . ‘changes with the specific statute in which it is found.’” Id. at 289-290. The Court also picked up on its observation in Doe v. Chao, see 540 U.S. at 625-26, that the civil remedies provision “‘parallels’ the remedial scheme for the common-law torts of libel per quod and slander, under which plaintiffs can recover ‘general damages’” – which “cover ‘loss of reputation, shame, mortification, injury to the feelings and the like and need not be alleged in detail and require no proof’” – “but only if they prove ‘special harm’ (also known as ‘special damages’)” – which “are limited to actual pecuniary loss, which must be specially pleaded and proved.” Cooper, 566 U.S., at 295. “This parallel,” the Court reasoned, “suggests the possibility that Congress intended the term ‘actual damages’ in the Act to mean special damages. The basic idea is that Privacy Act victims, like victims of libel per quod or slander, are barred from any recovery unless they can first show actual – that is, pecuniary or material – harm.” Id. at 296. Finally, the Court placed considerable emphasis on the fact that the Privacy Protection Study Commission (discussed above under “Introduction, Privacy Protection Study Commission”), which Congress established “to consider, among its other jobs, ‘whether the Federal Government should be liable for general damages,’” recommended that general damages be allowed; however, Congress “never amended the Act to include them.” Id. at 297. After Cooper, any prior case law suggesting that actual damages are not limited to proven pecuniary or economic harm has been abrogated. See also Cause v. DOD, 676 F. App’x 316, 318 (5th Cir. 2017) (concluding that plaintiff did not allege actual damages because “mental and emotional distress . . . do not meet the Supreme Court’s definition of actual damages under the Privacy Act” and plaintiff did not provide sufficient factual enhancement to establish “‘lost or jeopardized present or future financial opportunities,’” or

“how the disclosure of his records has caused their loss”); Freeman v. Fed. Bureau of Prisons, No. 19-CV-02569 (CKK), 2020 WL 4673412, at *4 (D.D.C. Aug. 12, 2020) (internal citations omitted) (finding plaintiff’s assertion that “improper disclosure has ‘caused and continue[s] to cause [him] to suffer and sustain intentional infliction of emotional distress’ insufficient in damages suit” because “Privacy Act does not allow a claim for damages based on . . . emotional harm”); Martinez v. Stackley, No. CV 16-00475 HG-RLP, 2018 WL 1093810, at *13 (D. Haw. Feb. 28, 2018), aff’d sub nom. Martinez v. Spencer, 771 F. App’x 403 (9th Cir. 2019) (indicating that damages under Privacy Act is “limited to proven pecuniary or economic harm”); Gonzalez v. Agriculture, No. 17-24171-CIV, 2018 WL 5071395, at *7 (S.D. Fla. Aug. 29, 2018) (dismissing plaintiff’s complaint because plaintiff did not show “that his removal from [the union] caused him to suffer actual damages”); Richardson v. Bd. of Governors of Fed. Reserve Sys., 288 F. Supp. 3d 231, 236–37 (D.D.C. 2018), aff’d, No. 18-5063, 2018 WL 4103305 (D.C. Cir. Aug. 15, 2018) (concluding that because plaintiff’s “allegations of harm rely on claims of emotional harm and other non-pecuniary alleged damages” they were insufficient to state a claim under the Privacy Act); Glass v. DOJ, 279 F. Supp. 3d 279, 281 (D.D.C. 2017), aff’d sub nom. Glass v. DOJ, No. 18-5030, 2018 WL 5115524 (D.C. Cir. Sept. 19, 2018) (concluding that plaintiff’s “vague description of the harms allegedly sustained as a result of Defendant’s disclosure cannot support a demand for actual damages that must be ‘limited to *proven* pecuniary or economic harm’”); Palmieri v. United States, 72 F. Supp. 3d 191, 213 (D.D.C. 2014), aff’d, 896 F.3d 579 (D.C. Cir. 2018) (noting that “[a]lthough gossip may cause an adverse effect, it does not constitute actual damages”); Cause, 676 F. App’x at 318 (concluding that “mental and emotional distress plaintiff alleges he suffered do not meet the Supreme Court’s definition of actual damages under the Privacy Act”); Patwardhan v. United States, No. 13-0076, 2014 U.S. Dist. LEXIS 36226, at *31 (C.D. Cal. Mar. 18, 2014) (finding profit and loss statements from consecutive years to be mere speculation that does not show actual damages); Makowski v. United States, 27 F. Supp. 3d 901, 914 (N.D. Ill. 2014) (finding it “reasonable to infer that the seventy days of unnecessary incarceration cost [plaintiff] prospective employment opportunities,” and that “[l]oss of economic opportunity is pecuniary harm”); Corbett v. TSA, 968 F. Supp. 2d 1171, 1188 (S.D. Fla. 2012) (dismissing plaintiff’s Privacy Act claims because he “alleges no actual damages separate and apart from the statutory violations themselves . . . [and] are thus insufficient to entitle him to any monetary award”); Grant v. United States, No. 2:11-cv-00360, 2012 WL 5289309, at *8 (E.D. Cal. Oct. 23, 2012) (finding plaintiff’s claim for \$5 million in general damages “as a result of ‘mental distress, emotional trauma, embarrassment, humiliation, grief,

anxiety, worry, mortification, show indignity, and ordeal” not cognizable under the Privacy Act under Cooper (citing Cooper, 132 S. Ct. at 1446, 1451-53, 1456).

Prior to Doe v. Chao and Cooper, the issue of what needs to be shown in order to recover damages under subsection (g)(4)(A) had historically engendered some inconsistent and confusing case law. See, e.g., Orekoya v. Mooney, 330 F.3d 1, 7-8 (1st Cir. 2003) (holding that “statutory damages [of \$1,000], if not actual damages, are available to individuals who suffer adverse effects from intentional and willful violations of the [Privacy Act] and that provable emotional distress may constitute an adverse effect”); Wilborn v. HHS, 49 F.3d 597, 603 (9th Cir. 1995) (finding no need to remand to district court for determination of amount of damages because plaintiff had limited damages sought to statutory minimum); Quinn v. Stone, 978 F.2d 126, 135 (3d Cir. 1992) (stating that subsection (g)(1)(D) “gives an individual adversely affected by any agency violation of the Act a judicial remedy whereby the individual may seek damages”); Waters v. Thornburg, 888 F.2d 870, 872 (D.C. Cir. 1989) (stating that to obtain relief under the Privacy Act plaintiff must establish that (1) the agency violated a provision of the Act; “(2) the violation of the Act was ‘intentional or willful,’” and “(3) this action had an ‘adverse effect’ on the plaintiff” and that “[i]f these three factors are satisfied, the plaintiff is entitled to the greater of \$1,000 or the actual damages sustained”); Johnson v. IRS, 700 F.2d 971, 977 & n.12, 986 (5th Cir. 1983) (recognizing entitlement to statutory minimum for proven physical and mental injuries even if “actual damages” were interpreted to include only pecuniary harm, but going on to hold that “actual damages” includes “proven mental and physical injuries”); Fitzpatrick v. IRS, 665 F.2d 327, 329-31 (11th Cir. 1982) (awarding statutory minimum \$1,000 damages, but denying recovery beyond the statutory minimum because “appellant proved only that he suffered a general mental injury”). See generally OMB Guidelines, 40 Fed. Reg. 28,948, at 28,970, https://www.justice.gov/paover/view_omb-75 (stating that “[a]ctual damages or \$1,000, whichever is greater,” are recoverable (emphasis added)).

3. Limits on Injunctive Relief for Damages Claims

Unlike amendment and access claims under subsections (g)(1)(A) and (g)(1)(B), injunctive relief is not available in damages claims under subsections (g)(1)(C) or (g)(1)(D).

It is well settled that injunctive relief as provided for in the Privacy Act is available only under subsections (g)(1)(A) (amendment) and (g)(1)(B)

(access) – both of which, incidentally, require exhaustion – and that injunctive relief is not available under subsections (g)(1)(C) or (g)(1)(D). See, e.g., Doe v. Chao, 540 U.S. at 635 (Ginsburg, J., dissenting); McLeod v. VA, 43 F. App'x 70, 71 (9th Cir. 2002) (quoting Cell Assocs. v. NIH, infra); Locklear v. Holland, No. 98-6407, 1999 WL 1000835, at *1 (6th Cir. Oct. 28, 1999); Risley v. Hawk, 108 F.3d 1396, 1397 (D.C. Cir. 1997) (per curiam); Doe v. Stephens, 851 F.2d at 1463; Hastings v. Judicial Conference of the United States, 770 F.2d 1093, 1104 (D.C. Cir. 1985); Edison, 672 F.2d at 846; Hanley v. DOJ, 623 F.2d 1138, 1139 (6th Cir. 1980) (per curiam); Parks, 618 F.2d at 684; Cell Assocs. v. NIH, 579 F.2d 1155, 1161-62 (9th Cir. 1978); Halliburton v. Labor, No. 17-CV-01045-MJW, 2018 WL 1256509, at *3 (D. Colo. Mar. 12, 2018) (dismissing 5 U.S.C. § 552a(g)(1)(D) claim where only a failure to produce disputed records was pleaded which is remedied solely by injunctive relief under 5 U.S.C. § 552a(g)(1)(B)); Makowski v. United States, 27 F. Supp. 3d 901, 915 (N.D. Ill. 2014); Kursar v. TSA, 581 F. Supp. 2d 7, 19 (D.D.C. 2008), aff'd per curiam, on other grounds, 442 F. App'x 565 (D.C. Cir. 2011); Tarullo v. Def. Contract Audit Agency, 600 F. Supp. 2d 352, 358 (D. Conn. 2009); AFGE v. HUD, 924 F. Supp. 225, 228 n.7 (D.D.C. 1996), rev'd on other grounds, 118 F.3d 786 (D.C. Cir. 1997); Houston, 494 F. Supp. at 29; see also Word v. United States, 604 F.2d 1127, 1130 (8th Cir. 1979) (no “exclusionary rule” for subsection (b) violations; “No need and no authority exists to design or grant a remedy exceeding that established in the statutory scheme.”); Shields v. Shetler, 682 F. Supp. 1172, 1176 (D. Colo. 1988) (Act “does not create a private right of action to enjoin agency disclosures”); 120 Cong. Rec. at 40,406, reprinted in Source Book at 862, https://www.justice.gov/opcl/paoverview_sourcebook; cf. New-Howard v. Shinseki, No. 09-5350, 2012 WL 2362546, at *8 (E.D. Pa. June 21, 2012) (“To the extent that Plaintiff seeks to enjoin Defendant from using the allegedly altered records in the course of further litigation, the statute in question does not authorize the relief requested.”). But see Fla. Med. Ass'n v. HEW, 479 F. Supp. 1291, 1299 & n.8 (M.D. Fla. 1979) construing subsection (g)(1)(D) to confer jurisdiction to enjoin agency’s disclosure of Privacy Act-protected record. However, courts have recognized the availability of equitable relief under the Administrative Procedure Act for claims governed by the Privacy Act (see the discussion above under “Civil Remedies”).

Given the well-settled law that injunctive relief is not available for Privacy Act damages claims, it would seem clear that injunctive relief is not available for any damages claim, but the D.C. Circuit has suggested that there may be an exception for subsection (e)(7) damages claims. In Haase v. Sessions, 893 F.2d 370, 373-75 (D.C. Cir. 1990), the D.C. Circuit, in dictum, suggested that its decision in Nagel v. HEW, 725 F.2d 1438, 1441 (D.C. Cir.

1984), could be read to recognize the availability of injunctive relief to remedy a subsection (e)(7) violation, under subsection (g)(1)(D); see also Becker v. IRS, 34 F.3d 398, 409 (7th Cir. 1994) (finding that the IRS had not justified maintenance of documents under subsection (e)(7), and stating that “the documents should be expunged”); Scott v. Conley, 937 F. Supp. 2d 60, 81-82 (D.D.C. 2013) (dismissing plaintiff’s subsection (e)(7) claim on other grounds, but stating “[a]lthough the Circuit did not explicitly decide the question in Haase, its language suggests that injunctive relief for (e)(7) violations under (g)(1)(D) would be available”); but see Wabun-Inini v. Sessions, 900 F.2d 1234, 1245 (8th Cir. 1990); Clarkson v. IRS, 678 F.2d 1368, 1375 n.11 (11th Cir. 1982); Comm. in Solidarity v. Sessions, 738 F. Supp. 544, 548 (D.D.C. 1990), aff’d, 929 F.2d 742 (D.C. Cir. 1991); see also Socialist Workers Party v. Attorney Gen., 642 F. Supp. 1357, 1431 (S.D.N.Y. 1986) (in absence of exhaustion, only damages remedy, rather than injunctive relief, is available for violation of subsection (e)(7)). The D.C. Circuit’s view in Haase is somewhat difficult to reconcile with the structure of subsection (g) and with the case law mentioned above.

4. Additional Considerations for Damages Claims

Plaintiffs are not entitled to the minimum recovery for each individual copy of a document that is disclosed.

The Court of Appeals for the District of Columbia Circuit has ruled that a plaintiff was not entitled to \$1,000 for each copy of a letter that was disclosed in violation of the Privacy Act to 4500 individuals. See Tomasello v. Rubin, 167 F.3d 612, 617-18 (D.C. Cir. 1999). The D.C. Circuit stated that “[w]hile it may be linguistically possible to read the language [of § 552a(g)(4)] so as to forbid the aggregation of several more-or-less contemporaneous transmissions of the same record into one ‘act[]’ or ‘failure [to comply with the Privacy Act],’ the result [sought in this case] shows that such a reading defies common sense.” Id. at 618. In reaching its determination “that each letter disclosure was not independently compensable,” the D.C. Circuit also reasoned that as a waiver of sovereign immunity, subsection (g)(4) “must be construed strictly in favor of the sovereign, and not enlarge[d] . . . beyond what the language requires.” Id. (quoting United States v. Nordic Vill., Inc., 503 U.S. 30, 34 (1992)); cf. Siddiqui v. United States, 359 F.3d 1200, 1201-03 (9th Cir. 2004) (finding that disclosure of tax information by IRS agent to 100 people in one room at one time constituted one act of disclosure for purposes of determining statutory damages under Internal Revenue Code).

One court has allowed a plaintiff to recover mitigation costs for certain Privacy Act claims.

One district court has applied the doctrine of mitigation to certain Privacy Act claims, holding that “an individual whose information is disclosed in violation of the Privacy Act may recover for costs incurred to prevent harm from that disclosure.” Beaven v. DOJ, No. 03-84, 2007 WL 1032301, at *8 (E.D. Ky. Mar. 30, 2007) (concluding that “plaintiffs’ out-of-pocket expenses [incurred in monitoring their financial information] to protect themselves from potential harm were caused by the instant Privacy Act violation”), aff’d in part, rev’d in part & remanded, on other grounds, 622 F. 3d 540 (6th Cir. 2010).

There is a circuit court split as to whether an individual can file a damages action when an agency destroys a Privacy Act record.

There is a split of authority on the issue of whether destruction of a Privacy Act record gives rise to a damages action. Compare Tufts v. Air Force, 793 F.2d 259, 261-62 (10th Cir. 1986), with Rosen v. Walters, 719 F.2d 1422, 1424 (9th Cir. 1983), and Waldrop v. Air Force, 3 Gov’t Disclosure Serv. (P-H) ¶ 83,016, at 83,453 (S.D. Ill. Aug. 5, 1981). See also Vaughn v. Danzig, 18 F. App’x 122, 124-25 (4th Cir. 2001) (per curiam) (finding no Privacy Act violation where record of nonjudicial punishment was maintained in files of plaintiff’s military unit at time of his discharge, but later was destroyed pursuant to records retention policy; “Although [plaintiff] seems to argue that the Privacy Act requires that records be maintained in perpetuity, he has cited no authority for that proposition”; “[A]gencies are not required to retain records on the possibility that a . . . Privacy Act request may be submitted.”); Dowd v. IRS, 776 F.2d 1083, 1084 (2d Cir. 1985) (per curiam) (declining to decide issue). Cf. Beaven, 2007 WL 1032301, at *16-17 (applying adverse inference because agency “destroyed the [records] intentionally and in bad faith” and concluding that “[t]he inference is conclusive as to disclosure, and the defendants’ conduct therefore constitutes a violation of the Privacy Act”), aff’d, 622 F. 3d 540.

F. Principles Applicable to All Privacy Act Civil Actions

The Privacy Act does not provide relief from federal criminal prosecution, cannot be used to collaterally attack a conviction or sentence, and is not a defense to a summons.

Several courts have stated that the civil remedies provided in the Privacy Act do not provide for any relief in the course of a federal criminal prosecution. See,

e.g., Heck v. Humphrey, 512 U.S. 477, 486-87 (1994) (finding that claims for unlawful actions that would render convictions or sentences invalid are precluded unless there has been reversal on direct appeal, expungement, invalidation, or issuance writ of habeas corpus); United States v. Bressler, 772 F.2d 287, 293 (7th Cir. 1985) (“[E]ven if the defendant had made a sustainable argument [under 5 U.S.C. § 552a(e)(3)], the proper remedy is a civil action under Section 552a(g)(1) of the Privacy Act, not dismissal of the indictment.”); United States v. Bell, 734 F.2d 1315, 1318 (8th Cir. 1984) (asserting that even if appellant’s (e)(3) argument was sufficiently raised at trial, “it cannot be a basis for reversing his conviction”); United States v. Gillotti, 822 F. Supp. 984, 989 (W.D.N.Y. 1993) (“[T]he appropriate relief for a violation of Section 552a(e)(7) is found in the statute and allows for damages as well as amendment or expungement of the unlawful records. . . . [T]here is nothing in the statute itself, nor in any judicial authority, which suggests that its violation may provide any form of relief in a federal criminal prosecution.”); cf. United States v. Moreno-Nevarez, No. 13-CR-0841, 2013 U.S. Dist. LEXIS 143900, at *10-14 (S.D. Cal. Oct. 2, 2013) (finding that “[r]egardless of the merits of Defendant’s contentions regarding possible violations of the Privacy Act, he has not presented grounds for suppressing the information in his criminal case” and “[t]he Privacy Act explicitly creates remedies for individuals harmed by violations of the statute”).

A plaintiff cannot use the Privacy Act to challenge a conviction or sentence. See Skinner v. DOJ & BOP, 584 F.3d 1093, 1101 (D.C. Cir. 2009) (affirming dismissal of damages claim under Privacy Act because claim is not cognizable unless plaintiff first secures relief through writ of habeas corpus); Leventhal v. Rios, No. 0:17-CV-05441, 2018 WL 3130682, at *3 (D. Minn. May 16, 2018) (indicating Privacy Act claim not cognizable under 28 U.S.C. § 2241 writ of habeas corpus petition); Hill v. Smoot, 308 F. Supp. 3d 14, 22 (D.D.C. 2018) (“‘absent a showing that the plaintiff’s conviction or sentence has been invalidated, . . . the plaintiff cannot recover damages’ for the alleged one-month he spent in custody following his arrest for a parole violation” (quoting Johnson v. United States, 590 F. Supp. 2d 101, 108–09 (D.D.C. 2008))); Semrau v. ICE, No. 5:13-cv-188, 2014 WL 4626708, at *5-*6 (S.D. Miss. Sept. 12, 2014) (finding claim that agency failed to maintain accurate records about plaintiff to extent that they supported his guilty verdict and deportation was collateral attack on verdict and barred by law).

Several courts also have found that failure to comply with the Privacy Act is not a proper defense to certain enforcement summons, such as a summons issued by the Internal Revenue Service (IRS). See, e.g., United States v. McAnlis, 721 F.2d 334, 337 (11th Cir. 1983) (holding that compliance with 5 U.S.C. § 552a(e)(3) is not prerequisite to enforcement of an IRS summons); United States v. Berney, 713

F.2d 568, 572 (10th Cir. 1983) (stating that Privacy Act “contains its own remedies for noncompliance”); United States v. Harris, 172 F.3d 54, at *2 (7th Cir. 1998) (unpublished table decision) (citing McAnlis and Berney and rejecting “irrelevant argument that . . . the Privacy Act . . . guarantee[s] [appellant] answers to his questions before he has to comply with the IRS summons”); Reimer v. United States, 43 F. Supp. 2d 232, 237 (N.D.N.Y. 1999) (rejecting argument to quash summons because, inter alia, “the disclosure requirements in 5 U.S.C. § 552a(e)(3) are not applicable to summons issued pursuant to 26 U.S.C. §§ 7602, 7609”); see also Phillips v. United States, 178 F.3d 1295, at *2 (6th Cir. 1999) (unpublished table decision) (holding Privacy Act notice requirements inapplicable to issuance of IRS summons, as 26 U.S.C. § 7852(e) “plainly states that the provisions of the Privacy Act do not apply, directly or indirectly, to assessing the possibility of a tax liability”); cf. Huene v. Treasury, No. 11-2110, 2012 WL 3027815, at *1 (E.D. Cal. July 24, 2012) (finding court “lacks jurisdiction over plaintiff’s claim on the basis of 26 U.S.C. § 7852(e), which renders certain provisions of the Privacy Act inapplicable to the determination of the existence of tax-related liability”); Estate of Myers v. United States, 842 F. Supp. 1297, 1300-02 (E.D. Wash. 1993) (recognizing applicability of subsection (e)(3) to IRS summons, and possibility “that a summons may be judicially enforceable yet not meet the disclosure requirements of the Privacy Act”).

Mandamus relief is not an appropriate remedy for a Privacy Act violation.

“Because the Privacy Act provides its own remedy for an agency’s improper refusal to process a proper request for information, [plaintiff] is not entitled to mandamus relief.” Kotmair v. Netsch, No. 93-490, 1993 U.S. Dist. LEXIS 10781, at *5 (D. Md. July 21, 1993); see also Harris v. BOP, No. 13-1144, 2013 U.S. Dist. LEXIS 106619, at *1 (D.D.C. July 23, 2013) (“Judicial review of an agency’s failure to amend records is available exclusively under the Privacy Act.”); Christian v. Army, No. 11-0276, 2011 WL 345945, at *1 (D.D.C. Jan. 31, 2011) (rejecting plaintiff’s attempt “to correct his military records via a writ of mandamus” on ground that Privacy Act “provides an adequate remedy for addressing plaintiff’s claims”); Carrick v. Spencer, No. 3:02MC95-V, 2003 U.S. Dist. LEXIS 11706, at *3-4 (W.D.N.C. June 6, 2003) (magistrate’s recommendation) (denying petition for writ of mandamus as “the Privacy Act establishes a procedure for filing suit in federal court if an agency refuses to comply with a request” and petitioner has not “shown, or attempted to show, that this procedure is inadequate to obtain the relief requested”), adopted, 2003 U.S. Dist. LEXIS 17189 (W.D.N.C. Sept. 2, 2003); cf. Graham v. Hawk, 857 F. Supp. 38, 41 (W.D. Tenn. 1994) (“[R]emedies under the Privacy Act [for alleged inaccuracy] preclude plaintiff’s entitlement to mandamus, even though his claim under that act is substantively meritless.”), aff’d, 59 F.3d 170 (6th Cir. 1995) (unpublished table decision).

The Privacy Act does not preclude individuals from seeking remedies under the Federal Tort Claims Act.

On the other hand, the United States Court of Appeals for the Third Circuit considered civil remedies for Privacy Act violations under the Federal Tort Claims Act (“FTCA”) and held that the Privacy Act “does not limit the remedial rights of persons to pursue whatever remedies they may have” under the FTCA for privacy violations consisting of record disclosures. O’Donnell v. United States, 891 F.2d 1079, 1084-85 (3d Cir. 1989); see also Stephens v. United States, No. 0:16-149-BHH-PJG, 2016 WL 11200987, at *2-3 (D.S.C. Dec. 9, 2016) (magistrate’s recommendation) (following O’Donnell), adopted in pertinent part & rev’d in other part (D.S.C. Jan. 19, 2017); Rosado-Montes v. United States, 8 F. Supp. 3d 55, 63 (D.P.R. 2014) (quoting O’Donnell and permitting FTCA claim against VA employees who accessed plaintiff’s medical records to proceed notwithstanding the Privacy Act); Beaven v. DOJ, No. 03-84, 2007 WL 1032301, at *21-25 (E.D. Ky. Mar. 30, 2007) (assuming jurisdiction over claims of invasion of privacy brought under FTCA and based on conduct held to violate Privacy Act, but determining that plaintiffs failed to prove elements of those claims), aff’d in part, rev’d in part & remanded, on other grounds, 622 F.3d 540 (6th Cir. 2010); cf. Alexander v. FBI, 691 F. Supp. 2d 182 (D.D.C. 2010) (implicitly recognizing that local or state common law tort and FTCA are alternative causes of action to Privacy Act, but finding that plaintiffs had not met specific requirements to prevail on those causes of action), aff’d on other grounds, 456 F. App’x 1 (D.C. Cir. 2011).

Alleged violations of the Privacy Act, however, cannot be the sole basis of a FTCA claim. Coleman v. United States, 912 F.3d 824, 835-36 (5th Cir. 2019); Burroughs v. Abrahamson, 964 F. Supp. 2d 1268, 1272 (D. Or. 2013) (explaining that “[b]ecause plaintiff’s Privacy Act claim is rooted in federal rather than state law, and because Oregon has no analogous law, plaintiff cannot allege a claim under the FTCA for negligent violation of the Privacy Act”); Tripp v. United States, 257 F. Supp. 2d 37, 45 (D.D.C. 2003) (dismissing plaintiff’s claim under the FTCA for negligent disclosure of private information, as plaintiff could point to no “duty analogous to that created by the federal Privacy Act under local law to state a claim upon which relief [could] be granted”); Fort Hall Landowners Alliance, Inc. v. BIA, No. 99-052, 2001 U.S. Dist. LEXIS 27315, at *20 (D. Idaho Mar. 28, 2001) (finding that “the alleged breach of a duty not to disclose personal information” was “pre-empted by the Privacy Act”); Hager v. United States, No. 86-3555, slip op. at 7-8 (N.D. Ohio Oct. 20, 1987) (“Because the Privacy Act does have its own enforcement mechanism” for plaintiff’s claims relating to disclosure of confidential information, “it preempts the FTCA.”).

The Court of Appeals for the District of Columbia Circuit has held that the Feres doctrine, which holds that “the [g]overnment is not liable under the Federal Tort Claims Act for injuries to servicemen where the injuries arise out of or are in the course of activity incident to service,” does not apply to the Privacy Act. Cummings v. Navy, 279 F.3d 1051, 1053-58 (D.C. Cir. 2002) (quoting Feres v. United States, 340 U.S. 135, 146 (1950), and concluding that “without regard to the identity of the plaintiff or the agency she is suing, the [Privacy Act] plainly authorizes injunctive relief . . . and monetary relief,” which remains “the best evidence of congressional intent” that Feres doctrine “does not extend to Privacy Act lawsuits brought by military personnel against the military departments”); see also Chang v. Navy, No. 01-5240, 2002 WL 1461859, at *1 (D.C. Cir. July 8, 2002) (citing Cummings to vacate district court opinion that held suit barred by Feres doctrine); Colon v. United States, 320 F. Supp. 3d 733, 742 (D. Md. 2018); Gamble v. Army, 567 F. Supp. 2d 150, 155 n.9 (D.D.C. 2008) (concluding that Feres “does not extend to Privacy Act lawsuits brought by military personnel against the military departments”).

In an earlier decision, however, the Court of Appeals for the Eighth Circuit had held that the plaintiff’s Privacy Act claims were barred under the Feres doctrine. See Uhl v. Swanstrom, 79 F.3d 751, 755-56 (8th Cir. 1996); cf. Dickson v. Wojcik, 22 F. Supp. 3d 830, 839 (W.D. Mich. 2014) (citing Uhl favorably and finding that “[w]hile there are cases finding that Feres generally does not bar a Privacy Act claim, see, e.g., Cummings, the Sixth Circuit has not ruled on the question”); Walsh v. United States, No. 1:05-CV-0818, 2006 WL 1617273, at *5 (M.D. Pa. June 9, 2006) (comparing, in dicta, Uhl and Cummings and noting that “[t]here is a split of authority on whether the Feres doctrine bars Privacy Act claims”), aff’d on other grounds, 328 F. App’x 806 (3d Cir. 2009), cert. denied, 558 U.S. 996 (2009). The Cummings opinion did not reference Uhl, the only other appellate decision on this issue.

The Privacy Act’s remedies generally preclude monetary damages for constitutional violations of government officials under Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics.

Several courts have held that the Privacy Act’s remedies preclude an action seeking monetary damages directly under the Constitution from individual government officials under Bivens v. Six Unknown Named Agents of Federal Bureau of Narcotics, 403 U.S. 388 (1971). See Fazaga v. FBI, 965 F.3d 1015, 1057-1058 (9th Cir. 2020) (holding that the Privacy Act and the Religious Freedom Restoration Act “taken together, provide an alternative remedial scheme for some, but not all, of Plaintiffs’ First and Fifth Amendment Bivens claims”); Liff v. Off. of Inspector Gen. for Labor, 881 F.3d 912, 918-924 (D.C. Cir. 2018) (“The

Privacy Act represents Congress's legislative judgment about the appropriate remedies with respect to the accuracy, fairness, and use of government information, and the judicial system is not in a position to revise that scheme by recognizing an additional constitutional remedy" for claims that government officials disseminated information that harmed plaintiff's reputation); Wilson v. Libby, 535 F.3d 697, 707 (D.C. Cir. 2008) (concluding that Privacy Act's comprehensive remedial scheme precludes Bivens claim even though that scheme does not necessarily provide plaintiffs with full relief); Abuhouran v. SSA, 291 F. App'x 469, at *2 (3d Cir. Aug. 4, 2008) (per curiam) (unpublished decision); Chung v. DOJ, 333 F.3d 273, 274 (D.C. Cir. 2003) (affirming district court's dismissal of plaintiff's Bivens claims "because . . . they are encompassed within the remedial scheme of the Privacy Act"); Downie v. City of Middleburg Hts., 301 F.3d 688, 696 (6th Cir. 2002) (agreeing with district court that "because the Privacy Act is a comprehensive legislative scheme that provides a meaningful remedy for the kind of wrong [plaintiff] alleges that he suffered, we should not imply a Bivens remedy"); see also Chesser v. Chesser, 600 F. App'x 900, 901 (4th Cir. 2015) (unpublished opinion) (citing Wilson and Downie); Bloch v. Exec. Off. of the President, 164 F. Supp. 3d 841, 860 n.26 (E.D. Va. 2016); Powerturbine, Inc. v. United States, No. 3:14-cv-0435-CAB-BLM, 2014 WL 12160753, at *7-9 (S.D. Cal. Dec. 15, 2014) ("Allowing a Bivens remedy for Powerturbine here would effectively recognize a right for corporations that Congress explicitly did not give individuals in the Privacy Act – the ability to sue government employees."); Lewis v. Parole Comm'n, 770 F. Supp. 2d 246, 251-52 (D.D.C. 2011); Hurt v. D.C. Court Servs., 612 F. Supp. 2d 54, 56 (D.D.C. 2009), aff'd in pertinent part per curiam sub nom. Hurt v. Cromer, No. 09-5224, 2010 WL 604863, at *1 (D.C. Cir. Jan. 21, 2010), rev'd in part on other grounds & remanded per curiam, 2010 WL 8753255 (D.C. Cir. June 11, 2010); Sudnick v. DOD, 474 F. Supp. 2d 91, 100 (D.D.C. 2007); Hatfill v. Ashcroft, 404 F. Supp. 2d 104, 116-17 (D.D.C. 2005); Clark v. BOP, 407 F. Supp. 2d 127, 131 (D.D.C. 2005); Newmark v. Principi, 262 F. Supp. 2d 509, 518-19 (E.D. Pa. 2003); Fares v. INS, 29 F. Supp. 2d 259, 262 (W.D.N.C. 1998), aff'd per curiam, 11 F. App'x 137 (4th Cir. 2001) (unpublished decision); Sullivan v. USPS, 944 F. Supp. 191, 195-96 (W.D.N.Y. 1996); Blazy v. Woolsey, No. 93-2424, 1996 WL 43554, at *1 (D.D.C. Jan. 31, 1996), subsequent decision sub nom. Blazy v. Tenet, 979 F. Supp. 10, 27 (D.D.C. 1997), summary affirmance granted, No. 97-5330, 1998 WL 315583 (D.C. Cir. May 12, 1998); Williams v. VA, 879 F. Supp. 578, 585-87 (E.D. Va. 1995); Mittleman v. Treasury, 773 F. Supp. 442, 454 (D.D.C. 1991); cf. Royer v. BOP, No. 1:10-cv-0146, 2010 WL 4827727, at *5 (E.D. Va. Nov. 19, 2010) (stating that plaintiff's Bivens claims "may simply collapse into [his] Privacy Act claims, at least insofar as they merely repeat the allegations that the BOP has maintained inaccurate records about [his] affiliation with terrorist groups"); Patterson v. FBI, 705 F. Supp. 1033, 1045 n.16 (D.N.J. 1989) (discussing the extent to which First

Amendment claim involves damages resulting from maintenance of records; “such an action is apt to be foreclosed by the existence of the Privacy Act”), aff’d, 893 F.2d 595 (3d Cir. 1990). But see Hartley v. Wilfert, 918 F. Supp. 2d 45, 55-56 (D.D.C. 2013) (allowing plaintiff’s First Amendment claim under Bivens to move forward because “the conduct here strays so far afield from the compass of the Privacy Act that it cannot be said that Congress ever contemplated the sort of claim here being covered by the statute”; defendant’s “actions here did not involve the sort of collection of information contemplated by the Act, instead, his words were merely a threat to intimidate [plaintiff] from continuing in her speech, just as ‘I will arrest you if you continue to protest’ or ‘I will take a picture of you for my book of crazy protesters’ would deter a person from speaking”); see also Alexander, 971 F. Supp. at 610-11 (agreeing with outcome in Blazy and Mittleman, supra, but concluding that their logic does not extend to prohibit recovery under local law for torts committed by individuals who, although government employees, were acting outside scope of their employment; holding that “Privacy Act does not preempt the common law invasion of privacy tort”).

Courts have differed as to whether plaintiffs are entitled to additional remedies beyond those available under the Privacy Act, particularly where other statutes are also applicable.

The Supreme Court has addressed Administrative Procedure Act (“APA”) judicial review equitable relief issues for claims governed by the Privacy Act. See 5 U.S.C. §§ 701-706 (2018). The Court stated that “[t]he Privacy Act says nothing about standards of proof governing equitable relief that may be open to victims of adverse determinations or effects, although it may be that this inattention is explained by the general provisions for equitable relief within the [APA].” Doe v. Chao, 540 U.S. 614, 619 n.1 (2004); cf. OMB 1975 Guidelines, 40 Fed. Reg. at 28,949, https://www.justice.gov/paoverview_omb-75 (stating in its Civil Remedies section that “[a]n individual may seek judicial review under other provisions of the Administrative Procedure Act”). Indeed, under the APA, the D.C. Circuit enjoined the Veterans Administration from disclosing medical records about an individual pursuant to a routine use that “would permit routine disclosure pursuant to a grand jury subpoena,” stating the disclosure would “circumvent the mandates of the Privacy Act.” Doe v. Stephens, 851 F.2d 1457, 1466-67 (D.C. Cir. 1988) (furthering the principle of “avoiding constitutional questions if at all possible” where the plaintiff did “not premise his claim for equitable relief on the APA,” but the court considered the claim under the APA rather than resolving the plaintiff’s constitutional claims); see also Fla. Med. Ass’n v. Dep’t of Health, Edu. & Welfare, 947 F. Supp. 2d 1325, 1351-56 (M.D. 2013) (vacating 1979 permanent injunction prohibiting public disclosure of reimbursements paid to Medicare providers that would

individually identify some providers, as no longer based on good law under Privacy Act; noting in dicta agency's final action to disclose information may be reviewed under APA); Arruda & Beaudoin v. Astrue, No. 11-10254, 2013 WL 1309249, at *14-15 (D. Mass. Mar. 27, 2013) (dismissing plaintiff's claim alleging that SSA's failure to timely respond to its request for information was not an agency action to be reviewed under APA, because APA provides no relief other than what is provided by the Privacy Act); Recticel Foam Corp. v. DOJ, No. 98-2523, slip op. at 9 (D.D.C. Jan. 31, 2002), appeal dismissed, No. 02-5118 (D.C. Cir. Apr. 25, 2002) (holding that court had jurisdiction under APA to enjoin FBI from disclosing investigative records in order to prevent future violation of subsection (b) of Privacy Act); Doe v. Herman, No. 97-0043, 1998 WL 34194937, at *4-7 (W.D. Va. Mar. 18, 1998) (invoking APA to issue preventative injunction in response to Privacy Act claim); cf. Haase v. Sessions, 893 F.2d 370, 374 n.6 (D.C. Cir. 1990) (stating in dicta that "[i]t is not at all clear to us that Congress intended to preclude broad equitable relief (injunctions) to prevent (e)(7) violations . . . [a]nd in the absence of such an explicit intention, by creating a general cause of action (under (g)(1)(D)) for violations of the Privacy Act, Congress presumably intended the district court to use its inherent equitable powers"); Rice v. United States, 245 F.R.D. 3, 7 (D.D.C. 2007) (noting that "there is some authority for awarding [declaratory] relief under the APA" for claims arising under Privacy Act); Doe v. Veneman, 230 F. Supp. 2d 739, 752 (W.D. Tex. 2002) (enjoining release of records in system of records, through "reverse FOIA" action, because release would violate the FOIA and Privacy Act), aff'd in part & rev'd in part on other grounds, 380 F.3d 807 (5th Cir. 2004).

However, courts in other cases have refused to allow claims brought under the APA where the relief sought is expressly provided by the Privacy Act. See, e.g., Harrison v. BOP, 248 F. Supp. 3d 172, 181-182 (D.D.C. 2017); Westcott v. McHugh, 39 F. Supp. 3d 21, 33 (D.D.C. 2014) (holding that "plaintiff cannot bring an APA claim to obtain relief for an alleged Privacy Act violation," and, citing Mittleman, supra, holding that plaintiff's APA claim simply restates plaintiff's Privacy Act claims); Echols v. Morpho Detection, Inc., No. C 12-1581, 2013 WL 1501523, at *2-3 (N.D. Cal. Apr. 11, 2013) (finding that "[p]laintiff does not provide any authority that demonstrates that he is required to make a greater showing in order to achieve relief under the Privacy Act or that adequate relief is not available under that Act" where plaintiff attempted to challenge agency's finding of his ineligibility to work under both Privacy Act and APA); Wilson v. McHugh, 842 F. Supp. 2d 310, 320 (D.D.C. 2012) ("To the extent [plaintiff] relies on the Privacy Act and believes the Privacy Act provides him a legal remedy, . . . [plaintiff] cannot seek review in this Court under the APA."); Tripp v. DOD, 193 F. Supp. 2d 229, 238-40 (D.D.C. 2002) (holding that "plaintiff can not bring an independent APA claim predicated on a Privacy Act violation"); Schaeuble v.

Reno, 87 F. Supp. 2d 383, 393-94 (D.N.J. 1998); Mittleman, 773 F. Supp. at 449 (finding that plaintiff's APA claim for failure to follow agency regulations and to provide plaintiff with hearing or other opportunity to rebut allegations against her in various government reports "is, in part, simply a restatement of her Privacy Act claims . . . [for which] Congress has provided plaintiff with statutory schemes and remedies through which she may seek relief").

In considering whether plaintiffs had a cause of action under the Declaratory Judgment Act ("DJA"), the D.C. District Court was recently "unconvinced" that plaintiffs were precluded from obtaining declaratory relief under the DJA "[b]ecause the Privacy Act provides for injunctive relief in specific situations." Morinville v. U.S. Patent and Trademark Office, 442 F. Supp. 3d 286, 295 (Feb. 26, 2020). In Morinville, the plaintiffs filed numerous claims addressing the Patent and Trademark Office's former "Sensitive Application Warning System" (SAWS), including a claim under the DJA requesting that the court declare that SAWS violated the Privacy Act. Id. at 289. In assessing the defendant's arguments in its motion to dismiss, the court found none of the purportedly supportive cases analogous to the situation, stating that "the Declaratory Judgment Act explicitly carves out several claims for which parties may not seek relief, and the Privacy Act is not among those carve-outs." Id. at 295-96; see also 28 U.S.C. § 2201. Ultimately, the court held that "relief under the [DJA] may be unnecessary, and the Court, in its discretion, may dismiss this claim. However, at the motion to dismiss stage, the Court is not prepared to say that Plaintiffs' [DJA] claim is duplicative of their Privacy Act claims or otherwise unnecessary or inappropriate." Morinville, 442 F. Supp. 3d at 296; cf. Schaeuble v. Reno, 87 F. Supp. 2d at 393 ("Assuming that the Court does have discretion, because Plaintiff, in good faith, tried to exhaust his administrative remedies, and it was Defendants' own failure to comport with the Privacy Act and its regulations that impeded Plaintiff's efforts to obtain administrative relief or exhaust his administrative remedies, the Court declines to withhold exercising its authority under the [DJA].").

The District Court for the District of Columbia has analyzed the relationship between the Privacy Act and the Health Care Quality Improvement Act ("HCQIA"), Pub. L. No. 99-660, 100 Stat. 3784, which "protect[s] patients from incompetent physicians by establishing a database to collect information related to professional competence or conduct which could adversely affect the health or welfare of patients." Doe v. Thompson, 332 F. Supp. 2d 124, 125 (D.D.C. 2004). In Doe, a dentist filed a subsection (g)(1)(B) claim against the Department of Health and Human Services. Id. at 127. However, "instead of reviewing the plaintiff's request pursuant to the Privacy Act, the [Department] responded by informing the plaintiff that the sole administrative remedy available to him was

the procedures promulgated by the [Department]" pursuant to HCQIA. Id. The court concluded that because the procedures promulgated by the Department pursuant to HCQIA "provide less protection than the procedures required by the Privacy Act," the Department "must adhere to the requirements of the Privacy Act when considering a dispute to a record" in the database established by HCQIA. Id. at 130, 132-33.

The D.C. District Court also has analyzed the relationship between the Privacy Act and the Health Insurance Portability and Accountability Act ("HIPAA"), 42 U.S.C. § 1320d-1320d-8 (2018), which "prohibits both the improper disclosure of individually identifiable health information and the improper acquisition of such information." Cacho v. Chertoff, No. 06-00292, 2006 WL 3422548, *2 (D.D.C. Nov. 28, 2006). In Cacho, the plaintiff brought a Privacy Act claim against the Department of Homeland Security "on the theory that [a Department employee] improperly accessed [the plaintiff's] medical record." Id. at *5. The court dismissed this claim on the ground that it "would be inconsistent with both HIPAA and the Privacy Act's plain language" to "recognize under the Privacy Act a private right of action that Congress has expressly denied under HIPAA." Id.

In addition, the District Court for the District of Columbia has dismissed a plaintiff's Privacy Act claim where the Attorney General invoked the State Secrets Privilege. Edmonds v. DOJ, 323 F. Supp. 2d 65, 80-82 (D.D.C. 2004), aff'd, 161 F. App'x 6 (D.C. Cir. 2005) (unpublished opinion). The court explained that "because the . . . documents related to the plaintiff's employment, termination and security review that comprise the system of records are privileged, and because the plaintiff would be unable to depose witnesses whose identities are privileged or to otherwise identify through discovery the individual or individuals who purportedly released the privileged information, the plaintiff is . . . unable to proceed with her Privacy Act claims." Id. at 81.

Courts may order expungement as equitable relief in actions under the Privacy Act or for Constitutional violations.

Several courts, including the United States Court of Appeals for the District of Columbia Circuit, have held that a court may order equitable relief in the form of the expungement of records either in an action under the Privacy Act or in a direct action under the Constitution. See, e.g., Abdelfattah v. DHS, 787 F.3d 524, 284-285 (D.C. Cir. 2015); Doe v. Air Force, 812 F.2d 738, 741 (D.C. Cir. 1987); Smith v. Nixon, 807 F.2d 197, 204 (D.C. Cir. 1986); Hobson v. Wilson, 737 F.2d 1, 65-66 (D.C. Cir. 1984), overruled in part on other grounds, Leatherman v. Tarrant Cnty. Narcotics Intel. & Coord. Unit, 507 U.S. 163 (1993); Ezenwa v. Gallen, 906

F. Supp. 978, 986 (M.D. Pa. 1995); cf. Shearson v. Holder, 725 F.3d 588, 595 (6th Cir. 2013) (refusing to entertain plaintiff’s argument that court should “use its equitable powers to expunge all the government records held by the Terrorist Screening Center that supported its placement of [plaintiff] in the terrorist databases” as court had no information about what those documents hold; affirming district court and finding it reasonable for plaintiff to exhaust administrative remedies under Traveler Redress Program); Dickson v. OPM, 828 F.2d 32, 41 (D.C. Cir. 1987) (suggesting that it is not resolved “whether as a general proposition the Privacy Act defines the scope of remedies available under the Constitution”); Clarkson v. IRS, 678 F.2d 1368, 1376 n.13 (11th Cir. 1982) (clarifying that court “[did] not intend to suggest that the enactment of the Privacy Act in any way precludes a plaintiff from asserting a constitutional claim for violation of his privacy or First Amendment rights. Indeed, several courts have recognized that a plaintiff is free to assert both Privacy Act and constitutional claims.”). See also the discussion of expungement of records under “5 U.S.C. § 552a(g)(1)(A) - Amendment Lawsuits,” above.

Finally, the courts have split over whether to grant class certifications in Privacy Act cases. For cases in which courts granted class certifications for claims brought under the Privacy Act, see Calvillo Manriquez v. DeVos, Case No. 17-cv-07210-SK, 2018 WL 5316175 (N.D. Cal. Oct. 15, 2018); Rice v. United States, 211 F.R.D. 10, 14 (D.D.C. 2002); Fort Hall Landowners Alliance, Inc. v. BIA, No. 99-052, slip op. at 10 (D. Idaho Aug. 16, 2002); Baker v. Runyon, No. 96-2619, 1997 WL 232606, at *4 (N.D. Ill. May 2, 1997); and Ingerman v. IRS, No. 89-5396, 1990 WL 10029523, at *2 (D.N.J. July 16, 1990). For cases in which courts denied class certifications for claims brought under the Privacy Act, see Doe v. Chao, 306 F.3d 170, 184 (4th Cir. 2002), aff’d on other grounds, 540 U.S. 614 (2004); Fort Hall Landowners Alliance, Inc. v. BIA, No. 99-052, 2007 WL 2187256, at *3 (D. Idaho July 16, 2007); Schmidt v. VA, 218 F.R.D. 619, 637 (E.D. Wis. 2003); and Lyon v. United States, 94 F.R.D. 69, 76 (W.D. Okla. 1982). For cases involving multiple plaintiffs, see Covert v. Harrington, 876 F.2d 751, 752 (9th Cir. 1989); Andrews v. VA, 838 F.2d 418, 419 (10th Cir. 1988); Parks v. IRS, 618 F.2d 677, 679 (10th Cir. 1980); and Romero-Vargas v. Shalala, 907 F. Supp. 1128, 1131 (N.D. Ohio Oct. 13, 1995).

1. Attorney Fees and Costs

“The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.” 5 U.S.C. § 552a(g)(2)(B), (g)(3)(B).

"[T]he United States shall be liable to the individual . . . [for] reasonable attorney fees as determined by the court." 5 U.S.C. § 552a(g)(4)(B).

Comment:

The Privacy Act is one of many federal statutes containing a "fee-shifting" provision allowing a prevailing plaintiff to recover attorney fees and costs from the government. It allows for such fees in both amendment and access suits. 5 U.S.C. §§ 552a(g)(2)(B) (amendment), (g)(3)(B) (access). The Privacy Act also allows for costs and attorney fees to be recovered in damages lawsuits, in addition to actual damages. 5 U.S.C. § 552a(g)(4)(B).

"Judgments, costs, and attorney's fees assessed against the United States under [subsection (g) of the Privacy Act] would appear to be payable from the public funds rather than from agency funds." OMB 1975 Guidelines, 40 Fed. Reg. at 28,949, https://www.justice.gov/paoverview_omb-75 (citing 28 U.S.C. § 2414 (2018); 31 U.S.C. § 724a (later replaced during enactment of revised Title 31, but see 31 U.S.C. § 1304 (2018) (first sentence of former § 724a) and 39 U.S.C. § 409(e) (2018) (last sentence of former § 724a); and 28 U.S.C. § 1924 (2018)).

"5 U.S.C. § 552a(g)(1)(A) - Amendment Lawsuits," "5 U.S.C. § 552a(g)(1)(B) - Access Lawsuits," "5 U.S.C. § 552a(g)(1)(C) - Damages Lawsuits for Failure to Assure Fairness in Agency Determination," "5 U.S.C. § 552a(g)(1)(D) - Damages Lawsuits for Failure to Comply with Other Privacy Act Provisions" are discussed in detail in separate sections above.

Pro se litigants, whether or not they are also attorneys, are not entitled to attorney fees for representing themselves.

The Supreme Court held that a pro se litigant who was also an attorney was not entitled to recover attorney fees under the fee-shifting provision of the statute authorizing attorney fees in civil rights suits against the government, 42 U.S.C. § 1988 (2018). Kay v. Ehrler, 499 U.S. 432, 437 (1991); see also Gahagan v. USCIS, 911 F.3d 298, 305 (5th Cir. 2018) (overruling Cazalas v. DOJ, 709 F.2d 1051 (5th Cir. 1983), and recognizing and applying Kay when ruling that "pro se attorneys are ineligible for fee awards under FOIA"). Although the Supreme Court in Kay did not expressly rule on the issue of the award of attorney fees to non-attorney pro se litigants, the Court recognized that "the Circuits are in agreement . . . that a pro se litigant who is not a lawyer is not entitled to attorney's fees" and was "satisfied that [those cases so holding] were correctly decided." 499 U.S. at 435.

The Court's rationale in Kay would seem to preclude an award of fees to any pro se Privacy Act litigant, as the Court observed that "awards of counsel fees to pro se litigants – even if limited to those who are members of the bar – would create a disincentive to employ counsel" and that "[t]he statutory policy of furthering the successful prosecution of meritorious claims is better served by a rule that creates an incentive to retain counsel in every such case." Id. at 438; see also Wilborn v. HHS, No. 91-538, slip op. at 14-16 (D. Or. Mar. 5, 1996) (rejecting argument that rationale in Kay should be construed as applying only to district court stage of litigation; "policy of the Privacy Act . . . would be better served by a rule that creates an incentive to retain counsel at all stages of the litigation, including appeals"), appeal voluntarily dismissed, No. 96-35569 (9th Cir. June 3, 1996); but cf. Smith v. O'Brien, No. 94-41371, 1995 WL 413052, at *2 (5th Cir. June 19, 1995) (per curiam) (citing Barrett v. Customs, infra, and stating: "Pro se litigants are not entitled to attorney fees under either the FOIA or the Privacy Act unless the litigant is also an attorney").

Indeed, the Court of Appeals for the District of Columbia Circuit summarily affirmed a district court decision which held that a "nonattorney pro se litigant cannot recover attorney's fees under the Privacy Act." Sellers v. BOP, No. 87-2048, 1993 U.S. Dist. LEXIS 787, at *1 (D.D.C. Jan. 26, 1993), summary affirmance granted, No. 93-5090, 1993 WL 301032 (D.C. Cir. July 27, 1993). See also Smith v. O'Brien, 1995 WL 413052, at *2 ("Pro se litigants are not entitled to attorney fees under either the FOIA or the Privacy Act unless the litigant is also an attorney."); Barrett v. Customs, 651 F.2d 1087, 1089 (5th Cir. 1981) (denying a non-attorney pro se litigant fees); Riser v. State, No. 09-3273, 2010 WL 4284925, at *8 (S.D. Tex. Oct. 22, 2010) (citing Barrett and Smith and denying non-attorney pro se plaintiff's request for attorney fees); Westendorf v. IRS, No. 3:92-cv-761WS, 1994 WL 714011, at *2 (S.D. Miss. July 7, 1994) (citing Barrett and holding that non-attorney pro se plaintiff is not entitled to attorney fees because there was no evidence pro se plaintiff was an attorney), appeal dismissed, No. 94-60503, slip op. at 2-3 (5th Cir. Nov. 17, 1994) (stating that district court's holding is correct under Barrett).

The D.C. Circuit has further ruled, however, that a plaintiff's pro se status does not preclude the recovery of fees for "consultations" with outside counsel. Blazy v. Tenet, 194 F.3d 90, 94 (D.C. Cir. 1999); see also id. at 98-99 (Sentelle, J., concurring but "writ[ing] separately only to distance [him]self from the majority's determination that a pro se litigant is entitled to recover counsel fees for consultations with attorneys not appearing or connected with appearances in the pro se litigation").

The courts are split as to whether courts considering Privacy Act fee claims should consult FOIA cases.

The subsection (g)(2)(B) and (g)(3)(B) attorney fees provisions for amendment and access suits under the Privacy Act are similar to 5 U.S.C. § 552(a)(4)(E), the FOIA's attorney fees provision. Courts are split regarding whether a court may consult FOIA decisions concerning a plaintiff's eligibility for attorney fees when assessing a plaintiff's eligibility for attorney fees under the Privacy Act. The D.C. Circuit has expressly ruled that the FOIA's criteria for determining a plaintiff's entitlement to attorney fees are inapplicable to a claim for fees under the Privacy Act. Blazy, 194 F.3d at 95-97 ("Even a cursory examination of these factors makes it clear that they have little or no relevance in the context of the Privacy Act."); see also Herring v. VA, No. 94-55955, 1996 WL 32147, at *5-6 (9th Cir. Jan. 26, 1996) (finding plaintiff to be "prevailing party" on access claim for her medical record with no mention or application of FOIA criteria); but see Sweatt v. Navy, 683 F.2d 420, 423 (D.C. Cir. 1982) (stating in dicta that cases construing whether plaintiffs had "substantially prevailed" for purposes of attorney fee provision in FOIA are apposite in Privacy Act context, although Blazy court distanced itself from this language).

On the other hand, the Fourth, Fifth, and Tenth Circuit Courts of Appeals have held that the FOIA's fee entitlement criteria apply to Privacy Act claims for attorney fees. See Gowan v. Air Force, 148 F.3d 1182, 1194-95 (10th Cir. 1998) (applying the FOIA's criteria and determining that plaintiff was not entitled to fees because his "suit was for his personal benefit rather than for the benefit of the public interest"); see also Reinbold v. Evers, 187 F.3d 348, 362 (4th Cir. 1999) (citing Gowan and stating in dicta that if determination is made that plaintiff substantially prevailed, court must evaluate FOIA factors to determine entitlement); Barrett v. Customs, 651 F.2d at 1088 (stating that FOIA's guidelines apply to claims for attorney fees under Privacy Act).

Despite the evolution of the "catalyst" theory under the FOIA, the courts have not definitively ruled on its applicability in Privacy Act cases.

In the FOIA context, the Supreme Court held in 2001 that "the 'catalyst theory' is not a permissible basis for the award of attorney's fees." Buckhannon Bd. & Care Home, Inc. v. W. Va. Dep't of Health & Human Resources, 532 U.S. 598, 610 (2001). In 2002, the D.C. Circuit followed that approach, holding that "in order for plaintiffs in FOIA actions to become eligible for an award of attorney's fees, they must have 'been

awarded some relief by [a] court,' either in a judgment on the merits or in a court-ordered consent decree." Oil, Chem. & Atomic Workers Int'l Union v. Energy, 288 F.3d 452, 455-56 (D.C. Cir. 2002) (quoting and applying Buckhannon). This interpretation of Buckhannon was widely followed for years, with the result that plaintiffs were denied attorney fees in FOIA cases in which the agency voluntarily disclosed the records at issue. *See, e.g., Union of Needletrades, Indus. & Textile Employees v. INS*, 336 F.3d 200, 206 (2d Cir. 2003); McBride v. Army, No. 06-4082, 2007 WL 1017328, at *3-4 (E.D. La. Mar. 30, 2007); Poulsen v. Customs & Border Prot., No. 06-1743, 2007 WL 160945, at *1 (N.D. Cal. Jan. 17, 2007); Landers v. Air Force, 257 F. Supp. 2d 1011, 1012 (S.D. Ohio 2003).

However, Congress amended the FOIA in 2007 to explicitly provide for attorney fees under a "catalyst theory." *See* OPEN Government Act of 2007, Pub. L. No. 110-175, 121 Stat. 2524. The FOIA now provides that a plaintiff is eligible to obtain attorney fees if records are obtained as a result of "(I) a judicial order, or an enforceable written agreement or consent decree; or (II) a voluntary or unilateral change in position by the agency, if the complainant's claim is not insubstantial." 5 U.S.C. § 552(a)(4)(E)(ii), as amended; *see also* Brayton v. Office of the U.S. Trade Representative, 641 F.3d 521, 525 (D.C. Cir. 2011) ("The purpose and effect of this law, which remains in effect today, was to change the 'eligibility' prong back to its pre-Buckhannon form."); Davis v. DOJ, 610 F.3d 750, 752 (D.C. Cir. 2010) ("Congress enacted the OPEN Government Act of 2007 to establish that the catalyst theory applied in FOIA cases.").

Although there has not been significant litigation regarding the "catalyst theory" in Privacy Act fee cases, at least one case arising in the Fourth Circuit, which, as noted above, has explicitly adopted the FOIA criteria for determinations of entitlement to fees, applied the catalyst theory in the Privacy Act context. Crockett v. VA, No. 7:17-CV-186, 2018 WL 1684284, at *4 (W.D. Va. Jan. 19, 2018), report and recommendation adopted Crockett v. VA, No. 7:17-CV-00186, 2018 WL 4550449 (W.D. Va. Sept. 21, 2018) (applying catalyst theory but ultimately concluding that plaintiff had "not produced evidence that his lawsuit was a catalyst for the VA's production of his records" and, therefore, was not eligible to recover attorneys' fees); *cf.* Reinbold v. Evers, 187 F.3d at 363 (recognizing without discussing catalyst theory in pre-OPEN Government Act case but upholding denial of fees where evidence showed that delay was result of staffing shortage rather than "that [plaintiff's] lawsuit was a catalyst for the [agency's] action"); Jacobs v. Reno, No. 3:97-CV-2698-D, 1999 WL 155708, at *4-5 (N.D. Tex. Mar. 11, 1999) (denying plaintiff's request for attorney fees and costs, and stating

without using “catalyst theory” terminology that plaintiff’s argument that his lawsuit caused agency “to comply with the Privacy Act when it would not otherwise have done so” was “too slim a reed on which to rest” his claim), aff’d, 208 F.3d 1006 (5th Cir. 2000) (unpublished table decision).

The impact of the OPEN Government Act in courts that have not tied the Privacy Act fee analysis to the FOIA is less clear, given that not many cases have addressed the issue. The D.C. District Court applied the “catalyst theory” in a case in which the plaintiff sought fees under the FOIA along with the Privacy Act but ultimately concluded that the plaintiffs had not “substantially prevailed.” Mobley v. DHS, 908 F. Supp. 2d 42, 45 (D.D.C. 2012); but see Sterrett v. Navy, No. 09-CV-2083-IEG POR, 2010 WL 330086, at *6 (S.D. Cal. Jan. 20, 2010) (applying different standards to Privacy Act and FOIA fee claims).

Although not explicitly addressed in the Privacy Act context, enhanced fees to compensate for risk in contingency fee arrangements generally are not permitted.

Under the FOIA, the D.C. Circuit had previously held that a fee enhancement as compensation for the risk in a contingency fee arrangement might be available in limited circumstances. See, e.g., Weisberg v. DOJ, 848 F.2d 1265, 1272 (D.C. Cir. 1988). The Supreme Court has clarified, however, that such enhancements are not available under statutes authorizing an award of reasonable attorney fees to a prevailing or substantially prevailing party. City of Burlington v. Dague, 505 U.S. 557, 561-66 (1992) (prohibiting contingency enhancement in environmental fee-shifting statutes). The Court further observed that case law “construing what is a ‘reasonable’ fee applies uniformly to all [federal fee-shifting statutes].” Id. In light of this observation, there seems to be little doubt that the same principle also prohibits fee enhancements under the Privacy Act. Id. at 562; see also King v. Palmer, 950 F.2d 771, 775 (D.C. Cir. 1991) (en banc) (Silberman, C.J., concurring).

Courts appear to differ as to whether attorney fees and costs can be recovered even without a showing of “actual damages.”

The Fourth Circuit held in a damages lawsuit brought under the Privacy Act, that “[t]he face of [subsection (g)(4)] leaves no room for confusion on this point” and “does not require a showing of actual damages . . . in order to receive costs and reasonable attorney fees.” Doe v. Chao, 435 F.3d 492, 495-96 (4th Cir. 2006). The Fourth Circuit further explained that “the word ‘sum’ – as it is used in [subsection (g)(4)] – requires a court to fulfill the

simple act of adding actual damages and fees and costs once the preceding elements of the statute are satisfied,” and therefore, plaintiff who establishes violation but does not recover damages is eligible for attorney fees. Id. In reaching its decision, the Fourth Circuit rejected the government’s argument that the Supreme Court had reached a contrary conclusion. Id. at 497, citing Doe v. Chao, 540 U.S. at 625 n.9. The Fourth Circuit Court of Appeals analyzed the Supreme Court’s footnote in Doe v. Chao and concluded that “in no place did the [Supreme Court] purport to interpret § 552a(g)(4)(B)”; instead, “The Supreme Court’s phrase . . . means nothing more than the obvious fact that the Government cannot be liable for actual damages if there are no actual damages.” 435 F.3d at 497.

Although a subsequent decision of the District Court of the District of Columbia questioned the Court Circuit’s conclusion, it did so in dicta. Rice v. United States, 245 F.R.D. 3, 7 n.6 (D.D.C. 2007) (“There is some question as to whether plaintiffs could recover costs and reasonable attorney fees under section 552a(g)(4) even without showing actual damages. . . As Judge Michael’s dissent in [Doe v. Chao, 435 F.3d at 507] points out, however, the Supreme Court’s [opinion in Doe v. Chao, 540 U.S. at 625 n.9] appears to foreclose such a recovery.”).

Attorney fees are only available in amendment cases if the plaintiff has exhausted administrative remedies; attorney fees are not available for administrative representation.

The D.C. Circuit has held that attorney fees are not available in a subsection (g)(1)(A) amendment case unless the plaintiff has exhausted his administrative remedies. See Haase v. Sessions, 893 F.2d 370, 373-75 (D.C. Cir. 1990); Sterrett v. Navy, 2010 WL 330086, at *6 (relying on Haase in subsection (g)(1)(B) access case and concluding that “a fee award would be improper because Plaintiff failed to exhaust her administrative remedies”).

Attorney fees are not recoverable for services rendered at the administrative level. See Kennedy v. Andrus, 459 F. Supp. 240, 244 (D.D.C. 1978), aff’d, 612 F.2d 586 (D.C. Cir. 1980) (unpublished table decision).

In addition to attorney fees, prevailing plaintiffs can also recover the costs of litigation.

Litigation costs (if reasonably incurred) can be recovered by all plaintiffs who substantially prevail. See Parkinson v. Comm’r, No. 87-3219, 1988 WL 12121, at *3 (6th Cir. Feb. 17, 1988); Walker v. DOJ, No. 00-0106, slip op. at 5-

6 (D.D.C. July 14, 2000); Young v. CIA, No. 91-527-A, slip op. at 2 (E.D. Va. Nov. 30, 1992), aff'd, 1 F.3d 1235 (4th Cir. 1993) (unpublished table decision). Compare Herring, No. 94-55955, 1996 WL 32147, at *5-6 (finding that plaintiff was “a prevailing party with respect to her access claim” because “the VA did not provide her access to all her records until she filed her lawsuit”), with Abernethy v. IRS, 909 F. Supp. 1562, 1567-69 (N.D. Ga. 1995) (“[T]he fact that records were released after the lawsuit was filed, in and of itself, is insufficient to establish Plaintiff’s eligibility for an award of attorneys’ fees.”), aff’d per curiam, 108 F.3d 343 (11th Cir. Feb. 13, 1997) (unpublished table decision). Further, the D.C. Circuit held that a pro se plaintiff’s claim for litigation costs under the Privacy Act is not limited by 28 U.S.C. § 1920 (governing litigation costs generally). Blazy, 194 F.3d at 94-95 (following reasoning of Kuzma v. IRS, 821 F.2d 930 (2d Cir. 1987) (FOIA case)).

2. Jurisdiction and Venue

“An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia. . .” 5 U.S.C. § 552a(g)(5).

Comment:

Federal district courts have exclusive jurisdiction over Privacy Act suits.

By its very terms, this section limits jurisdiction over Privacy Act matters to the federal district courts. 5 U.S.C. § 552a(g)(5). Accordingly, the U.S. Court of Federal Claims does not have jurisdiction over Privacy Act claims. See, e.g., Parker v. United States, 280 F. App’x 957, 958 (Fed. Cir. 2008) (affirming Court of Federal Claims’ determination that “the Court of Federal Claims is not the proper forum for such action. . . . district courts have jurisdiction in matters under the Privacy Act”); Braun v. United States, 144 Fed. Cl. 560, 571 (2019) (“Any claims that plaintiff wishes to pursue under the Privacy Act can only be brought in a District Court, and cannot be brought in this court.”); Frazier v. United States, No. 16-1287C, 2016 WL 6583715, at *2 (Fed. Cl. Nov. 1, 2016), aff’d, 683 F. App’x 938 (Fed. Cir. 2017); Madison v. United States, 98 Fed. Cl. 393, 395 (Fed. Cl. 2011); Treece v. United States, 96 Fed. Cl. 226, 232 (Fed. Cl. 2010); Addington v. United States, 94 Fed. Cl. 779, 784 (Fed. Cl. 2010); Stephanatos v. United States, 81 Fed. Cl. 440, 444 (Fed. Cl. 2008); Agee v. United States, 72 Fed. Cl. 284, 290 (Fed. Cl. 2006); Doe v.

United States, 74 Fed. Cl. 794, 798 (Fed. Cl. 2006). Likewise, neither the Merit Systems Protection Board nor the U.S. Tax Court has jurisdiction over Privacy Act claims. See, e.g., Carell v. MSPB, 131 F. App'x 296, 299 (Fed. Cir. 2005); Martin v. Army, No. 00-3302, 2000 WL 1807419, at *2 (Fed. Cir. Dec. 8, 2000) (per curiam) (MSPB); Minnich v. MSPB, No. 94-3587, 1995 U.S. App. LEXIS 5768, at *3 (Fed. Cir. Mar. 21, 1995) (per curiam) (MSPB); Strickland v. Comm'r, No. 9799-95, 2000 WL 274077, at *1 (T.C. Mar. 14, 2000) (U.S. Tax Court). Note, however, that final orders of the National Transportation Safety Board (NTSB) are reviewed in U.S. courts of appeals rather than district courts, even where the case in question involves the Privacy Act. See Creed v. NTSB, 758 F. Supp. 2d 1, 4-8 (D.D.C. 2011) (holding that judicial review provision of Independent Safety Board Act, 49 U.S.C. § 1153(a), operates to give exclusive jurisdiction to appropriate U.S. Court of Appeals or Court of Appeals for the District of Columbia Circuit to review final orders of NTSB).

D.C. Circuit decisions carry great weight in Privacy Act matters.

Because the Privacy Act specifically provides for venue in the District of Columbia, the Privacy Act decisions of the Court of Appeals for the District of Columbia Circuit are of great importance. Tyler v. U.S. BOP, 315 F. Supp. 3d 313, 315 n.1 (D.D.C. 2018), aff'd sub nom. Tyler v. BOP, No. 18-5187, 2019 WL 1752626 (D.C. Cir. Mar. 28, 2019) (“The venue provisions of both the Privacy Act and the FOIA identify the federal district court in the District of Columbia as a proper venue for such claims.”)

The text of the Privacy Act specifies the factors courts consider in making venue determinations.

Courts considering venue have weighed the factors specified in the statute: the plaintiff’s place of residence, the plaintiff’s principal place of business, or the place where agency records are located. See, e.g., Akutowicz v. United States, 859 F.2d 1122, 1126 (2d Cir. 1988) (finding “only proper venue for this action is the District of Columbia” where plaintiff resided and worked continuously in France and agency records were in D.C.); Shallow v. FBI, No. 1:19-CV-229, 2019 WL 2718493, at *2 (E.D. Va. June 27, 2019), aff'd, 788 F. App'x 189 (4th Cir. 2019) (transferring venue to District of Columbia where plaintiff’s mailing address was there and complaint made “no mention of Plaintiff having another residential address, a principal place of business, nor where the alleged agency records may be located”); Schneider v. Brennan, No. 15-CV-263-JDP, 2016 WL 29642, at *3 (W.D. Wis. Jan. 4, 2016) (transferring venue to district in which “relevant agency records” and

OVERVIEW OF THE PRIVACY ACT

employees involved in case were located); Doe v. Army, 99 F. Supp. 3d 159, 161 (D.D.C. 2015) (“Privacy Act cases may be brought where the plaintiff ‘resides, or has his principal place of business, or [where] the agency records are situated, or in the District of Columbia.’”); Echols v. Morpho Detection, Inc., No. C 12-1581, 2013 WL 1501523, at *6 (N.D. Cal. Apr. 11, 2013) (finding venue was improper because plaintiff resided and was employed in another district and records were in Washington, D.C. or Virginia, and finding that doctrine of pendent jurisdiction does not apply to special venue statutes like Privacy Act that specify proper venue); Budik v. United States, No. 09-3079, 2011 U.S. Dist. LEXIS 74655, at *4 (D. Md. July 11, 2011) (transferring Privacy Act claim to District of Columbia, where plaintiff resided and “where the records at issue were created and stored”; adding that “the United States District Court for the District of Columbia is surely more thoroughly vested in the complex issues surrounding suits brought against the United States under the Privacy Act than is this Court”); In re Dep’t of VA Data Theft Litig. v. Nicholson, 461 F. Supp. 2d 1367, 1368-69 (E.D. Ky. 2006) (explaining that District of Columbia “is a preferable transferee forum for this litigation” because it is “where likely relevant documents and witnesses may be found, inasmuch as many of the defendants are located in this district and the theft occurred in the Washington, D.C., metropolitan area”); Roberts v. DOT, No. 02-829, 2002 U.S. Dist. LEXIS 14116, at *1-2 (E.D. Pa. July 3, 2003) (transferring venue to Eastern District of New York, as “both plaintiff and the records are located within [that district]”); Troupe v. O’Neill, No. 02-4157, 2003 WL 21289977, at *3 (D. Kan. May 9, 2003) (transferring case to Northern District of Georgia as “agency records would be situated there”); Warg v. Reno, 19 F. Supp. 2d 776, 785 (N.D. Ohio 1998) (transferring case to District of Columbia in interest of justice where plaintiff resided in Maryland and records were located in Washington, D.C.); Finley v. NEA, 795 F. Supp. 1457, 1467 (C.D. Cal. 1992) (“[I]n a multi-plaintiff Privacy Act action, if any plaintiff satisfies the venue requirement of 5 U.S.C. § 552a(g)(5), the venue requirement is satisfied as to the remaining plaintiffs.”).

Although the Act specifies the D.C. District Court as an appropriate venue, that court at times has transferred cases elsewhere.

The District Court for the District of Columbia is always a proper venue, but the courts in the District of Columbia have transferred venue elsewhere when “private and public interest factors” make another jurisdiction “the more appropriate venue.” See Doe v. Army, 99 F. Supp. 3d at 162; see also Hooker v. NASA, 961 F. Supp. 2d 295, 297 (D.D.C. 2013) (transferring venue to Maryland where plaintiff lived there, agency was headquartered there,

and “other potential sources of proof, including records” and witnesses were in Maryland).

Similarly, in cases in which the plaintiff filed other claims in addition to a Privacy Act claim, the courts in the District of Columbia have often concluded that for purposes of judicial economy, the Privacy Act claim should be heard in the same jurisdiction as the other claims. See, e.g., Valerino v. Holder, 20 F. Supp. 3d 203, 206 (D.D.C. 2013) (concluding that Privacy Act claim was appropriately heard with Title VII claim in the Eastern District of Virginia “in the interests of justice” because that is where “the relevant conduct occurred,” and “most of the witnesses are located”); Tildon v. Alexander, 587 F. Supp. 2d 242, 243 n.1 (D.D.C. 2008) (transferring multi-claim cause of action to Maryland, even though Privacy Act allowed venue in District of Columbia, because venue for other claims was Maryland and “judicial economy . . . will be served by transferring this action in its entirety”); Dehaemers v. Wynne, 522 F. Supp. 2d 240, 248-49 (D.D.C. 2007) (concluding that appropriate venue for plaintiff’s Title VII and Rehabilitation Act claims was Virginia and, although plaintiff’s Privacy Act claims were properly in District of Columbia, court would not assume pendant jurisdiction over other claims, and plaintiff could “pursue a single action in [Virginia] either by seeking a dismissal without prejudice of his Privacy Act claim, or by moving this Court to transfer his Privacy Act claim”); Boers v. United States, 133 F. Supp. 2d 64, 65 (D.D.C. 2001) (transferring case under 28 U.S.C. § 1404(a) to plaintiff’s “home forum,” even though “venue is proper” in District of Columbia, given that “[a]ll the operative facts occurred in Arizona” and “it cannot be said that forcing a plaintiff to litigate in his home district will prejudice or burden the plaintiff in any way”), mandamus denied per curiam sub nom. In re Howard L. Boers, No. 01-5192 (D.C. Cir. Aug. 28, 2001).

Generally, for plaintiffs who are in prison, the jurisdiction where the plaintiff is incarcerated is the appropriate venue.

When the plaintiff is incarcerated, most courts have held that the appropriate venue under the Privacy Act is the jurisdiction where the plaintiff is incarcerated rather than the jurisdiction of his or her previous domicile. See, e.g., Pinson v. DOJ, 74 F. Supp. 3d 283, 294 (D.D.C. 2014) (finding that because plaintiff “is currently incarcerated in Colorado, a large portion of the records and witnesses at issue are located in the state, and . . . because of possible transportation difficulties,” Privacy Act claim is more appropriately litigated in District of Colorado); United States v. Barrenechea, No. 94-0206, 2013 WL 3014141, at *2 (N.D. Cal. June 17, 2013) (“Given that

Barrenechea is incarcerated in USP-Victorville, coupled with the fact that the challenged records are alleged to be located there, the Court notes that the Central District of California, not the Northern District, appears to be the appropriate venue for Barrenechea's Privacy Act claims."); United States v. Cornejo, No. 94-0206, 2013 WL 3052913, at *2 (N.D. Cal. June 17, 2013) (following Barrenechea); Royer v. BOP, No. 1:10-cv-0146, 2010 WL 4827727, at *4 (E.D. Va. Nov. 19, 2010) ("Royer's domicile may well be in the Eastern District of Virginia. However, in light of the fact that he is presently serving a 20-year sentence and is confined in a federal facility in Colorado, Royer has failed to set forth sufficient information establishing that he resides in this District for FOIA and Privacy Act purposes."); Harton v. BOP, No. 97-0638, slip op. at 3, 6-7 (D.D.C. Nov. 12, 1997) (stating that "the fact that the Privacy Act provides for venue in the District of Columbia does not, by itself, establish that each and every Privacy Act claim involves issues of national policy," and granting agency's motion to transfer to the jurisdiction where plaintiff was incarcerated, as complaint focused primarily on issues specific to plaintiff); but see Pickard v. DOJ, No. C 10-05253, 2011 WL 2199297, at *2-3 (N.D. Cal. June 7, 2011) (acknowledging that some courts have interpreted comparable venue language under FOIA to "conclude that residence is where the now-incarcerated defendant was last domiciled" and "find[ing] more persuasive the cases holding that an individual resides where he is incarcerated, at least for purposes of FOIA and the Privacy Act," but transferring case to jurisdiction where records were located).

One court has concluded that venue should be evaluated at the time the suit is filed.

Although apparently only one court has addressed the issue of whether venue should be considered at the time the suit was filed or at the time the cause of action arose, that court concluded that it would follow the general rule that "courts determine venue based on the facts at the time the suit was filed, not when the cause of action arose." Schneider v. Brennan, 2016 WL 29642, at *2 (indicating that court "has not found any decision specifically addressing this question in the context of a Privacy Act claim, but the general rule is widely followed," and referencing Daughetee v. CHR Hansen, Inc., No. 09-cv-41, 2011 WL 1113868, at *4 (N.D. Iowa Mar. 25, 2011) (collecting cases)).

3. Statute of Limitations

"An action to enforce any liability created under this section may be brought . . . within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented

any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.” 5 U.S.C. § 552a(g)(5).

Comment:

Courts have split over whether the Privacy Act’s statement that suits “may be brought . . . within two years” is jurisdictional.

The Second, Third, Sixth, Seventh, and Tenth Circuit Courts of Appeals and some district courts have held that the statute of limitations is jurisdictional in nature and have strictly construed it to be an “integral condition of the sovereign’s consent to be sued under the Privacy Act.” Bowyer v. Air Force, 875 F.2d 632, 635 (7th Cir. 1989) (quoting Diliberti v. United States, 817 F.2d 1259, 1262 (7th Cir. 1987)); accord Harrell v. Fleming, 285 F.3d 1292, 1293-94 (10th Cir. 2002); Weber v. Henderson, 33 F. App’x 610, 611 (3d Cir. 2002) (per curiam); Davis v. DOJ, 204 F.3d 723, 726 (7th Cir. 2000) (per curiam); Akutowicz v. United States, 859 F.2d 1122, 1126 (2d Cir. 1988); Davis v. Gross, No. 83-5223, 1984 U.S. App. LEXIS 14279, at *3-4 (6th Cir. May 10, 1984); Hussein v. Sessions, No. 16-cv-780, 2017 WL 1954767, at *4 (D. Minn. May 10, 2017), aff’d per curiam, 715 F. App’x 585 (8th Cir. 2018); Jagun v. Rodriguez, No. 15-2230, 2016 WL 4124225, at *8 (D. Md. Aug. 3, 2016); Doe v. FDIC, No. 11 Civ. 307, 2012 WL 612461, at *4 (S.D.N.Y. Feb. 27, 2012); Mauldin v. Napolitano, No. 10-12826, 2011 WL 3113104, at *2 (E.D. Mich. July 26, 2011); Bassiouni v. FBI, No. 02-8918, 2003 WL 22227189, at *2 (N.D. Ill. Sept. 26, 2003), aff’d on other grounds, 436 F.3d 712 (7th Cir. 2006); Logan v. United States, 272 F. Supp. 2d 1182, 1187 (D. Kan. 2003); Mangino v. Army, 818 F. Supp. 1432, 1437-38 (D. Kan. 1993), aff’d, 17 F.3d 1437 (10th Cir. 1994) (unpublished table decision). Consequently, a plaintiff’s failure to file suit within the specified time period has been held to “[deprive] the federal courts of subject matter jurisdiction over the action.” Diliberti, 817 F.2d at 1262.

However, the courts of appeals “have not unanimously adhered to the view that the Privacy Act’s statute of limitations is jurisdictional, such that a plaintiff’s failure to file a Privacy Act claim within the Privacy Act’s limitations period deprives a federal court of subject-matter jurisdiction over the claim.” Carter v. DOD, No. 16-0786, 2017 WL 2271416, at *8 (D.N.M.

Feb. 28, 2017). The Courts of Appeals for the District of Columbia and Ninth Circuits, as well as other district courts, have concluded that there is a “rebuttable presumption” in favor of equitable tolling in Privacy Act cases. The D.C. Circuit held that the “‘rebuttable presumption’ in favor of equitable tolling” in suits against the United States—the general rule announced in Irwin v. VA, 498 U.S. 89, 95 (1990)—applies to the Privacy Act. Chung v. DOJ, 333 F.3d 273, 277 (D.C. Cir. 2003) (overruling Griffin v. Parole Comm’n, 192 F.3d 1081, 1082 (D.C. Cir. 1999) (per curiam)). The D.C. Circuit concluded that “a Privacy Act claim for unlawful disclosure of personal information is sufficiently similar to a traditional tort claim for invasion of privacy to render the Irwin presumption applicable.” Chung, 333 F.3d at 276-77.

Although the D.C. Circuit appeared to limit its holding in Chung to “claim[s] for unlawful disclosure of personal information,” 333 F.3d at 277, the District Court for the District of Columbia has relied on Chung in considering equitable tolling in other types of Privacy Act claims without conducting the “similarity inquiry” articulated in Chung, 333 F.3d at 277, with respect to the individual claims. See, e.g., Earle v. Holder, 815 F. Supp. 2d 176, 180 (D.D.C. 2011) (considering apparent (g)(1)(A) and (g)(1)(C) claim, and applying principle that statute of limitations is subject to equitable tolling “when the plaintiff ‘despite all due diligence . . . is unable to obtain vital information bearing on the existence of his claim’” (quoting Chung, 333 F.3d at 278)), aff’d per curiam, No. 11-5280, 2012 WL 1450574 (D.C. Cir. Apr. 20, 2012); Bailey v. Fulwood, 780 F. Supp. 2d 20, 23, 27-28 (D.D.C. 2011) (citing Kursar and Chung for proposition that Privacy Act statute of limitations “is not a jurisdictional bar,” but ultimately dismissing apparent (g)(1)(C) claim because “there is no reason in this case to toll the running of the statute of limitations”); Kursar v. TSA, 751 F. Supp. 2d 154, 165-69 (D.D.C. 2010) (finding (g)(1)(C) claim not equitably tolled by plaintiff’s MSPB action challenging employment termination), aff’d per curiam, 442 F. App’x 565 (D.C. Cir. 2011).

The Ninth Circuit also has adopted the Supreme Court’s rebuttable presumption approach from Irwin and held that Privacy Act claims brought under subsection (g)(1)(D) and based on alleged violations of subsections (e)(5) and (e)(6) “are sufficiently similar to traditional tort actions such as misrepresentation and false light to warrant the application of Irwin’s rebuttable presumption.” Rouse v. State, 567 F.3d 408, 416 (9th Cir. 2009) (amended opinion) (citing Chung, 333 F.3d at 277). Because the Ninth Circuit agreed with Chung that no aspect of the Privacy Act “militate[s] against tolling,” the court concluded that “the Irwin presumption has not

been rebutted.” Rouse, 567 F.3d at 416-17. However, the court “decline[d] to decide whether equitable tolling is warranted on the facts of this case.” Id. at 417. See also Boyd v. United States, 932 F. Supp. 2d 830, 838 (S.D. Ohio 2013) (interpreting Irwin, the court held that “[i]n the absence of specific Congressional intent to the contrary, and considering the Privacy Act’s similarity to privacy actions in tort . . . the Privacy Act’s statute of limitations is a traditional statute of limitations”); Shearson v. Holder, 865 F. Supp. 2d 850, 867-68 (N.D. Ohio 2011) (noting the “split in the circuits as to whether the Privacy Act’s statute of limitations is jurisdictional in nature” but “agree[ing] with the courts that have adopted the Irwin approach and have held that Privacy Act claims are sufficiently similar to privacy tort claims to trigger the application of the Irwin rule”); Fort Hall Landowners All., Inc. v. BIA, No. 99-052, slip op. at 6-7 (D. Idaho Mar. 17, 2003) (citing Irwin and finding that the Privacy Act “does not use such language [of jurisdiction], and therefore does not present a jurisdictional bar”). But see Gonzalez v. United States, No. 18-cv-21789, 2018 WL 7825025, at *4-5 & n.5 (S.D. Fla. Oct. 11, 2018) (noting circuit split and that Eleventh Circuit “has not spoken” on jurisdictional issue, and finding no need to decide the issue); Carter, 2017 WL 2271416, at *12 (stating that “in light of [Irwin], the Court agrees with the Ninth Circuit’s and the D.C. Circuit’s reasoning that it does not make sense to treat the Privacy Act’s statute of limitations as a jurisdictional bar” but dismissing claims for lack of subject-matter jurisdiction because “bound to follow faithfully” Tenth Circuit precedent).

a. Statute of Limitations in Amendment suits

For Privacy Act amendment suits, the statute of limitations period begins when the agency denies the plaintiff’s request to amend.

In a subsection (g)(1)(A) amendment suits, the limitations period begins when the agency denies the plaintiff’s request to amend. See Englerius v. VA, 837 F.2d 895, 897-98 (9th Cir. 1988) (holding that the statute of limitations “commences at the time that a person knows or has reason to know that the request has been denied,” rather than as of the date of the request letter); see also Djenasevic v. EOUSA, 319 F. Supp. 3d 474, 482-83 (D.D.C. 2018) (dismissing amendment claims filed in 2016 on statute of limitations grounds because agency notified plaintiff of denial of request to amend records in 2011), aff’d per curiam, No. 18-5262, 2019 WL 5390964, at *1 (D.C. Cir. Oct. 3, 2019); Otero v. DOJ, 292 F. Supp. 3d 245, 253 (D.D.C. 2018) (holding that limitations period began when agency affirmed FBI’s decision to deny amendment of records), aff’d per curiam, No. 18-5080, 2019 WL 4565497 (D.C. Cir. Sept. 4, 2019); Kursar, 751 F.

Supp. 2d at 167 (finding that “the statute of limitations for this claim began running when the TSA denied [plaintiff’s] amendment request”); Bassiouni, 2003 WL 22227189, at *3-4 (acknowledging distinction as to when claim arises among four distinct Privacy Act causes of actions and finding that in an amendment cause of action, a claim arises “when an individual knows or has reason to know that his request to amend has been denied”); Blazy v. Tenet, 979 F. Supp. 10, 18 (D.D.C. 1997) (citing Englerius and finding that claim for amendment of sexual harassment allegations in personnel file did not begin to run until employee discovered that FBI, where plaintiff had applied for employment, never received corrective letter from CIA, prior to which time plaintiff did not and could not have known of CIA’s failure to amend), summary affirmance granted, No. 97-5330, 1998 WL 315583, at *1 (D.C. Cir. May 12, 1998). But see Campeau v. SSA, 575 F. App’x 35 (3d Cir. 2014) (per curiam) (finding that plaintiff was aware of his alleged injury after knowing SSA received his request and failed to acknowledge receipt “not later than 10 days (excluding [weekends and holidays]) after receipt,” as required by § 552a(d)(2)(A)); Wills v. OPM, No. 93-2079, slip op. at 2-3 (4th Cir. Jan. 28, 1994) (per curiam) (holding that cause of action triggers statute of limitations when plaintiff knows or should have known of alleged violation, which in this case was when plaintiff sent his first letter requesting amendment); Lee v. FBI, 172 F. Supp. 3d 304, 306-07 (D.D.C. 2016) (“Presumably Plaintiff knew or had reason to know that the Electronic Communication contained false or inaccurate information upon receipt of records from the FBI in response to his FOIA request.”); Alexander v. Mich. Adjutant Gen., 860 F. Supp. 2d 448, 456-57 (W.D. Mich. 2012) (ruling that limitations period began when plaintiff was terminated “approximately fifteen years prior to filing this action,” or “[g]iving plaintiff every benefit of the doubt” considering several “other dates that plaintiff could have claimed to have first ‘known,’” under any of which “plaintiff’s complaint would have been untimely”); cf. Foulke v. Potter, No. 10-CV-4061, 2011 WL 127119, at *3 n.4 (E.D.N.Y. Jan. 10, 2011) (holding plaintiff must amend complaint to plead Privacy Act amendment claim, but noting that claim would likely fail “[s]ince the documents which plaintiff seeks to have corrected were created in 2008, and plaintiff was clearly aware of the purported inaccuracies in such documents in 2008” where plaintiff never submitted an amendment request); Reitz v. USDA, No. 08-4131, 2010 WL 786586, at *9-10 (D. Kan. Mar. 4, 2010) (dismissing amendment claim where plaintiffs had not “specifie[d] any date for the alleged Privacy Act violations,” and working back from date of court filing, finding that plaintiffs had “not raised a material question of fact that any Privacy Act violation occurred” within

two years prior); Evans v. United States, No. 99-1268, 2000 WL 1595748, at *2 (D. Kan. Oct. 16, 2000) (finding that “plaintiff neither knew nor had reason to know of the alleged error in his records until the receipt of information provided by those witnesses who claimed the [Equal Opportunity] Complaint Summary inaccurately reported their testimony,” which prompted him to request “reconsideration and reinvestigation” of information). One district court “[found] it troubling that [a plaintiff] was aware of the existence of allegedly incorrect records in 2002, but waited until 2009 to request amendment of his records.” Kursar, 751 F. Supp. 2d at 167 n.11. “Nonetheless, the [c]ourt [was] not aware of any limitations period for seeking an amendment in a statute or otherwise compelled by binding case authority.” Id. (adding that “an equitable defense such as laches may be applicable in this instance” but declining to “consider the defense as it was not raised by” defendant).

Courts generally have held that the agency’s initial denial begins the limitations period, rather than the date of an agency’s administrative appeal determination.

In determining what constitutes the agency’s denial, it has been held that the agency’s initial denial should govern, rather than the date of the agency’s administrative appeal determination. See Quarry v. DOJ, 3 Gov’t Disclosure Serv. (P-H) ¶ 82,407, at 83,020-21 (D.D.C. Feb. 2, 1982); see also Singer v. OPM, No. 83-1095, slip op. at 2 (D.N.J. Mar. 8, 1984) (rejecting claim that limitations period began on date plaintiff’s appeal was dismissed as time-barred under agency regulation); cf. Shannon v. Gen. Elec. Co., 812 F. Supp. 308, 320 & n.10 (N.D.N.Y. 1993) (finding that cause of action for damages claim arose when plaintiff’s amendment request was partially denied and noting that “no caselaw can be found to support a finding that the pendency of the appeal has any affect upon the running of the statute of limitations”).

In cases “[w]here the agency has not issued an express denial of the request, the question [of] when a person learns of the denial requires a factual inquiry and cannot ordinarily be decided on a motion to dismiss.” Englerius, 837 F.2d at 897; see also Jarrell v. USPS, 753 F.2d 1088, 1092 (D.C. Cir. 1985) (holding that issue of material fact existed and therefore summary judgment was inappropriate where agency contended that cause of action arose when it issued final denial of expungement request but requester argued that due to agency’s excision of certain parts of documents, he was unaware of information until later point in time); Conklin v. BOP, 514 F. Supp. 2d 1, 5 (D.D.C. 2007) (denying motion to dismiss as “the date on which plaintiff knew or had reason to know of the

alleged Privacy Act violations is unclear”); Lechliter v. Army, No. 04-814, 2006 WL 462750, at *3-4 (D. Del. Feb. 27, 2006) (denying motion to dismiss because “[t]here does not appear to have been a final denial of [plaintiff’s] request” and “there [was], rather, some question regarding what was said” during a telephone call concerning status of request); cf. Bowles v. BOP, No. 08 CV 9591, 2010 WL 23326, at *3 (S.D.N.Y. Jan. 5, 2010) (stating that where “BOP failed to notify the Plaintiff one way or the other” of action on his administrative appeal, “[t]he troubling failure of the BOP to do their job and respond to Plaintiff’s claim, as well as the Plaintiff’s right to be made aware of these deadlines by those that maintain complete control over him are serious, factual questions that would need to be addressed before the statute of limitations issue could be resolved” but dismissing claim on other grounds without reaching these considerations).

b. Statute of Limitations in Access suits

For Privacy Act access suits, the statute of limitations period begins when the plaintiff knew, or should have known, of an agency’s failure to comply with the Privacy Act’s access provision.

Courts have enforced the statute of limitations against plaintiffs in subsection (g)(1)(B) access lawsuits where the plaintiff did not timely file after he or she knew or should have known of the violation. See Melvin v. SSA, 126 F. Supp. 3d 584, 603 (E.D.N.C. 2015) (finding plaintiff’s access claim untimely because plaintiff was aware of violation, at the latest, when she filed response in prior action stating that agency failed to provide her medical records), aff’d per curiam, 686 F. App’x 230 (4th Cir. 2017); Zied v. Barnhart, 418 F. App’x 109, 113-14 (3d Cir. 2011) (per curiam) (concluding that plaintiff “knew of the agency’s alleged errors when defendant . . . sent her a letter that was unresponsive to her Privacy Act requests and she responded”); Willis v. DOJ, 581 F. Supp. 2d 57, 69 (D.D.C. 2008) (ruling that “[a]pplication of the tolling doctrine is inappropriate in this case” because plaintiff “had sufficient knowledge” to bring action within limitations period); Levant v. Roche, 384 F. Supp. 2d 262, 270 (D.D.C. 2005) (concluding that plaintiff knew or should have known that his access request was denied when Air Force issued final decision on his Privacy Act and FOIA requests for documents); Bernard v. DOD, 362 F. Supp. 2d 272, 278-79 (D.D.C. 2005) (determining that it was “clear from the administrative record that the plaintiff knew or should have known about his ability to request his medical records . . . when he alleged he was denied them in the hospital at that time”); Logan v. United

States, 272 F. Supp. 2d 1182, 1187 (D. Kan. 2003) (finding that plaintiff's access claim was untimely as claim arose "when [the agency] disclosed the records to Plaintiff"); McClain v. DOJ, No. 97-0385, 1999 WL 759505, at *4 (N.D. Ill. Sept. 1, 1999) (finding that action "would have accrued when [plaintiff] knew or should have known that his request for access to his IRS records had been denied," which was more than nine years before he filed suit), aff'd on other grounds, 17 F. App'x 471 (7th Cir. 2001); Biondo v. Navy, 928 F. Supp. 626, 632, 634-35 (D.S.C. 1995) (stating that 1987 request "cannot serve as a basis for relief for a suit brought in 1992 because the Privacy Act has a two-year statute of limitations," and making similar statements as to undocumented requests for information made in mid-80s and in 1976-77), aff'd, 86 F.3d 1148 (4th Cir. 1996) (unpublished table decision); Burkins v. United States, 865 F. Supp. 1480, 1496 (D. Colo. 1994) (holding cause of action "should not be time-barred" because it would have accrued when plaintiff knew his request for access had been denied); Mittleman v. Treasury, 773 F. Supp. 442, 448, 450-51 n.7 (D.D.C. 1991) (holding that plaintiff "cannot attempt to resurrect" claims barred by statute of limitations by making subsequent request more than three years after she had first received information and almost six months after complaint had been filed).

The only judicial discussion of the Supreme Court's Irwin presumption of equitable tolling in the context of an access lawsuit is found in Rouse v. State, 548 F.3d 871, 876-77 (9th Cir. 2008), amended and superseded by 567 F.3d 408 (9th Cir. 2009). Although the opinion was superseded (apparently on mootness grounds, see id. at 411 & n.1), the Ninth Circuit determined that the Irwin rebuttable presumption did not apply to an access claim because it "has no analog in private litigation." 548 F.3d at 877-78.

Although the Privacy Act's two-year statute of limitations applies in subsection (g)(1)(B) access lawsuits, the FOIA's 6-year statute of limitations applies to the same access requests processed under FOIA. See Spannaus v. DOJ, 824 F.2d 52, 55-56 (D.C. Cir. 1987) (concluding that 28 U.S.C. § 2401(a)'s six-year statute of limitations applies to FOIA actions), overruled on other grounds by Jackson v. Modly, 949 F.3d 763, 778 (D.C. Cir. 2020) (holding "that § 2401(a)'s time bar is nonjurisdictional and . . . [o]ur decisions to the contrary, see, e.g., Spannaus, 824 F.2d at 55, are thus overruled."), petition for cert. filed (July 10, 2020) (No. 20-19); FOIA Guide, Litigation Considerations at 13, <https://www.justice.gov/oip/doj-guide-freedom-information-act-0> (recognizing six-year statute of limitations); see also H.R. Rep. No. 98-726, pt. 2, at 16-17 (1984), reprinted

in 1984 U.S.C.C.A.N. 3741, 3790-91 (noting amendment of Privacy Act in 1984 to include subsection (t)(2) and stating: “Agencies that had made it a practice to treat a request made under either [the Privacy Act or the FOIA] as if the request were made under both laws should continue to do so.”).

c. Statute of Limitations in Damages claims

For Privacy Act damages suits, the statute of limitations period begins when the plaintiff knew, or should have known, of an agency’s violation of the Privacy Act.

In damages claims, courts have deemed the statute of limitations to begin running at the time the plaintiff knew or should have known of the agencies Privacy Act violation. See, e.g., Chichakli v. Tillerson, 882 F.3d 229, 234 (D.C. Cir. 2018); Powell v. Donahoe, 519 F. App’x 21, 23 (2d Cir. 2013) (finding cause of action accrued when plaintiff “had actual knowledge of the release of his records”); Jackson v. Shinseki, 526 F. App’x 814, 816 (10th Cir. 2013) (holding improper disclosure claims were untimely as “Plaintiff was admittedly aware of these disclosures when his wife ‘filed his military psychiatric records in a state divorce action’”); Burnam v. Marberry, 313 F. App’x 455, 456 (3d Cir. 2009) (per curiam) (“cause of action under the Privacy Act arises when the individual either knew or had reason to know of the alleged error in maintaining the individual’s records and the individual was harmed by the alleged error.”); Shehee v. DEA, No. 05-5276, 2006 U.S. App. LEXIS 15586, at *2 (D.C. Cir. June 14, 2006) (per curiam); Duncan v. EPA, 89 F. App’x 635, 635 (9th Cir. 2004); Williams v. Reno, No. 95-5155, 1996 WL 460093, at *1 (D.C. Cir. Aug. 7, 1996) (per curiam); Tijerina v. Walters, 821 F.2d 789, 797-98 (D.C. Cir. 1987); Smith v. United States, 142 F. App’x 209, 210 (5th Cir. 2005) (per curiam) (affirming that “under section 552a(g)(5) of the Privacy Act, . . . a cause of action accrues when the plaintiff knew or should have known of the alleged violation”); Green v. Westphal, 94 F. App’x 902, 904 (3d Cir. 2004) (“A cause of action arises under the Privacy Act when the individual knows or has reason to know of the alleged error in the individual’s record and the individual is harmed by the alleged error.”); Bergman v. United States, 751 F.2d 314, 316-17 (10th Cir. 1984) (holding that limitations period for damages action under subsection (g)(1)(C) commences at time three conditions are met: (1) an error was made in maintaining plaintiff’s records; (2) plaintiff was wronged by such error; and (3) plaintiff either knew or had reason to know of such error); Gonzalez, 2018 WL 7825025, at *5 (finding that plaintiff “pled with adequate plausibility that due to the Agencies’ improper management of records and misleading communications to third parties, Plaintiff was

denied credit in December 2016 in violation of the Privacy Act, well within the Act's two-year limitations period"); Conway v. Pompeo, No. 1:16-cv-1087, 2018 WL 8800525, at *6-7 (E.D. Va. Sept. 17, 2018) (finding plaintiff's claim untimely because she knew of alleged violation, at the latest, when she filed second EEO grievance concerning "purported misprocessing of her retirement"), aff'd per curiam sub nom. Conway v. Haspel, 773 F. App'x 693 (4th Cir. 2019); Ashbourne v. Hansberry, 302 F. Supp. 3d 338, 347-48 (D.D.C. 2018) (denying motion to dismiss on statute of limitations grounds where defendants failed to "point to any specific allegation in the complaint that is timebarred"); Ricks v. United States, No. 17-cv-1016, 2018 WL 454455, at *5 (S.D. Cal. Jan. 17, 2018) (finding that plaintiff became aware of agency's disclosure of his medical and private information outside of the limitations period); Sabatini v. Price, No. 17-cv-1597, 2018 WL 1449416, at *3 (S.D. Cal. Jan. 16, 2018) (inferring that plaintiff knew of the alleged violations in early 2013 because February 2013 letter indicated that plaintiff retained counsel regarding request for removal of report); Carter, 2017 WL 2271416, at *11 (holding statute of limitations began to run when plaintiff discovered entry of allegedly false entry in his medical history); Jagun v. Rodriguez, 2016 WL 4124225, at *8; Gonzalez-Lora v. DOJ, 169 F. Supp. 3d 46, 53 (D.D.C. 2016) (stating that "even if res judicata and collateral estoppel do not bar plaintiff's claim, . . . allege[d] violations of . . . the Privacy Act arising from the DEA's response to the 2000 FOIA request" are outside the two-year statute of limitations); Agelli v. Burwell, 164 F. Supp. 3d 69, 75-76 (D.D.C. 2016) (finding that limitations period began when plaintiff received email from agency on October 2, 2014, the date of inquiry notice, rather than on the date she claimed to have first read the email); Marley v. Donahue, 133 F. Supp. 3d 706, 718 (D.N.J. 2015) (finding that, although complaint did not provide basis for Privacy Act claim or identify improperly disclosed record, Privacy Act claim was untimely even if agency disclosed record on date of plaintiff's resignation); Melvin, 126 F. Supp. 3d at 603 (finding plaintiff's claims regarding false statements in evaluation accrued when she received a copy of the evaluation); Jarrell v. McDonald, No. 3:15-cv-187, 2015 WL 4720607, at *3-4 (S.D. Ohio Aug. 7, 2015) (finding plaintiff knew of errors in his military personnel file more than two years before filing where plaintiff had previously filed lawsuits relating to the records); Gibson v. Holder, No. 3:14cv641, 2015 WL 5635125, at *7 (magistrate's recommendation) (finding that Privacy Act claims filed in 2014 were time-barred based on allegations in complaint that, in 1999, plaintiff obtained documents in his security investigation file that he described as "'full of outright lies, blatant distortions of facts, . . . and a host of other irregularities'"), adopted, 2015 WL 5634596 (N.D. Fla. Sept. 23, 2015);

Green v. Probation Office, No. 1:14 CV 2265, 2015 WL 2129521, at *2-3 (N.D. Ohio May 5, 2015) (finding “clearly plaintiff knew or had reason to know of the alleged violation as of 1995” when plaintiff sent letters and received response stating that presentence report could not be amended after the final version was filed with the court); Atkins v. Mabus, No. 12CV1390, 2014 WL 2705204, at *3-5 (S.D. Cal. June 13, 2014) (discussing statute of limitations for various claims of “inappropriate safeguards” to protect confidentiality of plaintiff’s medical condition and improper disclosure), rev’d and remanded on other grounds, 654 F. App’x 878 (9th Cir. 2016); Jarrell v. Nat’l Pers. Recs. Ctr., No. 3:11cv00434, 2013 WL 5346483, at *8-9 (recommending defendant’s summary judgment motion be granted as plaintiff’s claims were time-barred; “Because [plaintiff] raised his record-tampering allegations and claims in his June 1994 Complaint, there is no genuine dispute that by June 1994, [plaintiff] knew, or had reason to know, about the alleged records tampering of which he now complains.”) (magistrate’s recommendation), adopted, 2013 WL 5773930 (S.D. Ohio Oct. 24, 2013); Brockway v. VA Conn. Healthcare Sys., No. 3:10-CV-719, 2012 WL 2154263, at *13-14 (D. Conn. June 13, 2012) (dismissing claim as time-barred as plaintiff “was [] on notice that a possible disclosure of his VA medical records had occurred” when “a non-VA doctor” called “asking if [plaintiff] would like to receive psychotherapy from him” “well outside the requisite two-year statute of limitations”); Toolasprashad v. BOP, No. 09-0317, 2009 WL 3163068, at *2 (D.D.C. Sept. 29, 2009) (finding Privacy Act claim time-barred because plaintiff filed it more than two years after final agency action); cf. Bowyer v. Air Force, 875 F.2d 632, 636 (7th Cir. 1989) (applying stricter standard and holding that the limitations period begins to run when “plaintiff first knew or had reason to know that the private records were being maintained” (quoting Diliberti v. United States, 817 F.2d 1259, 1262-64 (7th Cir. 1987)); Brunotte v. Johnson, 892 F. Supp. 2d 199, 206 (D.D.C. 2012) (explaining that because “Plaintiff became aware of the email disclosure [on March 10, 2006]; and, regardless of whether she knew or should have known that the email was disseminated to [others] in addition to the [individuals she was aware of], Plaintiff attained the necessary knowledge of an alleged Privacy Act violation on that date”); Leibenguth v. United States, No. 08-CV-6008, 2009 WL 3165846, at *3 (W.D.N.Y. Sept. 29, 2009) (concluding that plaintiff’s claim for damages “based on the VA’s failure to disclose his medical records in a timely fashion” was time-barred because he filed it more than two years after he became aware of denial of his claim for disability benefits).

Some courts have held that once the plaintiff knows or has reason to know of a record's existence, even if based upon hearsay or rumors, the plaintiff has a "duty to inquire" into the matter – i.e., "two years from that time to investigate whether sufficient factual and legal bases existed for bringing suit." See Bowyer, 875 F.2d at 637; see also Diliberti, 817 F.2d at 1263-64 (stating that "[t]he hearsay and rumors which the plaintiff described in his affidavit were enough to put him on notice . . . and to impose upon him a duty to inquire into the veracity of those rumors"); Mangino, 818 F. Supp. at 1438 (quoting Diliberti).

Generally, the plaintiff knows or has reason to know of records in violation of the Privacy Act when the plaintiff suspects there is a violation rather than when the plaintiff actually possesses those records or when the government creates those records. See Diliberti, 817 F.2d at 1262 (stating that "relevant fact is not when the plaintiff first had physical possession of the particular records, but rather when he first knew of the existence of the records"); see also Duncan, 89 F. App'x at 636 (reasoning that "a certainty, or testimony under oath, is not required to begin the running of the limitations period, but rather 'what a reasonable person should have known'" (quoting Rose v. United States, 905 F.2d 1257, 1259 (9th Cir. 1990))).

Generally, constructive notice of the possible violation triggers the statute of limitations for damages claims.

If the plaintiff has constructive notice of the possible violation, the statute of limitations is triggered. See Diliberti, at 1262-63; see also Bowyer, 875 F.2d at 636 (stating that when agency employee confirmed that agency maintained private records on plaintiff relating to previous conflict with his supervisor, he had sufficient notice of possibly erroneous records). In the context of a damages action for wrongful disclosure, the D.C. Circuit rejected the government's argument that the limitations period commenced when the contested disclosure occurred, and observed that such an unauthorized disclosure "is unlikely to come to the subject's attention until it affects him adversely, if then." Tijerina, 821 F.2d at 797. But cf. Hill v. N.Y. Post, No. 08 Civ. 5777, 2010 WL 2985906, at *3 (S.D.N.Y. July 29, 2010) (explaining that claim brought "against the unnamed BOP staff for revealing private information regarding [plaintiff] contained in his records . . . accrued . . . upon the publication of the articles describing [plaintiff's] affair").

Consistent with the constructive notice theory, other courts have similarly found that the statute of limitations began to run where the evidence or circumstances indicated that the plaintiff knew of the violation or had been affected by it. See Jackson v. Shinseki, 526 F. App'x at 817 (holding that plaintiff was put "on notice of his ... claim, that Defendants failed to maintain his medical records in a way to ensure the fairness of his discharge" when defendant informed him that agency did not "'have a copy of [the] psychiatric evaluation' from his private psychiatrist that led to his ability to return to work"); Zied, 418 F. App'x at 113-14 (ruling that plaintiff "knew of the harm caused by" alleged inaccuracies in her SSA records, at the very latest, "when her eligible child benefits were stopped"); Lockett v. Potter, 259 F. App'x 784, 787 (6th Cir. 2008) ("EEOC hearings that took place in March 2002 and April 2003, which addressed [plaintiff's] complaints that the Postal Service's manner of storing and disseminating his records violated the Privacy Act . . . demonstrate that he knew about the alleged Privacy Act violation more than two years before his March 2006 filing of his complaint."); Harrell, 285 F.3d at 1293-94 (finding that the "limitations period began to run when [plaintiff] first became aware of the alleged errors in his presentence investigation reports" and that it was not "extended either by the government's subsequent actions or by his receipt of documents allegedly corroborating his assertions of error"); Weber v. Henderson, 33 F. App'x at 612 (finding plaintiff "knew that the entire file had been lost . . . when he was informed by the defendants in writing that the record had been misplaced"); Seldowitz v. OIG of State, 238 F.3d 414, at *3 (4th Cir. 2000) (per curiam) (unpublished table case) (following Tijerina and finding that statute of limitations began to run when plaintiff "had actual knowledge of the alleged error," even though he did not possess copy of them to make side-by-side comparison with annotated ones); Todd v. Holder, 872 F. Supp. 2d 1284, 1291 (N.D. Ala. 2012) (stating that [plaintiff] filed this action . . . approximately three and a half years after" alleged claims of wrongful disclosures to Office of Inspector General); Doe v. FDIC, No. 11 Civ. 307, 2012 WL 612461, at *5 (S.D.N.Y. Feb. 27, 2012) (dismissing claims for unlawful disclosure as time-barred where plaintiff had sent e-mail to her supervisor more than two years before filing suit in which she stated that agency had disclosed her medical information in possible violation of Privacy Act); Shearson, 865 F. Supp. 2d at 869 (concluding that "filings in [that case] demonstrate that Plaintiff should have known of alleged violations" at that time where plaintiff had submitted brief in prior case); Bailey v. Fulwood, 780 F. Supp. 2d 20, 27-28 (D.D.C. 2011) (concluding that plaintiff knew or should have known that agency had relied on a "subsequently dismissed" warrant in determining whether to grant him

parole when plaintiff received “denial notice” that “specifically informed Plaintiff that [the agency’s] decision was partially based on” that warrant); Jones v. BOP, No. 5:09-cv-216, 2011 WL 554080, at *2 (S.D. Miss. Feb. 7, 2011) (reasoning that federal prisoner “must have known no later than 2006 that his [presentence investigation report] included the [disputed] charge” because “he began pursuing his administrative remedies with respect to the [report] in 2006”); Ramey v. USMS, 755 F. Supp. 2d 88, 97-98 (D.D.C. 2010) (dismissing as time-barred claim alleging violation of subsection (e)(7) “to the extent [it] encompasses the Defendant’s collection and maintenance of information regarding [contractor’s] 2003 investigation” of plaintiff, during which plaintiff was interviewed by contractor); Kursar, 751 F. Supp. 2d at 167-68 (“[P]laintiff knew, or should have known, of the purported inaccuracies by as early as April 25, 2002,” because he “received notification on April 25, 2002, that the TSA intended to terminate him for ‘submitting false or incorrect information on his employment application and Standard Form 86’” and because he “acknowledged receipt of this [notification]”); Reitz v. USDA, No. 08-4131, 2010 WL 786586, at *9, *11 (D. Kan. Mar. 4, 2010) (dismissing claims filed in 2008 because “[m]ost of the plaintiffs’ letters in the record allege continuing ill effects from [Privacy Act] violations occurring in 1997 or other dates before 2006”); Gard v. Dep’t of Educ., 691 F. Supp. 2d 93, 99 (D.D.C. 2010) (finding that plaintiff “became aware of the alleged violation” when he “expressed his belief that his . . . records had been destroyed in a declaration to the U.S. Office of Special Counsel”), summary affirmance granted per curiam, No. 11-5020, 2011 WL 2148585 (D.C. Cir. May 25, 2011); Ramirez v. DOJ, 594 F. Supp. 2d 58, 62-64 (D.D.C. 2009) (dismissing complaint filed in 2007 as time-barred because in 2004 plaintiff “notified the prosecutors, the probation officer, and the presiding judge at sentencing of inaccuracies in the [presentence investigation report]”), aff’d per curiam on other grounds, No. 10-5016, 2010 WL 4340408 (D.C. Cir. Oct. 19, 2010); Sims v. New, No. 08-cv-00794, 2009 WL 3234225, at *4 (D. Colo. Sept. 30, 2009) (concluding that clock began in April 2002 even though plaintiff did not receive letter containing inaccuracy until December 2005, where plaintiff learned of inaccuracy in April 2002 and was informed shortly thereafter that the inaccuracy was the basis for adverse determination); Joseph v. Cole, No. 5:07-CV-225, 2007 WL 2480171, at *2 (M.D. Ga. Aug. 27, 2007) (barring accuracy lawsuit where plaintiff inmate admitted that he knew of errors in his presentence report when it was adopted by court thirteen years prior to filing of suit); Ingram v. Gonzales, 501 F. Supp. 2d 180, 184-85 (D.D.C. 2007) (finding that prisoner’s claim accrued “when he discovered that the erroneous career offender finding [in his presentence report] was being used by BOP

to determine his custody classification,” not at time of his sentencing); Counce v. Nicholson, No. 3:06cv00171, 2007 WL 1191013, at *14-15 (M.D. Tenn. Apr. 18, 2007) (barring subsection (b)/(g)(1)(D) claim where plaintiff first complained of Privacy Act violations to EEO counselor in November 2003 but did not file suit until February 2006); Kenney v. Barnhart, No. 05-426, 2006 WL 2092607, at *11-12 (C.D. Cal. July 26, 2006) (finding claim untimely because plaintiff filed it more than two years after he complained to SSA of inaccuracies in his credit reports, which were allegedly based on inaccuracies in SSA records); Peterson v. Tomaselli, No. 02 Civ. 6325, 2003 WL 22213125, at *8 (S.D.N.Y. Sept. 29, 2003) (finding that plaintiff’s claim arose when he “knew that the false documents existed”); Fort Hall Landowners All., Inc., No. 99-052, slip op. at 5 (finding that plaintiffs’ “claim accrued as soon as Plaintiffs either were aware, or should have been aware, of the existence of and source of injury, not when the Plaintiffs knew or should have known that the injury constituted a legal wrong”); Farrero, 180 F. Supp. 2d at 97 (finding that plaintiff should have known of potential violation when agency specifically informed him that it was maintaining certain documents regarding his alleged misconduct); Walker v. Ashcroft, No. 99-2385, 2001 U.S. Dist. LEXIS 27213, at *17 (D.D.C. Apr. 30, 2001) (“Contrary to Plaintiffs’ contention, the record establishes that Plaintiffs were aware of the FBI’s actions well before they received this report.”), summary affirmance granted per curiam, No. 01-5222, 2002 U.S. App. LEXIS 2485 (D.C. Cir. Jan. 25, 2002); Villescas v. Richardson, 124 F. Supp. 2d 647, 659 (D. Colo. 2000) (finding the statute of limitations began to run when plaintiff received declaration in another lawsuit describing disclosure of records, even though he did not receive actual documents); Armstrong v. BOP, 976 F. Supp. 17, 21-22 (D.D.C. 1997) (following Tijerina and finding plaintiff’s claim barred by statute of limitations where plaintiff had written letter more than two and one-half years earlier indicating that her prison file was lacking favorable information), summary affirmance granted per curiam, No. 97-5208, 1998 WL 65543 (D.C. Cir. Jan. 30, 1998); Nwangoro v. Army, 952 F. Supp. 394, 397-98 (N.D. Tex. 1996) (“[T]he limitations period commences not when the plaintiff first obtains possession of the particular records at issue, but rather when he first knew of their existence.”); Brown v. VA, No. 94-1119, 1996 WL 263636, at *1-2 (D.D.C. May 15, 1996) (holding Privacy Act claim barred by statute of limitations because plaintiff “knew or should have known that the Privacy Act may have been violated” when he submitted federal tort claim to VA concerning same matter “over two and a half years” before suit filed); Gordon v. DOJ, No. 94-2636, 1995 WL 472360, at *2 (D.D.C. Aug. 3, 1995) (finding statute of limitations ran from time of plaintiff’s

receipt of letter from sentencing judge rejecting information contained in presentencing report, at which point plaintiff “knew or . . . should have known what became inaccuracies in his presentencing report”); Rice v. Quinlan, No. 94-1519, slip op. at 2-3 & n.1 (D.D.C. Dec. 30, 1994) (holding plaintiff knew of contents of presentence report at time he filed “Objection to Presentence Investigation Report,” at which time statute of limitations began to run), summary affirmance granted per curiam sub nom. Rice v. Hawk, No. 95-5027, 1995 WL 551148 (D.C. Cir. Aug. 2, 1995); Szymanski, 870 F. Supp. at 378-79 (citing Bergman and Tijerina, and stating that “[b]ecause plaintiff was given the opportunity to review the documents he now maintains contain incorrect information and waived that opportunity, the Court finds that he should have known about any errors at the time of this waiver” but that, additionally, plaintiff had complained about same information in his appeal to Parole Commission more than two years previously); Malewich v. USPS, No. 91-4871, slip op. at 21-22 (D.N.J. Apr. 14, 1993) (finding statute began to run when plaintiff was aware that file was being used in investigation of plaintiff and when he was notified of proposed termination of employment), aff’d, 27 F.3d 557 (3d Cir. 1994) (unpublished table decision); Mangino, 818 F. Supp. at 1437-38 (applying Bergman, Bowyer, and Diliberti, and finding that cause of action accrued on date of letter in which plaintiff indicated knowledge of records being used by agency as basis for revoking his security clearance, rather than upon his receipt of records); Ertell v. Army, 626 F. Supp. 903, 908 (C.D. Ill. 1986) (finding limitations period commenced when plaintiff “knew . . . that there had been negative evaluations in his file which ‘may explain why he is not being selected;’” rather than upon actual discovery of such records); cf. Doe v. NSA, No. 97-2650, 1998 WL 743665, at *1-3 (4th Cir. Oct. 23, 1998) (per curiam) (citing Rose and Diliberti, and holding that appellant’s wrongful disclosure claim was time-barred because in accordance with principles of agency law, Privacy Act action accrued from time her attorney received her records).

Some courts, however, have construed the beginning of the statute of limitations period from other points, including when an individual discovers the inaccuracy or mishandling of the record, receives a Privacy Act notice, or becomes aware that an apparently untimely complaint “relates back” to a timely one.

In contrast to the constructive notice theory adopted by many courts, some courts have suggested that the limitations period for a subsection (g)(1)(C) damages action would commence when a plaintiff actually receives his record – i.e., when he actually discovers the inaccuracy. See Akutowicz v. United States, 859 F.2d 1122, 1126 (2d Cir. 1988) (noting that

“the latest possible time before which [plaintiff] could commence his suit was . . . two years after his discovery of the alleged misrepresentation in his record (i.e., the date when he received a copy of his record from the Department of State”); see also Rose v. United States, 905 F.2d 1257, 1259 (9th Cir. 1990) (holding that subsection (g)(1)(C) action accrued when plaintiff “became aware of the alleged mishandling of her records on . . . the date she received copy of her compensation file”); Lepkowski v. Treasury, 804 F.2d 1310, 1322-23 (D.C. Cir. 1986) (Robinson, J., concurring) (holding that subsection (g)(1)(C) action “accrued no later than the date upon which [plaintiff] received IRS’ letter . . . apprising him of destruction of the photographs and associated workpapers”); Middlebrooks v. Mabus, No. 1:11cv46, 2011 WL 4478686, at *4-5 (E.D. Va. Sept. 23, 2011) (finding that plaintiff “first learned of the alleged inaccuracies in her personnel record on . . . the date she received the Notice of her termination,” which “contained extensive factual recitals of the specific grounds for plaintiff’s termination”); Ciralsky v. CIA, 689 F. Supp. 2d 141, 158 (D.D.C. 2010) (concluding that statute of limitations “was triggered . . . when the CIA passed the [memorandum] and investigative file to Plaintiff” where claim was “based in whole or in part on the information contained in those documents”); Off v. U.S. Gov’ts, No. 2:09-CV-01525, 2010 WL 3862097, at *3 (D. Nev. Sept. 27, 2010) (“Because Plaintiff attached the SF-50 to at least one of the complaints he filed on November 12, 1998, Plaintiff knew or had reason to know of the allegedly incorrect SF-50 at that time.”), aff’d 472 F. App’x 789 (9th Cir. 2012); Brooks v. BOP, No. 04-0055, 2005 WL 623229, at *2 (D.D.C. Mar. 17, 2005) (barring claim where plaintiff inmate “has known of incorrect information in BOP records pertaining to him” since he received response from regional director, which “incorrectly stated that plaintiff had been found to have committed the more serious offense,” but plaintiff did not file suit until four years later); Harry v. USPS, 867 F. Supp. 1199, 1205 (M.D. Pa. 1994) (finding that although exact date when plaintiff should have known about alleged improper file maintenance was unclear, date of actual discovery was “sterling clear” – when plaintiff physically reviewed his files), aff’d, 60 F.3d 815 (3d Cir. 1995) (unpublished table decision); Shannon, 812 F. Supp. at 319-20 (finding causes of action arose when plaintiff learned of wrongs allegedly committed against him which was when he received documents that were allegedly inaccurate or wrongfully maintained); cf. Steele v. Cochran, No. 95-35373, 1996 WL 285651, at *1 (9th Cir. May 29, 1996) (citing Rose and holding that Privacy Act claim filed in 1994 was time-barred because plaintiff wrote letter to agency questioning validity of information disclosed to State Bar in 1991 and was formally informed by State Bar that he was denied admission in 1991).

One district court decision has also considered the statute of limitations in connection with a Privacy Act claim under subsection (e)(3) concerning the collection of information from individuals. Darby v. Jensen, No. 94-S-569, 1995 U.S. Dist. LEXIS 7007, at *7-8 (D. Colo. May 15, 1995), aff'd 78 F.3d 597 (10th Cir. 1996) (unpublished table decision). In that case, the court determined that the claim was time-barred, as more than two years had passed since the date upon which the plaintiff had received the request for information. Id.

Several courts have considered whether a Privacy Act claim not apparently raised in the initial complaint filed within the limitations period could be found to “relate back” to the date of that earlier complaint under Rule 15(c) of the Federal Rules of Civil Procedure. See Oja v. Army Corps of Eng’rs, 440 F.3d 1122, 1134-35 (9th Cir. 2006) (holding that amended complaint did not relate back to filing date of initial complaint because “[t]he fact that the language in the two disclosures is identical is inapposite because [plaintiff’s] claims . . . are based on the acts of disclosure themselves, each of which is distinct in time and place” where agency posted information pertaining to plaintiff on website in November 2000 and posted same information on second website in December 2000); Freeman v. EPA, No. 02-0387, 2004 WL 2451409, at *8-9 (D.D.C. Oct. 25, 2004) (concluding that even though “the new claim is similar in that it also involves disclosure of information . . . it is hardly conceivable that the defendants would have had notice regarding the new” claim, nor “does the new claim build on facts the plaintiffs previously alleged other than the very general factual context of the case,” and therefore, the claim fails to relate back); Fort Hall Landowners All., Inc., No. 99-052, slip op. at 13-15 (finding that Privacy Act wrongful disclosure claims first brought in amended and second amended complaints related back to original complaint); Tripp v. DOD, 219 F. Supp. 2d 85, 91-92 (D.D.C. 2002) (holding that plaintiff’s subsequent Privacy Act accounting claim was not barred by two-year statute of limitations because claim arose “out of the same conduct and occurrences alleged in the initial Complaint,” which dealt with improper disclosures of Privacy Act-protected records); cf. Yee v. Solis, No. C 08-4259, 2009 WL 5064980, at *2 (N.D. Cal. Dec. 23, 2009) (rejecting argument that motion for leave to amend complaint to add Privacy Act claim “should be denied because the proposed claim does not ‘relate [] back’ to plaintiff’s original claims” on ground that defendant “does not contend, let alone demonstrate, such additional claim is, in the absence of relation back, time-barred”), aff’d on other grounds, 472 F. App’x 471 (9th Cir. 2012).

d. Equitable Tolling of and Exceptions to Statute of Limitations

Equitable tolling applies in damages claims.

As discussed above, the D.C. Circuit has held that the rebuttable presumption in favor of equitable tolling that was established in Irwin applies to the Privacy Act's statute of limitations for a damages claim for unlawful disclosure. Chung v. DOJ, 333 F.3d 273, 276-77 (D.C. Cir. 2003). Further, because the D.C. Circuit could find no reason to think that Congress did not intend to equitably toll the Privacy Act's statute of limitations, it held that the government did not overcome this presumption. Id. at 278.

For other cases involving equitable tolling, see Hammoud v. U.S. Att'y, No. 14-14398, 2015 WL 4756582, at *5 (E.D. Mich. Aug. 12, 2015 (holding equitable tolling not appropriate when statute of limitations ran in 2009 and plaintiff's equitable tolling argument was based on attempts to contact agencies no earlier than 2012)); Grethen v. Clarke, No. 2:13cv416, 2015 WL 3452020, at *2 (E.D. Va. March 13, 2015) (finding that plaintiff's Privacy Act claim should not be tolled because pendency of plaintiff's habeas action did not impact plaintiff's Privacy Act claim); Boyd, 932 F. Supp. 2d at 838-840 (stating Sixth Circuit's five factors for determining whether equitable tolling applies: "(1) lack of notice of the filing requirement; (2) lack of constructive knowledge of the filing requirement; (3) diligence in pursuing one's rights; (4) absence of prejudice to the defendant; and (5) the plaintiff's reasonableness in remaining ignorant of the particular legal requirement"; finding "[t]here is no question that [plaintiff's] claim in this Court was brought outside the Privacy Act statute of limitations. Since the Court finds four of the five equitable tolling factors favor equitable tolling . . . and that the fifth does not weigh significantly against it, [plaintiff's] suit is not barred by the statute of limitations"); Padilla-Ruiz v. United States, 893 F. Supp. 2d 301, 306-09 (D.P.R. 2012) (finding equitable tolling "not a proper remedy to be employed in this case" as plaintiff "makes no connection . . . between his request of documents and the requirement that he needed to file suit [within time period]"), aff'd in part, vacated in part, & remanded on other grounds, 593 F. App'x 1 (5th Cir. 2015); Doe v. Winter, No. 1:04-CV-2170, 2007 WL 1074206, at *10-11 (M.D. Pa. Apr. 5, 2007) (noting that equitable tolling doctrine has been recognized by Third Circuit but finding that plaintiff failed to provide evidence for its application); Cannon-Harper v. U.S. Postmaster Gen., No. 06-10520, 2006 WL 2975492, at *1 (E.D. Mich. Oct. 17, 2006) (declining to apply equitable tolling to statute of limitations

for subsection (b)/(g)(1)(C) claim where plaintiff had initially filed claim in state court); Cooper v. BOP, No. 02-1844, 2006 WL 751341, at *3 (D.D.C. Mar. 23, 2006) (applying equitable tolling where court had sealed inmate’s presentence report because he “was unable to obtain vital information on the existence of his claim until he could review the [report]”); Freeman v. EPA, 2004 WL 2451409, at *9 (concluding that plaintiffs’ argument that they needed additional discovery to support their claim was “insufficient justification for this court to countenance any equitable adjustment to the statute of limitations”); Fort Hall Landowners All., Inc., No. 99-052, slip op. at 7 (holding that statute of limitations was not tolled based on facts before court).

An exception to the two-year statute of limitations rule occurs when there is a material and willful misrepresentation by an agency.

In addition, the statute’s own terms provide an exception to the requirement that an action be brought within two years from when the cause of action arose. 5 U.S.C. § 552a(g)(5). When an agency materially and willfully misrepresents information required by the statute to be disclosed to an individual, and the information so represented is material to establishing the liability of the agency, then the limitations period runs from the date upon which the plaintiff discovers the misrepresentation. Id.; see also Ciralsky, 689 F. Supp. 2d at 154 (finding where plaintiff argued that “by allegedly denying [the plaintiff’s] request . . . for pertinent information confirming his suspicion . . . the CIA committed a material and willful misrepresentation of information required to be disclosed to Plaintiff and material to establishing the liability of the Agency to him. . . . Taking the factual allegations of the complaint as true, such misrepresentation delays the start of the limitations period.”); Lacey v. United States, 74 F. Supp. 2d 13, 15-16 (D.D.C. 1999) (concluding that defendants made material and willful misrepresentations to plaintiffs by telling them that they lacked evidence and should wait for agency to finish its own investigation of claim before bringing suit, which tolled statute of limitations until agency “confirmed that there was substance to plaintiffs’ claim of violations”); Burkins, 865 F. Supp. at 1496 (“Accepting Plaintiff’s claims of agency misrepresentation as true, the statute may have been tolled.”); Pope v. Bond, 641 F. Supp. 489, 500 (D.D.C. 1986) (holding that FAA’s actions constituted willful and material representation because of its repeated denials of plaintiff’s request for access, which “prevents the statute of limitations from running until the misrepresentation is discovered”); cf. Sabatini v. Price, No. 17-cv-01597, 2018 WL 1638258, at *4 (S.D. Cal. April 5, 2018) (finding no “exceptional

circumstances” existed for exception for material and willful misrepresentations), aff’d sub nom. Sabatini v. Azar, 749 F. App’x 588 (9th Cir. 2019); United States v. Swecker, No. 4:09-cv-00013, 2015 WL 13309238, at *3-4 (S.D. Iowa Dec. 15, 2015) (finding defendants’ counterclaims of material and willful misrepresentation were undermined by the fact that the record contains forms signed by one of the defendants, and such defendant “cannot now claim that [she] was uninformed, or misled, about her Privacy Act Rights, when the form containing a statement of the agency’s Privacy Act policy was signed by [her] three separate times”); Weber, 33 F. App’x at 612 (finding that even if court were to consider claim not properly raised on appeal, “[t]here is no evidence in the record to show that the failure to disclose [a memorandum that plaintiff claims would have avoided much of the pending litigation] was the result of willful misrepresentation”); Boyd, 932 F. Supp. 2d at 836 (“Even accepting. . . that [agency] did ‘willfully and materially misrepresent’ facts regarding the statute of limitations for [plaintiff’s] Privacy Act claim, such a claim remains outside the Privacy Act’s statute of limitations exception”; “In order for the exception to apply, the undisclosed information must be material to the establishment of liability under the Act.”); Sims v. New, 2009 WL 3234225, at *4-5 (concluding that “[e]ven if Defendants concealed the actual contents of the [letter at issue] from Plaintiffs [for more than three years], Defendants did not fraudulently conceal the facts giving rise to Plaintiffs’ claims” because plaintiff knew of inaccuracy contained in letter when he requested it); Leibenguth, 2009 WL 3165846, at *3 (“Because the alleged misrepresentation was made with respect to when a rehearing would be held, and did not pertain to information required to be disclosed under the Privacy Act, plaintiffs have failed to establish that the alternative statute of limitations period applies.”); Mudd v. Army, No. 2:05-cv-137, 2007 WL 4358262, at *7 (M.D. Fla. Dec. 10, 2007) (concluding that plaintiff failed to establish that “information allegedly undermining the accuracy of the [record] was materially and willfully misrepresented by the [agency], or that it was information required under the Privacy Act to be disclosed to plaintiff, or that the allegedly misrepresented information was material to establishment of the liability”); Doe v. Thompson, 332 F. Supp. 2d 124, 134 (D.D.C. 2004) (finding no material and willful misrepresentation where agency “notified the plaintiff about the record and its contents . . . when the record was first created” and “changed the record twice [at plaintiff’s request] in an effort to produce an accurate record”); Marin v. DOD, No. 95-2175, 1998 WL 779101, at *1-2 (D.D.C. Oct. 23, 1998) (denying defendants’ motion to dismiss on ground that claim was time-barred and accepting plaintiff’s claim regarding timing of agency misrepresentation), summary affirmance granted, No.

99-5102, 1999 WL 1006404 (D.C. Cir. Oct. 8, 1999) (per curiam); Munson, No. 96-CV-70920-DT, slip op. at 4-5 (E.D. Mich. July 2, 1996) (finding statement that agency could find no record of disclosure of report to state police but that it would check further “does not provide any evidence of a willful and material misrepresentation”).

Note that the Seventh Circuit has stated that this special relief provision is necessarily incorporated into tests, such as the one set forth in Bergman, which focus on when a plaintiff first knew or had reason to know of an error in maintaining the plaintiff’s records. Diliberti, 817 F.2d at 1262 n.1; see also Malewich, No. 91-4871, slip op. at 25-27 (D.N.J. Apr. 14, 1993) (following Diliberti and precluding “the plaintiff from utilizing the discovery rule as a basis for extending the permissible filing date”). The government argued to the D.C. Circuit in Tijerina v. Walters that subsection (g)(5) “makes sense only if Congress intended the normal statutory period to commence at the time of the alleged violation, regardless of whether the potential plaintiff is or should be aware of the agency’s action.” See 821 F.2d at 797-98. The D.C. Circuit, however, rejected that argument and stated:

[T]he clause providing for a more liberal limitations period in cases of willful misrepresentation of material information . . . extends the normal limitations period in order to ensure that the government cannot escape liability by purposefully misrepresenting information . . . In such cases, the Act allows the period to commence upon actual discovery of the misrepresentation, whereas . . . for other actions under the Act, the period begins when the plaintiff knew or should have known of the violation. . . . [This] in no way affects the special treatment Congress provided for the particularly egregious cases of government misconduct singled out in the Act’s statute of limitations.

Id. at 798.

Continuing violations generally do not toll the statute of limitations period.

Additionally, it has been held that “[a] Privacy Act claim is not tolled by continuing violations.” Davis v. DOJ, 204 F.3d 723, 726 (7th Cir. 2000); see also Bowyer, 875 F.2d at 638 (citing Bergman and Diliberti, and rejecting argument that continuing violation doctrine should toll statute of limitations); Diliberti, 817 F.2d at 1264 (citing Bergman for same proposition); Bergman, 751 F.2d at 316-17 (ruling that limitations period

commenced when agency first notified plaintiff in writing that it would not reconsider his discharge or correct his job classification records and rejecting argument “that a new cause of action arose upon each and every subsequent adverse determination based on erroneous records”); Reitz, 2010 WL 786586, at *9-10 (dismissing as time-barred claims filed in 2008 “alleg[ing] continuing ill effects from violations occurring in 1997 or other dates before 2006” because “[a] new cause of action does not arise ‘upon each and every subsequent adverse determination based on erroneous records’” (quoting Harrell, 285 F.3d at 1293)); Blaylock v. Snow, No. 4:06-CV-142-A, 2006 WL 3751308, at *7 (N.D. Tex. Dec. 21, 2006) (ruling that “continuing violations do not toll the limitations period” in case involving several allegedly improper disclosures over course of three years); Thompson, 332 F. Supp. 2d at 132-33 (rejecting argument that “a new cause of action was created each time [the agency] disseminated [plaintiff’s] revised Report after [the agency] had been placed on notice of a potential problem and before it reviewed the revised Report for accuracy, relevance, completeness, and timeliness”); Jarrett v. White, No. 01-800, 2002 WL 1348304, at *6 (D. Del. June 17, 2002) (rejecting argument that continuing violation doctrine should toll statute of limitations), aff’d per curiam sub nom. Jarrett v. Brownlee, 80 F. App’x 107 (Fed. Cir. 2003); Malewich, No. 91-4871, slip op. at 23-25 (D.N.J. Apr. 14, 1993) (same); Shannon, 812 F. Supp. at 319-20 (stating that plaintiff “cannot revive a potential cause of action simply because the violation continued to occur; he can allege subsequent violations only if there are subsequent events that occurred in violation of the Privacy Act”); cf. Baker v. United States, 943 F. Supp. 270, 273 (W.D.N.Y. 1996) (citing Shannon with approval). But cf. Burkins v. United States, 865 F. Supp. 1480, 1496 (D. Colo. 1994) (citing Bergman and viewing plaintiff’s harm as “continuing transaction”).

The Court of Appeals for the Ninth Circuit, in Oja v. Army Corps of Engineers, applied the single publication rule in a case involving a subsection (b) claim based on multiple postings to two agency websites of information pertaining to the plaintiff. 440 F.3d at 1130-33. Under that rule, “the aggregate communication can give rise to only one cause of action . . . and result in only one statute of limitations period that runs from the point at which the original dissemination occurred.” Id. at 1130. The court rejected the argument that “the continuous hosting of private information on an Internet website [is] a series of discrete and ongoing acts of publication, each giving rise to a cause of action with its own statute of limitations.” Id. at 1132. Instead, the court held that the claim

was time-barred because the plaintiff filed it more than two years from when plaintiff became aware of the first posting. Id. at 1133.

Moreover, a plaintiff's voluntary pursuit of administrative procedures should not toll the running of the statute of limitations, because no administrative exhaustion requirement exists before a damages action can be brought. See Uhl v. Swanstrom, 876 F. Supp. 1545, 1560-61 (N.D. Iowa 1995), aff'd on other grounds, 79 F.3d 751 (8th Cir. 1996); see also Majied v. United States, No. 7:05CV00077, 2007 WL 1170628, at *3 (W.D. Va. Apr. 18, 2007); Molzen v. BOP, No. 05-2360, 2007 WL 779059, at *3 (D.D.C. Mar. 8, 2007); Mitchell v. BOP, No. 05-0443, 2005 WL 3275803, at *3 (D.D.C. Sept. 30, 2005); cf. Kursar, 751 F. Supp. 2d at 168-69 (holding that statute of limitations was not tolled by MSPB litigation regarding plaintiff's termination); Christensen v. Interior, 109 F. App'x 373, 375 (10th Cir. 2004) ("[T]here is no basis for tolling the limitations period while Plaintiff pursued his administrative claim [under the Federal Tort Claims Act], because there is no administrative exhaustion requirement when a plaintiff seeks damages under the Privacy Act."); Grethen v. Clarke, No. 2:13cv416, 2015 WL 3452020, at *2 (E.D. Va. Mar. 13, 2015) (dismissing Privacy Act claims as time-barred, noting that "pendency of the habeas action does not impact Plaintiff's claims under the Privacy Act").

Finally, one district court has applied a provision of the Servicemembers Civil Relief Act to toll the statute of limitations for a Privacy Act claim brought by an active duty member of the U.S. Marine Corps. See Baker v. England, 397 F. Supp. 2d 18, 23-24 (D.D.C. 2005), aff'd on other grounds, 210 F. App'x 16 (D.C. Cir. 2006). Under that statute, "[t]he period of a servicemember's military service may not be included in computing any period limited by law, regulation, or order for the bringing of any action or proceeding in a court." 50 U.S.C. § 3936 (formerly codified at 50 U.S.C. app. § 526(a)).

4. Jury Trial

There is no right to a jury trial under the Privacy Act.

Generally, the Seventh Amendment does not grant a plaintiff the right to trial by jury in actions against the federal government. U.S. Const. amend. VII. Under sovereign immunity principles, "the United States, as sovereign, 'is immune from suit save as it consents to be sued ... and the terms of its consent to be sued in any court define that court's jurisdiction to entertain the suit.'" Lehman v. Nakshian, 453 U.S. 156, 160 (1981) (citations omitted).

Further, a plaintiff has a right to a jury trial only when the right has been “unequivocally expressed” by Congress. Id.

The Privacy Act is silent on the right to a jury trial and, therefore, there is no right to a jury trial under the statute. Every court to have considered the issue has ruled accordingly. See e.g., Payne v. EEOC, No. 00-2021, 2000 WL 1862659, at *2 (10th Cir. Dec. 20, 2000) (holding that Privacy Act authorizes suit only against agencies, and even where United States “consents,” general rule is that Seventh Amendment does not grant plaintiff right to trial by jury); Harris v. USDA, No. 96-5783, 1997 WL 528498, at *3 (6th Cir. Aug. 26, 1997) (same); Buckles v. Indian Health Serv./Belcourt Serv. Unit, 268 F. Supp. 2d 1101, 1102-03 (D.N.D. 2003) (neither Privacy Act nor Freedom of Information Act permit suits against individuals and any tort claims against them are deemed actions against United States, and neither of these statutes provide right to jury trial); Stewart v. FBI, No. 97-1595, 1999 U.S. Dist. LEXIS 18773, at *7-9 (D. Or. Sept. 29, 1999) (plaintiff not entitled to jury trial on Privacy Act claims because “Privacy Act nowhere mentions the word ‘jury’”) (magistrate’s recommendation), adopted, No. 97-1595, 1999 U.S. Dist. LEXIS 18785 (D. Or. Nov. 24, 1999); Clarkson v. IRS, No. 8:88-3036-3K, 1990 U.S. Dist. LEXIS 6887, at *10 (D.S.C. May 10, 1990) (denying plaintiff’s demand for jury trial, “[u]nder settled principles of sovereign immunity,” plaintiff has this right only where Congress expressly grants it by statute), aff’d, 935 F.2d 1285 (4th Cir. 1991) (unpublished table decision); Calhoun v. Wells, No. 79-2337-2, 1980 WL 1638, at *1 n.2 (D.S.C. July 30, 1980) (considering request for damages under Privacy Act as “nonjury matters,” following district court’s order striking demand for jury trial, as “no such right exists under the Privacy Act”); Henson v. Army, No. 76-45-C5, 1977 U.S. Dist. LEXIS 16868, at *1 (D. Kan. Mar. 16, 1977) (agreeing with defendants that Privacy Act does not explicitly provide for jury trial and finding no such legislative intent). But cf. Tomasello v. Rubin, No. 93-1326, slip op. at 3-5, 19 (D.D.C. Aug. 19, 1997) (noting that court was “guided by” advisory jury verdict in awarding Privacy Act damages in case also involving non-Privacy Act claims), aff’d, 167 F.3d 612, 616-17 (D.C. Cir. 1999) (recounting fact of advisory jury verdict as to Privacy Act claims).

CRIMINAL PENALTIES

“Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.” 5 U.S.C. § 552a(i)(1).

“Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.” 5 U.S.C. § 552a(i)(2).

“Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.” 5 U.S.C. § 552a(i)(3).

Comment:

The Privacy Act allows for criminal penalties in limited circumstances.

An agency official who improperly discloses records with individually identifiable information or who maintains records without proper notice, is guilty of a misdemeanor and subject to a fine of up to \$5,000, if the official acts willfully. Similarly, any individual who knowingly and willfully obtains a record under false pretenses is guilty of a misdemeanor and subject to a fine up to \$5,000.

These provisions are solely penal and create no private right of action. See Palmieri v. United States, 896 F.3d 579, 586 (D.C. Cir. 2018) (concluding that plaintiff’s complaint “erroneously mixes and matches criminal and civil portions of the Privacy Act” by seeking redress under 5 U.S.C. § 552a(g)(1) for an alleged violation of 5 U.S.C. § 552a(i)(3)); Jones v. Farm Credit Admin., No. 86-2243, slip op. at 3 (8th Cir. Apr. 13, 1987); Unt v. Aerospace Corp., 765 F.2d 1440, 1448 (9th Cir. 1985) finding claim against private corporation under § 552a(i) was futile, as it provides for criminal penalties only and because information obtained was about that corporation and not individual); Pennsylvania Higher Educ. Assistance Agency v. Perez, 416 F. Supp. 3d 75, 88 (D. Conn. 2019) (concluding that “while [student loan servicer] and its employees could be subject to criminal liability for violations of the Privacy Act, [U.S. Dep’t of Education] has no authority to bring criminal prosecutions, and no relief the Court could issue against Education would forestall such a prosecution”); Ashbourne v. Hansberry, 302 F. Supp. 3d 338, 346 (D.D.C. 2018) (finding that

“[a]lthough section 552a(i) of the Privacy Act does provide criminal penalties for federal government employees who willfully violate certain aspects of the statute, [plaintiff] cannot initiate criminal proceedings against [individual agency employees] by filing a civil suit”); Singh v. DHS, No. 1:12cv00498, 2013 WL 1704296, at *24 (E.D. Cal. Apr. 19, 2013) (holding that plaintiff could not maintain civil action seeking imposition of criminal penalties); McNeill v. IRS, No. 93-2204, 1995 U.S. Dist. LEXIS 2372, at *9-10 (D.D.C. Feb. 7, 1995); Lapin v. Taylor, 475 F. Supp. 446, 448 (D. Haw. 1979) (dismissing action against attorney alleged to have removed documents from plaintiff’s medical files under false pretenses on grounds that § 552a(i) was solely penal provision and created no private right of action); see also FLRA v. DOD, 977 F.2d 545, 549 n.6 (11th Cir. 1992) (dictum) (noting that question of what powers or remedies individual may have for disclosure without consent was not before court, but noting that section 552a(i) was penal in nature and “seems to provide no private right of action”) (citing St. Michael’s Convalescent Hosp. v. Cal., 643 F.2d 1369 (9th Cir. 1981); cf. Grant v. United States, No. 2:11-cv-00360, 2012 WL 5289309, at *8 n.12 (E.D. Cal. ct. 23, 2012) (stating that plaintiff’s request that defendant be referred for criminal prosecution “is not cognizable, because this court has no authority to refer individuals for criminal prosecution under the Privacy Act”); Study v. United States, No. 3:08cv493, 2009 WL 2340649, at *4 (N.D. Fla. July 24, 2009) (granting plaintiff’s motion to amend his complaint but directing him to “delete his request [made pursuant to subsection (i)] that criminal charges be initiated against any Defendant” because “a private citizen has no authority to initiate a criminal prosecution”); Thomas v. Reno, No. 97-1155, 1998 WL 33923, at *2 (10th Cir. Jan. 29, 1998) (finding that plaintiff’s request for criminal sanctions did “not allege sufficient facts to raise the issue of whether there exists a private right of action to enforce the Privacy Act’s provision for criminal penalties,” and citing Unt and FLRA v. DOD); Kassel v. VA, 682 F. Supp. 646, 657 (D.N.H. 1988) (finding genuine issue of material fact as to whether agency released plaintiff’s confidential personnel files, which “if done in violation of [Privacy] Act, subjects defendant’s employees to criminal penalties” (citing 5 U.S.C. § 552a(i)(1)); Bernson v. ICC, 625 F. Supp. 10, 12-13 (D. Mass. 1984) (rejecting plaintiff’s request for criminal action under Privacy Act because “only the United States Attorney can enforce federal criminal statutes”).

There have been at least two criminal prosecutions for unlawful disclosure of Privacy Act-protected records. See United States v. Trabert, 978 F. Supp. 1368 (D. Colo. 1997) (finding defendant not guilty because prosecution did not prove “beyond a reasonable doubt that defendant ‘willfully disclosed’ protected material”; “gross negligence” was “insufficient for purposes of prosecution under § 552a(i)(1)”; United States v. Gonzales, No. 76-132 (M.D. La. Dec. 21, 1976) (entering guilty plea). See also In re Mullins (Tamposi Fee Application), 84 F.3d 1439, 1441 (D.C. Cir. 1996) (per curiam) (concerning application for reimbursement of attorney fees where

Independent Counsel found that no prosecution was warranted under Privacy Act because there was no conclusive evidence of improper disclosure of information).

TEN EXEMPTIONS

The Privacy Act explicitly exempts, or allows agencies to exempt, certain categories of records, or information within a record, from certain Privacy Act provisions. One “special” exemption allows agencies to exempt from the Privacy Act’s access and amendment provisions information compiled in anticipation of civil litigation. Two “general” exemptions allow agencies to exempt certain records from all Privacy Act provisions except those specifically articulated as not subject to the general exemptions. Seven “specific” exemptions allow agencies to exempt certain records from Privacy Act provisions specifically articulated as subject to exemption.

A. 5 U.S.C. § 552a(d)(5) - Special Exemption for Information Compiled for Civil Action

“[N]othing in this [Act] shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.” 5 U.S.C. § 552a(d)(5).

Comment:

Information compiled in anticipation of civil litigation is exempt from the Privacy Act’s access and amendment provisions.

The subsection (d)(5) provision is sometimes overlooked because it is not located with the other exemptions in sections (j) and (k). On its face, it is only an exemption from the access provisions of the Privacy Act, but by implication, it also operates as an exemption from the amendment provisions. See, e.g., Smith v. United States, 142 F. App’x 209, 210 (5th Cir. 2005) (per curiam) (holding that plaintiff had no right to amend record that was “prepared in response to [his] [Federal Tort Claims Act] claim” because it fell within coverage of the exemption to access in subsection (d)(5) and, therefore, was “also exempt from the amendment requirements of the Act” (emphasis added)).

Subsection (d)(5) shields from the Privacy Act’s general access provisions information that is compiled in anticipation of court proceedings or quasi-judicial administrative hearings. See 120 Cong. Rec. at 36,959-60, reprinted in Source Book, at 936-38, https://www.justice.gov/opcl/paoverview_sourcebook. Courts have found little difficulty applying the plain language of subsection (d)(5). See e.g., Lewis v. U.S. Dep’t of Labor, 419 F.3d 970, 977 and n. 9 (9th Cir. 2005) (documents prepared in connection with anticipated civil litigation recognized as exempt); Martin v. Office of Special Counsel, MSPB, 819 F.2d 1181, 1188-89 (D.C. Cir. 1987) (finding that proceeding before MSPB is quasi-judicial

and documents prepared in anticipation of MSPB hearing were properly withheld); Davidson v. United States, 264 F. Supp. 3d 97, 111 (D.D.C. 2017), aff'd sub nom. Davidson v. Dep't of State, 728 F. App'x 7 (D.C. Cir. 2018) (exemption "unquestionably" protects from disclosure "documents prepared for actions in the district courts," "documents prepared for quasi-judicial administrative proceedings," and "documents prepared in connection with litigation to which the agency is a potential party or a potential material participant") (internal citations omitted); Menchu v. HHS, No. 3:12-CV-1366, 2014 WL 1217128, at *4-5 (D. Or. Mar. 21, 2014) (finding that purpose and function of hearing before Departmental Appeals Board are same as for civil litigation, and that investigatory notes prepared by Office of Civil Rights were properly withheld); McCready v. Principi, 297 F. Supp. 2d 178, 189-90 (D.D.C. 2003), aff'd in part & rev'd in part on other grounds sub nom. McCready v. Nicholson, 465 F.3d 1 (D.C. Cir. 2006) (affirming decision that reports issued by U.S. Department of Veterans Affairs' Inspector General critical of plaintiff were properly withheld because they could have led to adverse action against her); Nazimuddin v. IRS, No. 99-2476, 2001 WL 112274, at *3-4 (S.D. Tex. Jan 10, 2001) (finding that information prepared in anticipation of disciplinary action of plaintiff were properly withheld); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28, 949, https://www.justice.gov/paoverview_omb-75 (indicating intent for "civil proceeding" term to cover "quasi-judicial and preliminary judicial steps").

While the subsection (d)(5) exemption extends to any information prepared in reasonable anticipation of civil liberation, even if prepared by non-attorneys, the exemption is not as broad as FOIA Exemption 5.

Indeed, this Privacy Act provision has been held to be similar to the attorney work-product privilege. See, e.g., Martin v. Office of Special Counsel, 819 F.2d at 1187-89; Hernandez v. Alexander, 671 F.2d 402, 408 (10th Cir. 1982); Mobley v. CIA, 924 F. Supp. 2d 24, 60-62 (D.D.C. 2013). Furthermore, the attorney work-product privilege has been extended to information prepared by non-attorneys. See Varville v. Rubin, No. 3:96CV00629, 1998 U.S. Dist. LEXIS 14006, at *9-12 (D. Conn. Aug. 18, 1998) (citing Martin and Smiertka, *infra*, for proposition that courts "have interpreted the exemption in accordance with its plain language and have not read the requirements of the attorney work product doctrine into Exemption (d)(5)," and finding "the fact that the documents at issue were not prepared by or at the direction of an attorney is not determinative in deciding whether Exemption (d)(5) exempts the documents from disclosure"); see also Davidson v. State, 206 F. Supp. 3d 178, 194 (D.D.C. 2016) (finding that, in addition to communications with attorney, "exchanges among Department of State employees regarding legal developments in the lawsuit filed by Mr. Davidson" were properly exempted under (d)(5)); Blazy v. Tenet, 979 F. Supp.

10, 24 (D.D.C. 1997) (construing subsection (d)(5) to protect communications between CIA's Office of General Counsel and members of plaintiff's Employee Review Panel while panel was deciding whether to recommend retaining plaintiff), summary affirmance granted, No. 97-5330, 1998 WL 315583, at *1 (D.C. Cir. May 12, 1998); Smiertka v. Treasury, 447 F. Supp. 221, 227-28 (D.D.C. 1978) (construing subsection (d)(5) to cover documents prepared by and at direction of lay agency staff persons during period prior to plaintiff's firing), remanded on other grounds, 604 F.2d 698 (D.C. Cir. 1979); see also Nazimuddin, 2001 WL 112274, at *3-4 (applying subsection (d)(5) to internal memorandum from anonymous informant to plaintiff's supervisor prepared in anticipation of disciplinary action of plaintiff); Taylor v. Dep't of Educ., No. 91 N 837, slip op. at 3, 6 (D. Colo. Feb. 25, 1994) (applying subsection (d)(5) to private citizen's complaint letter maintained by plaintiff's supervisor in anticipation of plaintiff's termination); Gov't Accountability Project v. Office of Special Counsel, No. 87-0235, 1988 WL 21394, at *5 (D.D.C. Feb. 22, 1988) (stating that subsection (d)(5) "extends to any records compiled in anticipation of civil proceedings, whether prepared by attorneys or lay investigators"); Crooker v. Marshals Serv., No. 85-2599, slip op. at 2-3 (D.D.C. Dec. 16, 1985) (stating that subsection (d)(5) protects information "regardless of whether it was prepared by an attorney"); Barrett v. Customs Serv., No. 77-3033, slip op. at 2-3 (E.D. La. Feb. 22, 1979) (applying subsection (d)(5) to "policy recommendations regarding plaintiff[s] separation from the Customs Service and the possibility of a sex discrimination action").

While this provision may be applied broadly to "any information" compiled in reasonable anticipation of a civil action or proceeding and is not limited to information prepared only by attorneys, it is not as broad as Exemption 5 of the FOIA, which shields inter- or intra-agency communications that would be privileged in litigation. 5 U.S.C. § 552(b)(5). For example, subsection (d)(5) of the Privacy Act does not incorporate the deliberative process privilege, which may be invoked by agencies to withhold records in response to FOIA requests. See, e.g., Savada v. DOD, 755 F. Supp. 6, 9 (D.D.C. 1991).

Agencies cannot waive their rights to invoke the subsection (d)(5) exemption.

In addition, the D.C. Circuit Court of Appeals has held that an agency cannot waive the applicability of subsection (d)(5). McCready, 297 F. Supp. 2d at 189-90 (concluding that "[s]ubsection (d)(5) states that 'nothing in this section shall allow' access to information compiled in anticipation of a civil action" and that "[s]ince 'shall' is a mandatory word," the agency could not waive its right to invoke subsection (d)(5)); see also Louis v. U.S. Dep't of Labor, 419 F.3d at 979 (finding that an individual has no right to even demand information exempted by subsection (d)(5)).

Agencies do not need to promulgate regulations to exempt information compiled for civil litigation in accordance with subsection (d)(5).

Unlike all of the other Privacy Act exemptions discussed below, subsection (d)(5) is entirely “self-executing,” inasmuch as it does not require an implementing regulation in order to be effective. Louis, 419 F.3d at 479 (“Unlike the section (k) exemptions, which require an agency to exempt a system from access through rulemaking, subsection (d)(5) is a self-executing exception to the general access granted to individuals in subsection (d)(1)”).

B. 5 U.S.C. § 552a(j) - Two General Exemptions for Central Intelligence Agency and Criminal Law Enforcement

“The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is –

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of

(A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status;

(B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or

(C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision.

At the time rules are adopted under this subsection, the agency shall include in

the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.”
5 U.S.C. § 552a(j).

Comment:

The Privacy Act allows agencies to exempt certain records in systems of records maintained by the CIA or criminal law enforcement agencies.

One district court has described subsection (j) as follows: “Put in the simplest terms, what Congress gave Congress can take away, which it did here by conferring on agencies the power to exempt certain records from the Privacy Act.” Williams v. Farrow, 334 F. Supp. 2d 898, 905 (E.D. Va. 2004). The court went on to explain that “Congress, at most, granted” an “inchoate right” to individuals. Id. “[B]y specifically granting agencies . . . the power to exempt certain records from the Privacy Act,” “Congress conditioned any right [an individual] might have to assert a Privacy Act claim on whether [a particular agency] exercises this power.” Id. Thus, “[w]hen [an agency] exercise[s] this exemption power, any inchoate claim [an individual] may once have had [is] extinguished.” Id.

For cases involving subsection (j)(1), which applies only to records maintained by the CIA, see Alford v. CIA, 610 F.2d 348, 348-49 (5th Cir. 1980); Mobley v. CIA, 924 F. Supp. 2d 24, 55-56 (D.D.C. 2013); Braun v. FBI, No. 18-cv-2145, 2019 WL 3343948, at *6 (D.D.C. July 25, 2019); Bassiouni v. CIA, No. 02-4049, 2004 U.S. Dist. LEXIS 5290, at *13-24 (N.D. Ill. Mar. 30, 2004), aff’d, 392 F.3d 244 (7th Cir. 2005); Pipko v. CIA, 312 F. Supp. 2d 669, 678-79 (D.N.J. 2004); Blazy v. Tenet, 979 F. Supp. 10, 23-25 (D.D.C. 1997), summary affirmance granted, No. 97-5330, 1998 WL 315583 (D.C. Cir. May 12, 1998).

1. Law Enforcement Components

Subsection (j)(2) applies to systems of records maintained by “an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws.” This threshold requirement is usually met by obvious law enforcement components such as the FBI, DEA, and ATF. In addition, several other Department of Justice components qualify to use the (j)(2) exemption, including:

- the Federal Bureau of Prisons, see, e.g., Skinner v. BOP, 584 F.3d 1093, 1096 (D.C. Cir. 2009); White v. Prob. Office, 148 F.3d 1124, 1125 (D.C. Cir. 1998); Kellett v. BOP, No. 94-1898, 1995 WL 554647,

OVERVIEW OF THE PRIVACY ACT

at *3 (1st Cir. Sept. 18, 1995) (per curiam); Duffin v. Carlson, 636 F.2d 709, 711 (D.C. Cir. 1980);

- the U.S. Attorney's Office, see, e.g., Boyd v. EOUSA, 87 F. Supp. 3d 58, 87 (D.D.C. 2015); Watson v. DOJ, No. 12-2129, 2013 WL 4749916, at *3 (W.D. La. Sept. 3, 2013); Plunkett v. DOJ, 924 F. Supp. 2d 289, 306-07 (D.D.C. 2013);
- the Office of the Pardon Attorney, see, e.g., Binion v. DOJ, 695 F.2d 1189, 1191 (9th Cir. 1983);
- the Marshals Service, see, e.g., Barouch v. DOJ, 962 F. Supp. 2d 30, 68 n.21 (D.D.C. 2013); Boyer v. Marshals Serv., No. 04-1472, 2005 WL 599971, at *2-3 (D.D.C. Mar. 14, 2005); and
- the U.S. Parole Commission, see, e.g., Fendler v. Parole Comm'n, 774 F.2d 975, 979 (9th Cir. 1985).

Outside of the Department of Justice, other entities that courts have found meet the threshold requirement include:

- the Naval Criminal Investigative Service, "the criminal law enforcement investigative branch of the United States Navy," see Palmieri v. U.S., 194 F. Supp. 3d 12, 22 (D.D.C. 2016);
- the Criminal Investigation Division of the Internal Revenue Service, see Carp v. IRS, No. 00-5992, 2002 WL 443478, at *6 (D.N.J. Jan. 28, 2002);
- the U.S. Secret Service, a component of the Department of Homeland Security, see Arnold v. U.S. Secret Serv., 524 F. Supp. 2d 65, 66 (D.D.C. 2007);
- the Postal Inspection Service, a U.S. Postal Service component, see Anderson v. USPS, 7 F. Supp. 2d 583, 586 n.3 (E.D. Pa. 1998), aff'd, 187 F.3d 625 (3d Cir. 1999) (unpublished table decision);
- the Air Force Office of Special Investigations, see, e.g., Gowan v. Air Force, 148 F.3d 1182, 1189-90 (10th Cir. 1998); Butler v. Air Force, 888 F. Supp. 174, 179 (D.D.C. 1995), aff'd per curiam, No. 96-5111 (D.C. Cir. May 6, 1997); and

- Inspector General's Offices, see Seldowitz v. OIG, No. 00-1142, 2000 WL 1742098, at *4 (4th Cir. Nov. 13, 2000) (per curiam); Mumme v. Labor, 150 F. Supp. 2d 162, 172 (D. Me. 2001), aff'd, No. 01-2256 (1st Cir. June 12, 2002); Smith v. Treasury Inspector Gen. for Tax Admin., No. 11-2033, 2011 WL 6026040, at *2 (D. Md. Dec. 1, 2011), aff'd per curiam, 474 F. App'x 929 (4th Cir. 2012).

However, it has been held that the "principal" law enforcement function threshold requirement is not met where only one of the principal functions of the component maintaining the system is criminal law enforcement. See Alexander v. IRS, No. 86-0414, 1987 WL 13958, at *4 (D.D.C. June 30, 1987) (discussing IRS's Internal Security Division's "conduct investigation" system).

2. Compiled for Certain Law Enforcement Purposes

In order to exempt certain records under the subsection (j)(2) exemption, agencies must establish that the information is being compiled for one of the specifically enumerated criminal law enforcement purposes.

Once an agency has satisfied the threshold requirement of establishing that it is a law enforcement component, it must establish that the system of records at issue consists of information compiled for one of the criminal law enforcement purposes listed in subsection (j)(2)(A)-(C), e.g., to identify criminal offenders, for a criminal investigation, or compiled at any stage of the enforcement of the criminal laws. See, e.g., Mobley v. CIA, 806 F.3d 568, 586 (D.C. Cir. 2016) (finding that FBI's records compiled for purpose of ascertaining facts and circumstances of U.S. citizen's detention abroad satisfied legitimate law enforcement purpose); Jordan v. DOJ, 668 F. 3d 1188, 1201-02 (10th Cir. 2011) (affirming decision that prisoner's request for psychological records and copied mail compiled during his incarceration were exempt under (j)(2)(C), which permits agencies to exempt reports identifiable to individual that have been compiled at any stage of enforcement, from arrest through release); Boyd, 87 F. Supp. 3d at 87 (finding that EOUSA properly applied exemption under (j)(2)(B) to withhold plaintiff's criminal case files); Barouch v. DOJ, 87 F. Supp. 3d 10, 32 (D.D.C. 2015) (finding that ATF failed to establish record located in agent's personal file qualified for (j)(2) exemption and remanding for further processing and clarification); Boehm v. FBI, 948 F. Supp. 2d 9, 18 n.2 (D.D.C. 2013) (finding defendants met their burden to show that Exemption (j)(2) applies to records compiled for "investiga[ting] child sex trafficking and drug violations"); Taccetta v. FBI, No. 10-6194, 2012 WL 2523075, at *5

(D.N.J. June 29, 2012) (holding that “[a]ll records created by the FBI in its investigation of violations of criminal law are exempt from disclosure under the Privacy Act”); Smith v. Treasury Inspector Gen. for Tax Admin., 2011 WL 6026040, at *3 (rejecting argument that report of investigation “cannot be properly exempted because any claim that [plaintiff] violated a criminal law ceased to be ‘colorable’ once the AUSA declined to prosecute him” on ground that “whether or not an investigation is ‘criminal’ depends on what is being investigated and not the ultimate conclusion of the investigators or the decision of a prosecutor”), aff’d per curiam, 474 F. App’x 929 (4th Cir. 2012); Shearson v. DHS, No. 1:06 CV 1478, 2007 WL 764026, at *11 (N.D. Ohio Mar. 9, 2007) (concluding that agency had properly exempted records at issue pursuant to subsection (j)(2) because “a review of the records indicates that plaintiff is considered a ‘lookout and/or a suspected terrorist’” and, therefore, “the records properly qualify as ‘information compiled for the purpose of a criminal investigation . . . and associated with an identifiable individual’”), aff’d in pertinent part, rev’d in part, & remanded, on other grounds, 638 F. 3d 498 (6th Cir. 2011); Holz v. Westphal, 217 F. Supp. 2d 50, 54-56 (D.D.C. 2002) (finding subsection (j)(2) inapplicable to report of investigation even though report was maintained in exempt system of records, because agency’s operating regulations provided that underlying report was never within agency’s purview and therefore was not compiled for criminal law enforcement purpose); cf. Kates v. King, 487 F. App’x 704, 706 (3d Cir. 2012) (per curiam) (“Indeed, the BOP has exempted its central record system, where an inmate’s PSI is located,” which was used in plaintiff’s sentencing).

Agencies must publish the reasons for exempting each system of records under subsection (j); it is not clear whether the stated reason limits the scope of the subsection (j) exemption.

An important requirement of subsection (j) is that an agency must state in the Federal Register “the reasons why the system of records is to be exempted” from a particular subsection of the Act. 5 U.S.C. § 552a(j) (final sentence); see also 5 U.S.C. § 552a(k) (same). It is unclear whether an agency’s stated reasons for exemption – typically, a list of the adverse effects that would occur if the exemption were not available – limit the scope of the exemption when it is applied to specific records in the exempt system in particular cases. See Exner, 612 F.2d at 1206 (framing issue but declining to decide it). As discussed below, a confusing mass of case law in this area illustrates the struggle to give legal effect to this requirement.

Because of the broad scope of the subsection (j)(2) exemption, courts are deferential to agencies in access suits under this provision and are not authorized to review disputed information in camera.

Given the breadth of this law enforcement exemption, an agency's burden of proof is generally less stringent than under the FOIA, at least in the access context. See Binion, 695 F.2d at 1192-93 (9th Cir. 1983) (referencing legislative history in support of "a broad exemption" because these records "contain particularly sensitive information" (quoting H.R. Rep. No. 1416, 93d Cong., 2d Sess. 18 (1974))). Indeed, several courts have observed that the Vaughn rationale requiring itemized indices of withheld records is inapplicable to Privacy Act cases where a general exemption has been established. Shapiro v. DEA, 721 F.2d 215, 218 (7th Cir. 1983), vacated as moot sub nom. DOJ v. Provenzano, 469 U.S. 14 (1984) (finding moot because Central Intelligence Information Act amended Privacy Act by providing that agency cannot rely on exemption in Privacy Act to withhold records accessible under FOIA); see also Campbell v. DOJ, 133 F. Supp. 3d 58, 69 (D.D.C. 2015) (concluding that DOJ Criminal Division system of records was exempted from access provisions of Privacy Act under (j)(2) law enforcement exemption but analyzing FOIA under provisions other than section 7 law enforcement exemptions); Schulze v. FBI, No. 1:05-CV-0180, 2010 WL 2902518, at *15 (E.D. Cal. July 22, 2010) (concluding that the (j)(2) "exemption is both categorical and enduring."); Miller v. FBI, No. 77-C-3331, 1987 WL 18331, at *2 (N.D. Ill. Oct. 7, 1987).

Moreover, in access cases the Act does not grant courts the authority to review the information at issue in camera to determine whether subsection (j)(2)(A)-(C) is applicable. See 5 U.S.C. § 552a(g)(3)(A) (in camera review only where subsection (k) exemptions are invoked); see also Reyes v. DEA, 647 F. Supp. 1509, 1512 (D.P.R. 1986), vacated & remanded on other grounds, 834 F.2d 1093 (1st Cir. 1987). But see Exner v. FBI, 612 F.2d 1202, 1206-07 (9th Cir. 1980) (concluding that whether or not "district court had statutory authority to review any of [the] records with respect to which the government was claiming the (j)(2)(B) exemption . . ." district court "did examine the documents and concluded that they were exempt"); Bailey v. BOP, 133 F. Supp. 3d 50, 57-58 (D.D.C. 2015) (declining to rule on BOP's asserted (j)(2) exemption until it had a chance to review documents in camera). However, the lack of authority to review documents in camera under this provision may be an academic point in light of the FOIA's grant of in camera review authority under 5 U.S.C. § 552(a)(4)(B).

Courts are divided as to whether published reasons for the exemption limit the scope of the exemption in access and amendment cases.

Most courts have permitted agencies to claim the subsection (j)(2) law enforcement exemption as a defense in access and/or amendment cases – some without regard to the specific records at issue or the regulation’s stated reasons for the exemption. For cases regarding access, *see, e.g., Binion*, 695 F.2d at 1192-93; *Duffin*, 636 F.2d at 711; *Exner*, 612 F.2d at 1204-07; *Ryan v. DOJ*, 595 F.2d 954, 956-57 (4th Cir. 1979); *Bernegger v. EOUSA*, 334 F. Supp. 3d 74, 94 (D.D.C. 2018); *House v. DOJ*, 147 F. Supp. 3d 197, 209 (D.D.C. 2016); *Barouch*, 962 F. Supp. 2d at 68 n. 21; *Mobley v. CIA*, 924 F. Supp. 2d at 66-67; *Adionser v. DOJ*, 811 F. Supp. 2d 284, 301 (D.D.C. 2011), *aff’d per curiam*, No. 11-5093, 2012 WL 5897172, at *1 (D.C. Cir. Nov. 5, 2012); *Marshall v. FBI*, 802 F. Supp. 2d 125, 133-34 (D.D.C. 2011); *Vazquez v. DOJ*, 764 F. Supp. 2d 117, 120 (D.D.C. 2011) (regarding access to accounting of disclosures); *Murray v. BOP*, 741 F. Supp. 2d 156, 162 (D.D.C. 2010); *Blackwell v. FBI*, 680 F. Supp. 2d 79, 91 (D.D.C. 2010); *Holt v. DOJ*, 734 F. Supp. 2d 28, 39 (D.D.C. 2010); *Jordan v. DOJ*, No. 07-cv-02303, 2009 WL 2913223, at *26-27 (D. Colo. Sept. 8, 2009); *Maydak v. DOJ*, 254 F. Supp. 2d 23, 34-35 (D.D.C. 2003) (regarding access to accounting of disclosures); *Anderson v. Marshals Serv.*, 943 F. Supp. 37, 39-40 (D.D.C. 1996); *Hatcher*, 910 F. Supp. at 2-3; *Whittle v. Moschella*, 756 F. Supp. 589, 595-96 (D.D.C. 1991); *Simon v. DOJ*, 752 F. Supp. 14, 23 (D.D.C. 1990), *aff’d*, 980 F.2d 782 (D.C. Cir. 1992); *Yon v. IRS*, 671 F. Supp. 1344, 1347 (S.D. Fla. 1987); *Stimac v. Treasury*, 586 F. Supp. 34, 35-37 (N.D. Ill. 1984); *Cooper v. DOJ*, 578 F. Supp. 546, 547 (D.D.C. 1983); *Stimac v. FBI*, 577 F. Supp. 923, 924-25 (N.D. Ill. 1984); *Turner v. Ralston*, 567 F. Supp. 606, 607-08 (W.D. Mo. 1983), *superseded by statute on other grounds*, Central Intelligence Agency Information Act, Pub. L. No. 98-477, codified at 5 U.S.C. § 552a(t); *Nunez v. DEA*, 497 F. Supp. 209, 211 (S.D.N.Y. 1980); *but see Campbell*, 133 F. Supp. 3d at 69 (concluding that (j)(2) exemption applied only to system of records expressly exempted from access provisions by regulation).

For cases regarding amendment, *see, e.g., Castaneda v. Henman*, 914 F.2d 981, 986 (7th Cir. 1990); *Wentz v. DOJ*, 772 F.2d 335, 337-39 (7th Cir. 1985); *Fendler*, 774 F.2d at 979; *Majid v. FBI*, 245 F. Supp. 3d 63, 69-71 (D.D.C. 2017); *Ford v. DOJ*, 208 F. Supp. 3d 237, 246 (D.D.C. 2016); *Abdelfattah v. DHS*, 893 F. Supp. 2d 75, 81 (D.D.C. 2012); *Bhatia v. Office of the U.S. Attorney, N. Dist. of Cal.*, No. C 09-5581, 2011 WL 1298763, at *6 (N.D. Cal. Mar. 29, 2011), *aff’d*, 507 F. App’x 649 (9th Cir. 2013); *Study v. United States*, No. 3:08cv493, 2010 WL 1257655, at *4 (N.D. Fla. Mar. 4, 2010); *Davis v. BOP*, No. 06-1698, 2007 WL 1830863, at *2 (D.D.C. June 26, 2007); *Enigwe v. BOP*,

No. 06-457, 2006 WL 3791379, at *3 n.2 (D.D.C. Dec. 22, 2006); Cooper v. BOP, No. 02-1844, 2006 WL 751341, at *3 (D.D.C. Mar. 23, 2006); Fisher v. BOP, No. 05-0851, 2006 WL 401819, at *1 (D.D.C. Feb. 21, 2006); Aquino v. Stone, 768 F. Supp. 529, 530-31 (E.D. Va. 1991), aff'd, 957 F.2d 139 (4th Cir. 1992); Anderson v. DOJ, No. 87-5959, 1988 WL 50372, at *1 (E.D. Pa. May 16, 1988); Smith v. DOJ, No. 81-CV-813, 1983 U.S. Dist. LEXIS 10878, at *15-20 (N.D.N.Y. Dec. 13, 1983); and Varona Pacheco v. FBI, 456 F. Supp. 1024, 1034-35 (D.P.R. 1978).

For cases that discuss both access and amendment, see Donelson v. BOP, 82 F. Supp. 3d. 367, 372 (D.D.C. 2015); Shapiro, 721 F.2d at 217-18.

The Court of Appeals for the Seventh Circuit has gone so far as to hold that subsection (j)(2) “does not require that a regulation’s rationale for exempting a record from [access] apply in each particular case.” Wentz, 772 F.2d at 337-38 (quoting Shapiro, 721 F.2d at 218). This appears also to be the view of the Court of Appeals for the First Circuit. See Irons v. Bell, 596 F.2d 468, 471 (1st Cir. 1979) (“None of the additional conditions found in Exemption 7 of the FOIA, such as disclosure of a confidential source, need be met before the Privacy Act exemption applies.”); see also Reyes, 647 F. Supp. at 1512 (noting that “justification need not apply to every record and every piece of a record as long as the system is properly exempted” and that “[t]he general exemption applies to the whole system regardless of the content of individual records within it”).

The Ninth and Seventh Circuits have construed subsection (j)(2) law enforcement exemption regulations to permit exemption of systems of records from provisions of the Act even where the stated reasons do not appear to be applicable in the particular case. See, e.g., Alexander v. United States, 787 F.2d 1349, 1351-52 & n.2 (9th Cir. 1986) (dismissing subsection (g)(1)(C) damages action – alleging violation of subsection (e)(5) – on ground that system of records was exempt from subsection (g) even though implementing regulation mentioned only “access” as rationale for exemption); Wentz, 772 F.2d at 336-39 (dismissing amendment action on ground that system of records was exempt from subsection (d) even though implementing regulation mentioned only “access” as rationale for exemption and record at issue had been disclosed to plaintiff). Note, however, that the Ninth Circuit significantly narrowed the breadth of its holding in Alexander. Fendler v. BOP, 846 F.2d at 550, 554 n.3 (9th Cir. 1988) (observing that agency in Alexander “had clearly and expressly exempted its system of records from both subsection (e)(5) and subsection (g) . . . [but that for] some unexplained reason, the Bureau of Prisons, unlike

the agency involved in Alexander, did not exempt itself from [subsection (e)(5)].

Further, in Fendler, the court appears to have moved toward an earlier, narrow view stated in a concurring opinion in Exner, 612 F.2d at 1207-08 (construing subsection (j)(2)(B) as “coextensive” with FOIA Exemption 7 and noting that “reason for withholding the document was consistent with at least one of the adverse effects listed in the [regulation]”). Other courts support this narrow construction. *See, e.g., Powell v. DOJ*, 851 F.2d 394, 395 (D.C. Cir. 1988) (per curiam) (finding that agency’s regulation failed to specifically state any reason for exempting its system from amendment and that reasons stated for exempting it from access were limited, and thus (j)(2) does not permit an agency to refuse “disclosure or amendment of objective, noncontroversial information” such as race, sex, and correct addresses); Rosenberg v. Meese, 622 F. Supp. 1451, 1460 (S.D.N.Y. 1985) (ordering access to sentencing transcript contained in same exempt system of records on ground that proffered “reasons are simply inapplicable when the particular document requested is a matter of public record.”). Apparently, because the contents of the particular records at issue were viewed as innocuous – i.e., they had previously been made public – each court found that the agency had lost its exemption (j)(2) claim. Powell, 851 F.2d at 395; Rosenberg, 622 F. Supp. at 1460.

3. Additional Issues Relating to the Criminal Law Enforcement Exemption

Some courts have upheld agency regulations, consistent with the text of the subsection (j) exemption, to exempt their systems of records from the Privacy Act’s civil remedies provision.

The issue discussed above also has arisen when an agency’s regulation exempts its system of records from subsection (g) – the Privacy Act’s civil remedies provision. Oddly, the language of subsection (j) appears to permit this. *See* OMB 1975 Guidelines, 40 Fed. Reg. at 28,971, https://www.justice.gov/paoverview_omb-75.

However, in Tijerina v. Walters, 821 F.2d 789, 795-97 (D.C. Cir. 1987), the D.C. Circuit held that an agency cannot insulate itself from a wrongful disclosure damages action (*see* 5 U.S.C. § 552a(b), (g)(1)(D)) in such a manner. It construed the subsection (j) law enforcement exemption to permit an agency to exempt only a system of records – and not the agency itself – from other provisions of the Act. *See* 821 F.2d at 796-97. The result in Tijerina was influenced by the fact that subsection (j) by its terms does not

permit exemption from the subsection (b) restriction-on-disclosure provision. Id. In Tijerina, the government argued that “subsection (g) is ‘conspicuously absent’ from the list” of specific provisions that are not eligible for exemption under (j)(2), and that that “omission demonstrates that Congress intended agencies to be able to elude civil liability for any violation of the Act,” including subsection (b)’s disclosure prohibition. Id. at 795. While the D.C. Circuit noted that “some other courts ha[d] indicated in dicta” to the contrary, “[h]aving considered the issue at length [in Tijerina], in which it [wa]s squarely presented, [the Court] declined to follow that view.” Id. (citing Kimberlin v. DOJ, 788 F.2d 434, 436 n.2 (7th Cir. 1986), and Ryan v. DOJ, 595 F.2d 954, 958 (5th Cir. 1979)). In ruling that the exemption does not operate in this manner the Court stated:

The Act’s statutory language, framework, and legislative history persuade us that the government is urging a completely anomalous use of the exemption provision that makes the Act a foolishness. The interpretation offered by the government would give agencies license to defang completely the strict limitations on disclosure that Congress intended to impose.

Tijerina, 821 F.2d at 797. See also Doe v. FBI, 936 F.2d 1346, 1351-52 (D.C. Cir. 1991) (explaining that “the touchstone for an agency’s liability to suit under the Act is the substantive obligation underlying the plaintiff’s claim” and holding that a cause of action under (g)(1)(A) could “not lie with regard to records that the agency has properly exempted from the Act’s amendment requirements,” because “Tijerina merely held that an agency cannot escape liability for violating non-exemptible Privacy Act obligations simply by exempting itself from the Act’s remedial provisions”).

The Court of Appeals for the Sixth Circuit has considered this issue as well and followed the approach taken by the D.C. Circuit’s Court of Appeals. See Shearson v. DHS, 638 F.3d 498 (6th Cir. 2011). Although the D.C. Circuit in Tijerina had characterized cases as dicta, the Sixth Circuit viewed those same cases as “implicat[ing] a Circuit split in authority,” and determined that the D.C. Circuit “expresses the better view . . . [that] an agency is permitted to exempt a system of records from the civil remedies provision if the underlying substantive duty is exemptible.” Id. at 503-04 (remanding claims brought under (b) and (e)(7)); Nakash v. DOJ, 708 F. Supp. 1354, 1358-65 (S.D.N.Y. 1988) (agreeing with Tijerina after extensive discussion of case law and legislative history). But see Saleh v. United States, No. 09-cv-02563, 2011 WL 2682803, at *6 (D. Colo. Mar. 8, 2011) (magistrate’s recommendation) (concluding that “Plaintiff has no private right of action

pursuant to the Privacy Act with respect to the alleged dissemination of one of his grievances” because agency had exempted system of records from subsection (g) civil remedies), adopted in pertinent part, 2011 WL 2682728, at *1 (D. Colo. July 8, 2011).

While other courts have indicated that agencies may employ subsection (j)(2) to exempt their systems of records from the subsection (g) civil remedies provision, generally, these cases suggest that the regulation’s statement of reasons for exempting a system of records from the subsection (g) civil remedies provision itself constitutes a limitation on the scope of the exemption. See Fendler, 846 F.2d at 553-54 & n.3 (declining to dismiss subsection (g)(1)(C) damages action – alleging violation of subsection (e)(5) – on ground that agency’s “stated justification for exemption from subsection (g) bears no relation to subsection (e)(5)”; Alford v. CIA, 610 F.2d 348, 349 (5th Cir. 1980) (declining to decide whether agency may, by regulation, deprive district courts of jurisdiction to review decisions to deny access); Ryan v. DOJ, 595 F.2d 954, 957-58 (4th Cir. 1979) (dismissing access claim, but not wrongful disclosure claim, on ground that record system was exempt from subsection (g) because regulation mentioned only “access” as reason for exemption); Nakash, 708 F. Supp. at 1365 (alternative holding) (declining to dismiss wrongful disclosure action for same reason); Kimberlin v. DOJ, 605 F. Supp. 79, 82 (N.D. Ill. 1985), aff’d, 788 F.2d 434 (7th Cir. 1986); cf. Shearson v. DHS, 638 F.3d at 503 (holding that agency may not claim exemption from (g) civil remedies unless “the underlying substantive duty is exemptible,” and questioning “whether [the agency’s] efforts to exempt the system of records from § 552a(g) were procedurally adequate” because “[t]he agency’s stated justification for exempting the [system of records] from § 552a(g) is ambiguous regarding the extent to which the rule exempts the [system of records] from the civil-remedies provision”).

The Federal Bureau of Prisons has claimed the subsection (j)(2) exemption, among others, for many of its systems of records.

The Federal Bureau of Prisons has promulgated rules exempting a number of its systems of records – among them, notably, the Inmate Central Records System – from various subsections of the Act, including (d), (e)(5), and (g). See 28 C.F.R. § 16.97 (2012). Among the most frequently litigated Privacy Act claims are those brought by federal inmates against BOP based on one or more allegedly inaccurate records. In a typical case, an inmate sues BOP seeking amendment of or damages arising out of an allegedly inaccurate record contained in a BOP system of records – usually the Inmate Central Records System. Courts have consistently dismissed these claims on the

ground that BOP has exempted the system of records containing the allegedly inaccurate record from the pertinent subsection of the Act. See, e.g., Kates v. King, 487 F. App'x 704, 706 (3d Cir. 2012) (per curiam); Blackshear v. Lockett, 411 F. App'x 906, 907-08 (7th Cir. 2011); Flores v. Fox, 394 F. App'x 170, 172 (5th Cir. 2010); Davis v. United States, 353 F. App'x 864, 864 (4th Cir. 2009) (per curiam); Skinner, 584 F.3d at 1096; Martinez v. BOP, 444 F.3d 620, 624 (D.C. Cir. 2006); Scaff-Martinez v. BOP, 160 F. App'x 955, 956 (11th Cir. 2005); Barbour v. Parole Comm'n, No. 04-5114, 2005 WL 79041, at *1 (D.C. Cir. Jan. 13, 2005); Williams v. BOP, 85 F. App'x 299, 306 n.14 (3d Cir. 2004); Locklear v. Holland, 194 F.3d 1313, 1313 (6th Cir. 1999); Duffin, 636 F.2d at 711; Lee v. English, No. 19-3029, 2019 WL 3891147, at *8 (D. Kan. Aug. 19, 2019); Hall v BOP, 132 F. Supp. 3d 60, 69 (D.D.C. 2015), aff'd, No. 15-5303, 2016 WL 6237817 (D.C. Cir. Sept. 1, 2016); Wingo v. Farley, No. 4:12-CV-2072, 2013 WL 2151638, at *3 (N.D. Ohio May 16, 2013); Andrews v. Castro, No. 3:CV-12-1518, 2012 U.S. Dist. LEXIS 178909, at *1-2 (M.D. Pa. Dec. 18, 2012), aff'd, 2013 WL 6579347, at *1 (M.D. Pa. Dec. 13, 2013); Anderson v. BOP, No. 12-1478, 2012 U.S. Dist. LEXIS 132716, at *1-2 (D.D.C. Sept. 7, 2012); Lange v. Taylor, 5:10-CT-3097, 2012 WL 255333, at *3 (E.D.N.C. Jan. 27, 2012); Earle v. Holder, 815 F. Supp. 2d 176, 181-83 (D.D.C. 2011), aff'd per curiam, No. 11-5280, 2012 WL 1450574, at *1 (D.C. Cir. Apr. 20, 2012); Thomas v. Caraway, No. 10-2031, 2011 WL 2416643, at *3 (D. Md. June 10, 2011); Blanton v. Warden, No. 7:10-cv-552, 2011 WL 1226010, at *3 (W.D. Va. Mar. 30, 2011); Keyes v. Krick, No. 09-cv-02380, 2011 WL 1100128, at *7 (D. Colo. Mar. 23, 2011); Davis v. United States, No. CIV-10-1136, 2011 WL 704894, at *5 (W.D. Okla. Jan. 4, 2011) (magistrate's recommendation), adopted, 2011 WL 693639, at *1 (W.D. Okla. Feb. 18, 2011), aff'd, 426 F. App'x 648 (10th Cir. 2011); Cruel v. BOP, No. 2:09CV00189, 2010 WL 3655644, at*3 (E.D. Ark. Sept. 9, 2010); Banks v. BOP, No. 5:09cv147, 2010 WL 3737923, at *6 (S.D. Miss. Aug. 19, 2010) (magistrate's recommendation), adopted, 2010 WL 3767112, at *1 (S.D. Miss. Sept. 17, 2010); Bowles v. BOP, No. 08 CV 9591, 2010 WL 23326, at *4-5 (S.D.N.Y. Jan. 5, 2010); Jackson v. DOJ, No. 09-0846, 2009 WL 5205421, at *4 (D. Minn. Dec. 23, 2009); but cf. Christoferson v. Thomas, 548 F. App'x 487, 488 (9th Cir. 2013) (noting that "inmates may sue under the federal Privacy Act in spite of the regulations that purport to block their claims").

As discussed in detail above under subsection "5 U.S.C. § 552a(e)(5) - Maintain Accurate, Relevant, Timely, and Complete Records" of this Overview, it was not until 2002 that the BOP exempted many of its systems of records, including the Inmate Central Records System, from subsection (e)(5) pursuant to subsection (j)(2). See 28 C.F.R. § 16.97(j) (codifying 67 Fed. Reg. 51,754 (Aug. 9, 2002)). Thus, inmates' subsection (e)(5)/(g)(1)(C) claims

arising subsequent to August 9, 2002, should not succeed. See, e.g., Fisher v. BOP, No. 06-5088, 2007 U.S. App. LEXIS 5140, at *1 (D.C. Cir. Mar. 1, 2007) (per curiam).

Information that is exempt under subsection (j)(2) remains exempt, even if it is recompiled into a non-law enforcement record, so long as the purpose for which the agency claimed the subsection (j)(2) exemption remains.

Another important issue arises when information originally compiled for law enforcement purposes is recompiled into a non-law enforcement record. The D.C. Circuit confronted this issue in Doe v. FBI, 936 F.2d 1346 (D.C. Cir. 1991), and applied the principles of a Supreme Court FOIA decision concerning recompilation, FBI v. Abramson, 456 U.S. 615 (1982), to Privacy Act-protected records. It held that “information contained in a document qualifying for subsection (j) or (k) exemption as a law enforcement record does not lose its exempt status when recompiled in a non-law enforcement record if the purposes underlying the exemption of the original document pertain to the recompilation as well.” Doe v. FBI, 936 F.2d at 1356. Consistent with the U.S. Supreme Court’s decision in Abramson, the D.C. Circuit determined that recompilation does not change the basic “nature” of the information. Id.; accord OMB 1975 Guidelines, 40 Fed. Reg. at 28,971, https://www.justice.gov/paoverview_omb-75 (“The public policy which dictates the need for exempting records . . . is based on the need to protect the contents of the records in the system – not the location of the records. Consequently, in responding to a request for access where documents of another agency are involved, the agency receiving the request should consult the originating agency to determine if the records in question have been exempted.”). By the same token, law enforcement files recompiled into another agency’s law enforcement files may retain the exemption of the prior agency’s system of records. See Dupre v. FBI, No. 01-2431, 2002 WL 1042073, at *2 n.2 (E.D. La. May 22, 2002) (finding that Suspicious Activity Report maintained in exempt Department of the Treasury system of records remained exempt under that system of records when transferred to FBI for law enforcement purposes).

For subsection (g)(1)(B) access claims, courts have held that an agency can promulgate an exemption even after the date an individual makes a Privacy Act request; agencies need not raise the exemption in administrative proceedings before raising it in court.

In the context of a subsection (g)(1)(B) access claim, the District Court for the Northern District of California has ruled that an agency “is entitled to rely

on exemptions promulgated after the dates on which [the plaintiff] made his Privacy Act requests.” Hasbrouck v. Customs & Border Prot., No. C 10-3793, 2012 WL 177563, at *3 (N.D. Cal. Jan. 23, 2012) (“[R]etroactivity’ simply is not implicated, because plaintiff’s claim in essence seeks prospective injunctive relief – an order requiring CBP to turn over information now. As such, this is one of the many circumstances in which ‘a court should apply the law in effect at the time it renders its decision,’ notwithstanding the happenstance that [plaintiff] made his Privacy Act requests before the current exemptions were promulgated.”).

Finally, note that in the context of a subsection (g)(1)(B) claim for access to records, some courts have recognized that “there is no requirement that an agency administratively invoke an exemption in order to later rely on it in federal court.” Barnard v. DHS, 598 F. Supp. 2d 1, 24 (D.D.C. 2009); see also, e.g., Cuban v. SEC, 744 F. Supp. 2d 60, 89-90 (D.D.C. 2010).

C. 5 U.S.C. § 552a(k) - Seven Specific Exemption Rules Agencies May Promulgate

“The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is –

[The seven specific exemptions are discussed in order below.]

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.” 5 U.S.C. § 552a(k).

Comment:

Subsection (k) permits agencies to publish rules exempting certain systems of records from specific Privacy Act provisions.

As noted above, subsection (g)(3)(A) grants courts considering access claims the authority to “examine the contents of any agency records in camera to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section.” 5 U.S.C. § 552a(g)(3)(A). Further, some courts have held that reasonable segregation of protected and unprotected information is required under the Act whenever a subsection (k)

exemption is invoked so that the requested information can be disclosed without disclosing information that must be withheld. *See, e.g., May v. Air Force*, 777 F.2d 1012, 1015-17 (5th Cir. 1985) (concluding that concerns about releasing information about identity of source could “could be easily remedied” by typing document, putting it in third-party’s handwriting, or amalgamating information into one report); *Nemetz v. Treasury*, 446 F. Supp. 102, 105 (N.D. Ill. 1978).

The District Court for the District of Columbia has rejected the argument that an agency failed to comply with subsection (k) because the agency’s statement of reasons for exempting the system of records “appears only in the Federal Register, and not in the Code of Federal Regulations where the rule was eventually codified.” *Nat’l Whistleblower Ctr. v. HHS*, 849 F. Supp. 2d 13, 23 (D.D.C. 2012). The court first pointed out that “[s]ubsection (k)(2) requires only that an agency’s rule exempting investigative material comply with the Administrative Procedure Act’s requirement that ‘the agency shall incorporate in the rules adopted a concise general statement of their basis and purpose.’” *Id.* (quoting 5 U.S.C. § 553(c)). The court concluded that “§ 553(c) is satisfied when a statement of the rule’s basis and purpose is included in the preamble to the Final Rule appearing in the Federal Register.” *Id.*

1. 5 U.S.C. § 552a(k)(1) - FOIA Exemption 1, Classified Information

“The head of any agency may promulgate rules, in accordance with the requirements (including general notice) . . . to exempt any system of records . . . if the system of records is –

(1) subject to the provisions of section 552(b)(1) of this title.” 5 U.S.C. § 552a(k)(1).

Comment:

Subsection (k)(1) exempts classified information from certain Privacy Act provisions.

Subsection (k)(1) simply incorporates FOIA Exemption 1, which exempts classified information from disclosure. *See* 5 U.S.C. § 552(b)(1); *Taylor v. NSA*, 618 F. App’x 478, 482 (11th Cir. 2015); *Mobley v. CIA*, 924 F. Supp. 2d 24, 64-65 (D.D.C. 2013); *Makky v. Chertoff*, 489 F. Supp. 2d 421, 441 (D.N.J. 2007); *Blum v. NSA*, No. A-09-CA-769-SS, 2010 WL 11537459, at *4 (W.D. Tex. Apr. 12, 2010); *Pipko v. CIA*, 312 F. Supp. 2d 669, 677-78 (D.N.J. 2004); *Bassiouni v. CIA*, No. 02-4049, 2004 WL 1125919, at *4 (N.D. Ill. Mar. 30, 2004), *aff’d on other grounds*, 392 F.3d 244 (7th Cir. 2004); *Snyder v. CIA*,

230 F. Supp. 2d 17, 23 (D.D.C. 2003); Blazy v. Tenet, 979 F. Supp. 10, 23-25 (D.D.C. 1997), summary affirmance granted, No. 97-5330, 1998 WL 315583, at *1 (D.C. Cir. May 12, 1998); Laroque v. DOJ, No. 86-2677, 1988 WL 28334, at *2 (D.D.C. Mar. 16, 1988); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,972, https://www.justice.gov/paoverview_omb-75.

The exemption has been construed to permit the withholding of classified records from an agency employee with a security clearance who seeks only private access to records about himself. See Martens v. Commerce, No. 88-3334, 1990 U.S. Dist. LEXIS 10351, at *10-11 (D.D.C. Aug. 6, 1990) (the exemption is “based on the nature of the material, not the nature of the individual requester.”).

When responding to a request for access to records covered by this exemption, an agency may refuse to admit or deny the existence of responsive intelligence information, known as a “Glomar response,” and is not required to redact and disclose allegedly non-secret, non-exempt portions of classified documents. See Willis v. NSA, No. 17-cv-2038 (KBJ), 2019 WL 1924249 (D.D.C. April 30, 2019) (“[T]his Court concludes that NSA’s Glomar response . . . is logically and plausibly rooted in national security concerns regarding the revelation of classified information . . . and, therefore, to the extent that Willis’s request sought NSA intelligence information about herself, NSA’s response does not violate the FOIA or the Privacy Act.”); Taylor v. NSA, 618 Fed. Appx. at 481-82; Office of Capital Collateral Counsel ex rel. Mordenti v. DOJ, 331 F.3d 799, 801 n. 3 (11th Cir. 2003) (citing Phillipi v. CIA, 546 F.2d 1008 (D.C. Cir. 1976) and finding that “[a] Glomar response neither confirms nor denies the existence of documents sought in the FOIA request. This term has its origin in a case involving a FOIA request for information on the GLOMAR EXPLORER submarine-retrieval ship.”).

2. 5 U.S.C. § 552a(k)(2) - Investigative Law Enforcement Materials

“The head of any agency may promulgate rules, in accordance with the requirements (including general notice) . . . to exempt any system of records . . . if the system of records is –

...

(2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such

material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [September 27, 1975], under an implied promise that the identity of the source would be held in confidence. . .’ 5 U.S.C. § 552a(k)(2).

Comment:

This exemption covers: (1) material compiled for criminal investigative law enforcement purposes, by nonprincipal function criminal law enforcement entities; and (2) material compiled for other investigative law enforcement purposes, by any agency.

The material must be compiled for some investigative “law enforcement” purpose, such as a civil investigation or a criminal investigation by a nonprincipal function criminal law enforcement agency. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,972-73, https://www.justice.gov/paoverview_omb-75; see also, e.g., Montenegro v. FBI, No. 1:16CV1400, 2017 WL 2692613 (E.D. Va. June 22, 2017) (holding that U.S. Immigration and Customs Enforcement properly withheld information contained in Alien file, Index, and National File Tracking system); Gowan v. Air Force, 148 F.3d 1182, 1188-89 (10th Cir. 1998) (regarding fraud, waste, and abuse complaint to OIG); Menchu v. HHS, 965 F. Supp. 2d 1238, 1248 (D. Or. 2013) (discussing investigation by HHS Office for Civil Rights of discrimination complaint against health system), aff’d, 2014 WL 1217128, at * 1 (D. Or. Mar. 21, 2014); Berger v. IRS, 487 F. Supp. 2d 482, 497-98 (D.N.J. 2007) (discussing civil trust fund recovery penalty investigation), aff’d 288 F. App’x 829 (3d Cir. 2008); Melius v. Nat’l Indian Gaming Comm’n, No. 98-2210, 1999 U.S. Dist. LEXIS 17537, at *14-15, 18-19 (D.D.C. Nov. 3, 1999) (regarding law enforcement investigation into suitability of person involved in gaming contracts); Shewchun v. INS, No. 95-1920, slip op. at 3, 8-9 (D.D.C. Dec. 10, 1996) (regarding investigation into deportability pursuant to Immigration and Nationality Act), summary affirmance granted, No. 97-5044 (D.C. Cir. June 5, 1997); Viotti v. Air Force, 902 F. Supp. 1331, 1335 (D. Colo. 1995) (discussing inspector general’s fraud, waste, and abuse investigation into plaintiff’s travel records), aff’d, 153 F.3d 730 (10th Cir. 1998) (unpublished table decision); Jaindl v. State, No. 90-1489, slip op. at 3 (D.D.C. Jan. 31, 1991) (regarding non-principal function law enforcement agency assisting in apprehension of plaintiff by revoking his passport), summary affirmance granted, No. 91-5034 (D.C. Cir. Jan. 8, 1992); Barber v. INS, No. 90-0067C, slip op. at 6-9 (W.D. Wash. May 15, 1990) (discussing enforcement of

Immigration and Nationality Act); Welsh v. IRS, No. 85-1024, slip op. at 2-3 (D.N.M. Oct. 21, 1986) (regarding taxpayer audit); Spence v. IRS, No. 85-1076, slip op. at 2 (D.N.M. Mar. 27, 1986) (regarding taxpayer audit); Nader v. ICC, No. 82-1037, 1983 U.S. Dist. LEXIS 11380, at *14 (D.D.C. Nov. 23, 1983) (discussing investigation to determine whether to bar attorney from practicing before ICC for knowingly submitting false, inaccurate, and misleading statements to agency); Heinzl v. INS, 3 Gov't Disclosure Serv. (P-H) ¶ 83,121, at 83,725 (N.D. Cal. Dec. 18, 1981) (discussing investigation regarding possible deportation); Lobosco v. IRS, No. 77-1464, 1981 WL 1780, at *3 (E.D.N.Y. Jan. 14, 1981) (regarding taxpayer audit); but cf. Louis v. Labor, No. 03-5534, slip op. at 8 (W.D. Wash. Mar. 8, 2004) (finding that records compiled for purposes of Federal Employee Compensation Act claim were properly exempt based on stated reasons for exemption in agency's regulation without discussing whether records were indeed compiled for investigative law enforcement purposes as is statutorily required).

In general, the subsection (k)(2) exemption does not apply to routine background security investigation files, but does apply to investigations of employees suspected of illegal activity.

In general, subsection (k)(2) does not include material compiled solely for the purpose of a routine background security investigation of a job applicant. See Vymetalik v. FBI, 785 F.2d 1090, 1093-98 (D.C. Cir. 1986) (noting applicability of narrower subsection (k)(5) to such material and ruling that "specific allegations of illegal activities" must be involved in order for subsection (k)(2) to apply); Bostic v. FBI, No. 1:94 CV 71, slip op. at 7-8 (W.D. Mich. Dec. 16, 1994) (following Vymetalik). The exemption of material compiled for employment or classified access that would identify a confidential source is addressed in subsection (k)(5) of the Privacy Act (discussed *infra*).

However, material compiled for the purpose of investigating agency employees for suspected violations of law can fall within subsection (k)(2). See Strang v. U.S. Arms Control & Disarmament Agency, 864 F.2d 859, 862-63 n.2 (D.C. Cir. 1989) ("Unlike Vymetalik, this case involves not a job applicant undergoing a routine check of his background and his ability to perform the job, but an existing agency employee investigated for violating national security regulations."); Nazimuddin v. IRS, No. 99-2476, 2001 WL 112274, at *2, 4 (S.D. Tex. Jan. 10, 2001) (protecting identity of confidential source in document prepared in anticipation of disciplinary action resulting from investigation of employee's alleged misuse of Lexis/Nexis research

account); Croskey v. Office of Special Counsel, 9 F. Supp. 2d 8, 11 (D.D.C. 1998) (finding Office of Special Counsel Report of Investigation, which was developed to determine whether plaintiff had been fired for legitimate or retaliatory reasons, exempt from access and amendment provisions of Privacy Act pursuant to subsection (k)(2)), summary affirmation granted, No. 98-5346, 1999 WL 58614 (D.C. Cir. Jan. 12, 1999); Cohen v. FBI, No. 93-1701, slip op. at 4-6 (D.D.C. Oct. 3, 1995) (applying Vymetalik and finding that particular information within background investigation file qualified as “law enforcement” information “withheld out of a legitimate concern for national security,” thus “satisf[ying] the standards set forth in Vymetalik,” which recognized that “[i]f specific allegations of illegal activities were involved, then th[e] investigation might well be characterized as a law enforcement investigation” and that “[s]o long as the investigation was ‘realistically based on a legitimate concern that federal laws have been or may be violated or that national security may be breached’ the records may be considered law enforcement records” (quoting Vymetalik, 785 F.2d at 1098, in turn quoting Pratt v. Webster, 673 F.2d 408, 421 (D.C. Cir. 1982))); see also Viotti, 902 F. Supp. at 1335 (concluding, “as a matter of law, that [Report of Inquiry] was compiled for a law enforcement purpose as stated in 5 U.S.C. § 552a(k)(2)” where “original purpose of the investigation . . . was a complaint to the [Inspector General] of fraud, waste and abuse,” even though “complaint was not sustained and no criminal charges were brought,” because “plain language of the exemption states that it applies to the purpose of the investigation, not to the result”); Mittleman v. Treasury, 919 F. Supp. 461, 469 (D.D.C. 1995) (finding that Inspector General’s report “pertain[ing] to plaintiff’s grievance against Treasury officials and related matters . . . falls squarely within the reach of exemption (k)(2)”), aff’d in part & remanded in part on other grounds, 104 F.3d 410 (D.C. Cir. 1997); Fausto v. Watt, 3 Gov’t Disclosure Serv. (P-H) ¶ 83,217, at 83,929-30 (4th Cir. June 7, 1983) (holding that investigation prompted by a “hotline” tip and conducted to avoid fraud, waste, and abuse qualified under (k)(2)); Frank v. DOJ, 480 F. Supp. 596, 597 (D.D.C. 1979).

Notwithstanding the general rule stated in Vymetalik, a few courts have found that an agency may rely on subsection (k)(2) to withhold materials from pre-employment background security investigation files. For example, in Doe v. DOJ, 790 F. Supp. 17, 19-21 (D.D.C. 1992), the court determined that, although subsection (k)(5) was “directly applicable,” subsection (k)(2) also applied to records of an FBI background check on a prospective Department of Justice attorney. It determined that the Department of Justice, as “the nation’s primary law enforcement and security agency,” had a legitimate law enforcement purpose in ensuring that “officials like Doe . . .

be ‘reliable, trustworthy, of good conduct and character, and of complete and unswerving loyalty to the United States.’” Id. at 20 (quoting Exec. Order No. 10,450, 18 Fed. Reg. 2489 (Apr. 29, 1953)). Likewise, in Cohen v. FBI, No. 93-1701 (D.D.C. Oct. 3, 1995), the court found subsection (k)(2) to be applicable to one document in a prospective employee’s background investigation file because that document was “withheld out of a legitimate concern for national security” and it “satisfie[d] the standards set forth in Vymetalik,” which recognized that “[i]f specific allegations of illegal activities were involved, then th[e] investigation might well be characterized as a law enforcement investigation” and that “[s]o long as the investigation was “realistically based on a legitimate concern that federal laws have been or may be violated or that national security may be breached” the records may be considered law enforcement records.” Cohen, No. 93-1701, slip op. at 3-6 (D.D.C. Oct. 3, 1995) (quoting Vymetalik, 785 F.2d at 1098, in turn quoting Pratt, 673 F.2d at 421).

Similarly, subsection (k)(2) has been held in at least one case to apply to background investigations of prospective FBI/DEA special agents. See Putnam v. DOJ, 873 F. Supp. 705, 717 (D.D.C. 1995) (finding that subsection (k)(2) was properly invoked to withhold information that would reveal identities of individuals who provided information in connection with former FBI special agent’s pre-employment investigation).

Individuals are entitled to access investigative records used as a basis for denying their rights, privileges, or benefits.

Although the issue has not been the subject of much significant case law, the OMB 1975 Guidelines explain that the “Provided, however” provision of subsection (k)(2) means that “[t]o the extent that such an investigatory record is used as a basis for denying an individual any right, privilege, or benefit to which the individual would be entitled in the absence of that record, the individual must be granted access to that record except to the extent that access would reveal the identity of a confidential source.” 40 Fed. Reg. at 28,973, https://www.justice.gov/paoverview_omb-75; cf. Castillo v. DHS, No. 11-69, 2011 WL 13282126 (D.N.M. Nov. 22, 2011) (noting that, pursuant to subsection (k)(2), names of individuals confidentially interviewed during Citizenship and Immigration Services investigation into an allegedly sham marriage were being withheld by the agency); Iewett v. State, No. 11 cv 1852, 2013 WL 550077, at *10 (D.D.C. Feb. 14, 2013) (upholding agency’s reliance on subsection (k)(2) to withhold “a law enforcement report requesting assistance in locating and apprehending [plaintiff] in order to protect a confidential source’s identity”); Nazimuddin,

2001 WL 112274, at *4 (protecting identity of source under express promise of confidentiality pursuant to subsection (k)(2) without discussion of whether investigatory record was used to deny right, privilege, or benefit); Guccione v. Nat'l Indian Gaming Comm'n, No. 98-CV-164, 1999 U.S. Dist. LEXIS 15475, at *11-12 (S.D. Cal. Aug. 5, 1999) (approving agency invocation of subsection (k)(2) to protect third-party names of individuals who had not been given express promises of confidentiality where plaintiff did not contend any denial of right, privilege, or benefit).

The District Court for the District of Colorado has found that forced early retirement resulted in a loss of a benefit, right, or privilege for purposes of the subsection (k)(2) exemption.

A few decisions have discussed what constitutes a denial of a “right, privilege, or benefit” sufficient to require that the agency grant access to records otherwise exempt from access under subsection (k)(2). For example, in Viotti v. Air Force, 902 F. Supp. at 1335-36, the District Court for the District of Colorado determined that an Air Force Colonel’s forced early retirement “resulted in a loss of a benefit, right or privilege for which he was eligible – the loss of six months to four years of the difference between his active duty pay and retirement pay,” and “over his life expectancy . . . the difference in pay between the amount of his retirement pay for twenty-six years of active duty versus thirty years of active duty.” Id. The court found that “as a matter of law, based on [a report of inquiry, plaintiff] lost benefits, rights, and privileges for which he was eligible” and thus he was entitled to an unredacted copy of the report “despite the fact that [it] was prepared pursuant to a law enforcement investigation.” Id. It went on to find that “the ‘express’ promise requirement” of (k)(2) was not satisfied where a witness “merely expressed a ‘fear of reprisal.’” Id. (citing Londrigan v. FBI, 670 F.2d 1164, 1170 (D.C. Cir. 1981) (Londrigan I)).

The District Court for the District of Oregon has found that that depriving an individual of the right to be present at, and seek medical services from, a health system facility resulted in a loss of a benefit, right, or privilege for purposes of the subsection (k)(2) exemption.

Likewise, the District Court for the District of Oregon held that subsection (k)(2) required access to interview notes compiled by the Office for Civil Rights of the Department of Health and Human Services in the course of its investigation of a discrimination complaint filed by the plaintiff against a health system. Menchu, 965 F. Supp. 2d at 1248. The notes concerned accusations made by an employee of the health system that the plaintiff had

harassed her, which led the health system to bar the plaintiff from its facilities. Id. at 1241. The agency denied the plaintiff's discrimination claim, upholding the health system's decision to bar the plaintiff from its facilities. Id. at 1249. In rejecting the agency's argument that its regulations – which were promulgated pursuant to subsection (k)(2) and which purported to exempt the notes from the Act's access provisions – permitted it to withhold the notes, the Court reasoned that "the records created by the Agency during the investigation, and the continued maintenance of such material, deprived [the plaintiff] of 'a right, privilege, or benefit that he would otherwise be entitled by Federal law' – the right to be present on, pursue employment at, and seek medical services from, [the health system's] facilities in a nondiscriminatory manner." Id.

A number of courts have found that plaintiffs have failed to articulate a deprivation of a right or benefit in accordance with the subsection (k)(2) exemption.

In contrast, the District Court for the District of Columbia found no deprivation of rights or benefits that would require granting access to subsection (k)(2) records. Nat'l Whistleblower Ctr. v. HHS, 849 F. Supp. 2d 13, 24 (D.D.C. 2012). The plaintiffs in Nat'l Whistleblower Ctr. claimed to have suffered adverse employment actions as the result of the Office of Inspector General's maintenance of certain investigative records to which they sought access. Id. The OIG disputed that any employment actions "occurred as a result of the maintenance" of its investigative file, especially as the results of its investigation found no misconduct. Id. The OIG maintained that any action taken by the FDA against plaintiffs "was at FDA's discretion." Id. The court agreed, stating: "In sum, OIG's maintenance of its investigative files did not cause Plaintiffs to be denied rights or benefits; instead, FDA's maintenance of its own investigative files resulted in any adverse employment actions suffered by Plaintiffs." Id. See also, e.g., Gowan v. Air Force, 148 F.3d at 1189 (finding that individual was not entitled to access Inspector General complaint protected by subsection (k)(2), because "the charges in the complaint were deemed unworthy of further action").

In Doe v. DOJ, 790 F. Supp. at 21 n.4, 22, the court determined that the disclosure requirement in subsection (k)(2) did not apply, on grounds that the plaintiff "ha[d] no entitlement to a job with the Justice Department." The court, however, failed to discuss whether the denial of a federal job would amount to the denial of a "privilege" or "benefit." See also [aind], No. 90-1489, slip op. at 2 n.1 (noting that "[b]ecause there is no general right to possess a passport," application of (k)(2) was not limited in that case).

The limited right of access under the subsection (k)(2) exemption does not include the right to amend.

Even when applicable, the limited right to obtain access to records protected under subsection (k)(2) does not include the right to have such records amended. See 5 U.S.C. § 552a(k)(2) (requiring only that “material shall be provided to [the] individual except to the extent that disclosure of such material would reveal the identity of a [confidential source]” (emphasis added)). For example, the Court of Appeals for the Tenth Circuit, in affirming Viotti, supra, noted that subsection (k)(2)’s limiting exception applied only in the context of access requests and did not apply to limit the exemption’s applicability with regard to amendment requests. Viotti v. Air Force, 153 F.3d at 2 n.2; see also Gowan, 148 F.3d at 1189 (concluding that subsection (k)(2) did not require disclosure of the record to the subject individual, while separately observing that the record remained exempt from amendment under that subsection).

The Privacy Act does not impose a temporal limitation on the applicability of the subsection (k)(2) exemption.

Unlike with Exemption 7(A) of the Freedom of Information Act, 5 U.S.C. § 552(b)(7)(A) (2018), there is no temporal limitation on the scope of subsection (k)(2). See Irons v. Bell, 596 F.2d 468, 471 (1st Cir. 1979); Lobosco, 1981 WL 1780, at *4. But see Anderson v. Treasury, No. 76-1404, slip op. at 9-11 (D.D.C. July 19, 1977) (finding subsection (k)(2) inapplicable to investigatory report regarding alleged wrongdoing by IRS agent where investigation was closed and no possibility of any future law enforcement proceedings existed).

Records exempted under the subsection (k)(2) exemption should still be exempt if the records are subsequently added into non-law enforcement records.

Information that originally qualifies for subsection (k)(2) protection should retain that protection even if it subsequently is recompiled into a non-law enforcement record. See Doe v. FBI, 936 F.2d 1346, 1356 (D.C. Cir. 1991) (discussing under subsection (j)(2)); accord OMB 1975 Guidelines, 40 Fed. Reg. at 28,971, https://www.justice.gov/paoverview_omb-75.

Suits alleging an agency's wrongful disclosure of records pursuant to a promise of confidentiality in accordance with the subsection (k)(2) exemption are unusual and have not prevailed.

Finally, two courts have ruled in favor of the agency in cases brought by individuals who allegedly provided information pursuant to a promise of confidentiality and sought damages resulting from disclosure of the information and failure to sufficiently protect their identities pursuant to subsection (k)(2). Bechhoefer v. DOJ, 934 F. Supp. 535, 538-39 (W.D.N.Y. 1996), vacated & remanded, 209 F.3d 57 (2d Cir. 2000) (finding that information at issue did qualify as "record" under Privacy Act); Sterling v. United States, 798 F. Supp. 47, 49 (D.D.C. 1992). In Sterling, the District Court for the District of Columbia stated that the plaintiff was "not barred from stating a claim for monetary damages [under (g)(1)(D)] merely because the record did not contain 'personal information' about him and was not retrieved through a search of indices bearing his name or other identifying characteristics," 798 F. Supp. at 49, but in a subsequent opinion the court ultimately ruled in favor of the agency, having been presented with no evidence that the agency had intentionally or willfully disclosed the plaintiff's identity. Sterling v. United States, 826 F. Supp. 570, 571-72 (D.D.C. 1993), summary affirmance granted, No. 93-5264 (D.C. Cir. Mar. 11, 1994). However, the District Court for the Western District of New York in Bechhoefer, when presented with an argument based on Sterling, stated that it did not "find the Sterling court's analysis persuasive." Bechhoefer, 934 F. Supp. at 538-39. Having already determined that the information at issue did not qualify as a record "about" the plaintiff, that court recognized that subsection (k)(2) "does not prohibit agencies from releasing material that would reveal the identity of a confidential source" but rather "allows agencies to promulgate rules to exempt certain types of documents from mandatory disclosure under other portions of the Act." Id. The court went on to state that "plaintiff's reliance on § 552a(k)(2) [wa]s misplaced," and that subsection (k) was "irrelevant" to the claim before it for wrongful disclosure. Id. at 539.

3. 5 U.S.C. § 552a(k)(3) - Secret Service Records

"The head of any agency may promulgate rules, in accordance with the requirements (including general notice) . . . to exempt any system of records . . . if the system of records is –

...

(3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056

of Title 18. . ." 5 U.S.C. § 52a(k)(3).

Comment:

By its text, this exemption would apply to certain systems of records maintained by the United States Secret Service. For a discussion of this exemption, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,973, https://www.justice.gov/paoverview_omb-75.

4. **5 U.S.C. § 552a(k)(4) - Statistical Records**

“The head of any agency may promulgate rules, in accordance with the requirements (including general notice) . . . to exempt any system of records . . . if the system of records is –

. . .

(4) required by statute to be maintained and used solely as statistical records. . .” 5 U.S.C. § 552a(k)(4).

Comment:

For a discussion of this exemption, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,973, https://www.justice.gov/paoverview_omb-75.

5. **5 U.S.C. § 552a(k)(5) - Source-Identifying Investigatory Material Compiled for Determining Suitability, Eligibility, or Other Qualification**

“The head of any agency may promulgate rules, in accordance with the requirements (including general notice) . . . to exempt any system of records . . . if the system of records is –

. . .

(5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [September 27, 1975], under an implied promise that the identity of the source would be held in confidence.” 5 U.S.C. § 552a(k)(5).

Comment:

Known as the “Erlenborn Amendment,” the subsection (k)(5) exemption is generally applicable to source-identifying materials in background employment and personnel-type investigative files.

This exemption is generally applicable to source-identifying material in background employment and personnel-type investigative files. See OMB 1975 Guidelines, 40 Fed. Reg. at 28,973-74, https://www.justice.gov/paoverview_omb-75; 120 Cong. Rec. at 40,884-85, reprinted in Source Book at 860, 996-97, https://www.justice.gov/opcl/paoverview_sourcebook. The Court of Appeals for the District of Columbia Circuit has held that exemption (k)(5) is also applicable to source-identifying material compiled for determining eligibility for federal grants, stating that “the term ‘Federal contracts’ in Privacy Act exemption (k)(5) encompasses a federal grant agreement if the grant agreement includes the essential elements of a contract and establishes a contractual relationship between the government and the grantee.” Henke v. Commerce, 83 F.3d 1445, 1453 (D.C. Cir. 1996). In addition, exemption (k)(5) is applicable to information collected for continued as well as original employment. See Hernandez v. Alexander, 671 F.2d 402, 406 (10th Cir. 1982). In situations where “specific allegations of illegal activities” are being investigated, an agency may be able to invoke subsection (k)(2) – which is potentially broader in its coverage than subsection (k)(5). See, e.g., Vymetalik v. FBI, 785 at 1093-98.

Subsection (k)(5) – known as the “Erlenborn Amendment” – was among the most hotly debated of any of the Act’s provisions because it provides for absolute protection to those who qualify as confidential sources, regardless of the adverse effect that the material they provide may have on an individual. See 120 Cong. Rec. at 36,655-58, reprinted in Source Book at 908-19, https://www.justice.gov/opcl/paoverview_sourcebook.

However, an agency cannot rely upon subsection (k)(5) to bar a requester’s amendment request, as the exemption applies only to the extent that disclosure of information would reveal the identity of a confidential source. See Vymetalik, 785 F.2d at 1096-98; see also Doe v. FBI, 936 F.2d at 1356 n.12 (noting that subsection (k)(5) would not apply where FBI refused to amend information that had already been disclosed to individual seeking amendment); Bostic, No. 1:94 CV 71, slip op. at 9 (W.D. Mich. Dec. 16, 1994) (holding that application of exemption (k)(5) in this access case is not contrary to, but rather consistent with, Vymetalik and Doe v. FBI because in those cases exemption (k)(5) did not apply because relief sought was

amendment of records).

It should be noted that information that originally qualifies for subsection (k)(5) protection should retain that protection even if it subsequently is recompiled into a non-law enforcement record. See *Doe v. FBI*, 936 F.2d 1346, 1356 (D.C. Cir. 1991) (discussing under subsection (j)(2)); accord OMB 1975 Guidelines, 40 Fed. Reg. at 28,971, https://www.justice.gov/paoverview_omb-75.

Subsection (k)(5) is a narrow exemption, requiring an expressed promise of confidentiality after the effective date of the Privacy Act, and is limited to source-identifying material.

Even so, subsection (k)(5) is a narrow exemption in two respects. First, in contrast to Exemption 7(D) of the FOIA, 5 U.S.C. § 552(b)(7)(D) (2018), it requires an express promise of confidentiality for source material acquired after the effective date of the Privacy Act (September 27, 1975). See, e.g., *Lamb v. Millennium Challenge Corp.*, 334 F.3d 204, 218 (D.D.C. 2018) (concluding that further information was needed to determine whether subsection (k)(5) applied, including whether promise of confidentiality was implied or “express,” as required by the subsection); *Viotti v. Air Force*, 902 F. Supp. at 1336 (finding that “‘express’ promise requirement” of subsection (k)(2) was not satisfied when witness “merely expressed a ‘fear of reprisal’”), aff’d, 153 F.3d 730 (10th Cir. 1998) (unpublished table decision).

For source material acquired prior to the effective date of the Privacy Act, an implied promise of confidentiality will suffice. See 5 U.S.C. § 552a(k)(5); cf. *Londrigan v. FBI*, 722 F.2d 840, 844-45 (D.C. Cir. 1983) (*Londrigan II*) (finding no “automatic exemption” for FBI background interviews prior to effective date of Privacy Act; inferring that interviewees were impliedly promised confidentiality where FBI showed that it had pursued “policy of confidentiality” to which interviewing agents conformed their conduct). See generally *DOJ v. Landano*, 508 U.S. 165 (1993) (setting standards for demonstrating implied confidentiality under FOIA Exemption 7(D)). Second, in contrast to the second clause of FOIA Exemption 7(D), subsection (k)(5) protects only source-identifying material, not all source-supplied material.

Of course, where source-identifying material is exempt from Privacy Act access under subsection (k)(5), it typically is exempt under the broader exemptions of the FOIA as well. See, e.g., *Keenan v. DOJ*, No. 94-1909, slip op. at 16-17 (D.D.C. Mar. 25, 1997), subsequent decision, slip op. at 5-7

(D.D.C. Dec. 16, 1997); Bostic v. FBI, No. 1:94 CV 71, slip op. at 8-9, 12-13 (W.D. Mich. Dec. 16, 1994); Miller v. United States, 630 F. Supp. 347, 348-49 (E.D.N.Y. 1986); Patton v. FBI, 626 F. Supp. 445, 446-47 (M.D. Pa. 1985), aff'd, 782 F.2d 1030 (3d Cir. 1986) (unpublished table decision); Diamond v. FBI, 532 F. Supp. 216, 232 (S.D.N.Y. 1981), aff'd, 707 F.2d 75 (2d Cir. 1983).

One court has held that subsection (k)(5) protects source-identifying material even where the identity of the source is known. See Volz v. DOJ, 619 F.2d 49, 50 (10th Cir. 1980). Another court has suggested to the contrary. Doe v. U.S. Civil Serv. Comm'n, 483 F. Supp. 539, 576-77 (S.D.N.Y. 1980) (holding the addresses of three named persons “not exempt from disclosure under (k)(5) . . . because they didn’t serve as confidential sources and the plaintiff already knows their identity”).

Subsection (k)(5) is not limited to those sources who provide derogatory comments, see Londrigan I, 670 F.2d at 1170; see also Voelker v. FBI, 638 F. Supp. 571, 572-73 (E.D. Mo. 1986). The exemption is not limited to information that would reveal the identity of the source in statements made by those confidential sources, but also protects information that would reveal the source’s identity in statements provided by third parties. See Haddon v. Freeh, 31 F. Supp. 2d 16, 21 (D.D.C. 1998). Also, the exemption’s applicability is not diminished by the age of the source-identifying material. See Diamond, 532 F. Supp. at 232-33.

Promises of confidentiality should not be automatic, and courts have suggested that agencies utilize the promise of confidentiality sparingly.

OMB’s policy guidance indicates that promises of confidentiality are not to be made automatically. OMB 1975 Guidelines, 40 Fed. Reg. at 28,974, https://www.justice.gov/paoverview_omb-75. Consistent with the OMB 1975 Guidelines, the Office of Personnel Management has promulgated regulations establishing procedures for determining when a pledge of confidentiality is appropriate. See 5 C.F.R. § 736.102 (2012); see also Larry v. Lawler, 605 F.2d 954, 961 n.8 (7th Cir. 1978) (suggesting that finding of “good cause” is prerequisite for granting of confidentiality to sources).

Nevertheless, the District Court for the District of Columbia has held that in order to invoke exemption (k)(5) for sources that were in fact promised confidentiality, it is not necessary that the sources themselves affirmatively sought confidentiality, nor must the government make a showing that the sources would not have furnished information without a promise of confidentiality. Henke v. Commerce, No. 94-0189, 1996 WL 692020, at *9-10

(D.D.C. Aug. 19, 1994). The court went on to state: “[T]he question of whether the reviewers expressed a desire to keep their identities confidential is wholly irrelevant to the Court’s determination of whether they were in fact given promises of confidentiality.” Id. at *10. On appeal, the Court of Appeals for the District of Columbia Circuit stated that while it “would not go quite that far,” as agencies “must use subsection (k)(5) sparingly,” agencies may make determinations that promises of confidentiality are necessary “categorically,” as “[n]othing in either the statute or the case law requires that [an agency] apply subsection (k)(5) only to those particular reviewers who have expressly asked for an exemption and would otherwise have declined to participate in the peer review process.” Henke v. Commerce, 83 F.3d at 1449.

6. 5 U.S.C. § 552a(k)(6) - Testing or Examination Materials

“The head of any agency may promulgate rules, in accordance with the requirements (including general notice) . . . to exempt any system of records . . . if the system of records is –

. . .

(6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process.” 5 U.S.C. § 552a(k)(6).

Comment:

Courts generally have found that FOIA Exemption 2 reflects the same concerns and covers the same information as the testing and examination material exemption.

Material exempt from Privacy Act access under subsection (k)(6) is also typically exempt from FOIA access under FOIA Exemption 2 (exempting records “related solely to the internal personnel rules and practices of the agency”). See Kelly v. Census Bureau, No. C 10-04507, 2011 U.S. Dist. LEXIS 100279, at *6 (N.D. Cal. Sept. 7, 2011); Patton v. FBI, 626 F. Supp. 445, 447 (M.D. Pa. 1985) (finding that disclosure would give future applicants unfair advantage and would impair usefulness and value of system, while noting that FOIA Exemption 2 is broader in scope than Privacy Act subsection (k)(6)), aff’d, 782 F.2d 1030 (3d Cir. 1986); see also Robinett v. USPS, No. 02-1094, slip op. at 15 & n.2, 16-18 (E.D. La. July 24, 2002) (finding that information showing “how much [the agency] reduced [the plaintiff’s] application score because of [a traffic violation]” was “just the type of information that courts have found could compromise an agency’s

evaluation process” and thus was exempt from disclosure under subsection (k)(6), and further, noting that although court did not need to address agency’s FOIA Exemption 2 argument “[i]n light of the Court’s finding that the information fits under another FOIA exemption,” FOIA Exemption 2 “has been read to reflect the same concerns and cover the same information as the exemption codified in Section 552a(k)(6)”.

The Ninth Circuit has found that the testing and examination material exemption applies to the agency’s test or examination, the minimum passing score, and the individual test scores.

Subsection (k)(6) applies not only to an agency’s test or examination, but also to the minimum passing score and individual test scores. See Rojas v. FAA, 941 F.3d 392, 403 (9th Cir. 2019) (holding that term “testing material” refers to “items needed to conduct a test or examination to determine an individual’s proficiency or knowledge”), aff’g in relevant part Rojas v. FAA, No. CV-15-1709-PHX-SMM, 2017 U.S. Dist. LEXIS 157661 (D. Ariz. Sept. 28, 2017) (applying both FOIA Exemption 2 and Privacy Act subsection (k)(6) where agency’s Biographical Assessment for hiring air traffic controllers continued to be significantly threatened by sophisticated applicant pool willing to compromise Assessment and overall hiring process, and knowledge of minimum passing score was restricted to limited number of FAA personnel).

For a further discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,974, https://www.justice.gov/paoverview_omb-75.

7. 5 U.S.C. § 552a(k)(7) - Source-Identifying Armed Services Promotion Material

“The head of any agency may promulgate rules, in accordance with the requirements (including general notice) . . . to exempt any system of records . . . if the system of records is –

. . . (7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section [September 27, 1975], under an implied promise that the identity of the source would be held in confidence.” 5 U.S.C. § 552a(k)(7).

Comment:

For an example of the application of this exemption, see May v. Air Force, 777 F.2d 1012, 1015-17 (5th Cir. 1985). For a further discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,974, https://www.justice.gov/paoverview_omb-75.

DISCLOSURE OF SOCIAL SECURITY NUMBER

“(a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his social security account number.

(2) the provisions of paragraph (1) of this subsection shall not apply with respect to—

(A) any disclosure which is required by Federal statute, or

(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.” Section 7 of the Privacy Act of 1974, as amended, 5 U.S.C. § 552a note (Disclosure of Social Security Number).

Comment:

Section 7 was passed into law as part of the Privacy Act of 1974, Public Law 93–579, 88 Stat 1896. Unlike section 3 of the Privacy Act, however, which Congress designated as an amendment to Title V of the United States Code, Congress made no such statement about section 7. Thus, the reviser of the United States Code placed section 7 in a “Historical and Statutory” note following section 552a. See 5 U.S.C. § 552a (note). The fact that section 7 was never codified and appears only in the “Historical and Statutory Notes” section of the United States Code, does not diminish its weight, however: “The reverse is true: ‘the Code cannot prevail over the Statutes at Large when the two are inconsistent.’” Schwier v. Cox, 340 F.3d 1284, 1288 (11th Cir. 2003) (quoting United States v. Welden, 377 U.S. 95 (1964) (internal quotations omitted)). Therefore, section 7 carries the force of law.

To constitute a violation of section 7, an agency must not only request that an individual disclose a social security number, but also deny a “right, benefit, or privilege” to that individual because of the individual’s refusal to disclose the social security number. See, e.g., El-Bey v. N.C. Bd. of Nursing, No. 1:09CV753, 2009 WL 5220166, at *2 (M.D.N.C. Dec. 31, 2009) (dismissing plaintiff’s “Privacy Act/Social Security Act claim” because “Plaintiff alleges only that Defendants requested his number, not that they denied him a legal right based on its non-disclosure so as to

potentially violate the Privacy Act”); Johnson v. Fleming, No. 95 Civ. 1891, 1996 WL 502410, at *1, 3-4 (S.D.N.Y. Sept. 4, 1996) (finding no violation of section 7(b) notice requirement or section 7(a)(1) because plaintiff did not establish that police officer denied a “right, benefit, or privilege” when plaintiff refused to provide police officer with his social security number).

Although this provision applies beyond federal agencies, it does not apply to: (1) any disclosure which is required by federal statute; or (2) any disclosure of a social security number to any federal, state, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual. See Sec. 7(a)(2)(A)-(B).

A. Exception for Disclosures Required by Federal Statute

Federal, state, and local agencies may deny an individual a right, benefit, or privilege provided by law because of such individual’s refusal to disclose the individual’s social security number if the disclosure is required by federal statute.

A key statute that requires the disclosure of social security numbers is the Social Security Act (SSA), which expressly permits a state agency to use social security numbers for the purpose of identifying individuals “in the administration of any tax, general public assistance, driver’s license, or motor vehicle registration law within its jurisdiction,” see 42 U.S.C. § 405(c)(2)(C)(i) (2018). The SSA also permits a state agency to use social security numbers to issue birth certificates and to enforce child support orders, the Secretary of Agriculture to use social security numbers in administering the Food and Nutrition Act of 2008, and the Federal Crop Insurance Corporation to use them in administering the Federal Crop Insurance Act. See 42 U.S.C. §§ 405(c)(2)(C)(i), (ii), (iii), (iv).

Several courts have interpreted subsection 7(a)(2)(A) as creating an exception to the general requirement that an individual cannot be denied a benefit for failure to disclose a social security number. See Tankersley v. Almand, 837 F.3d 390, 398-399 (4th Cir. 2016) (holding that the Tax Reform Act, 42 U.S.C.

§ 405(c)(2)(C)(i), which authorizes states to require an individual “who is or appears to be [affected by the administration of any tax law within its jurisdiction]” to disclose the individual’s social security number, permitted Maryland to compel plaintiff to provide his social security number to the Client Protection Fund of the Bar of Maryland “on pain of suspension of his law license.”); Peterson v. City of Detroit, 76 F. App’x 601, 602 (6th Cir. 2003) (denying applicant’s assertion that city violated Section 7 of Privacy Act when it denied him taxicab license for failure to provide his social security number on

grounds that, “insofar as [section 7 of the Privacy Act] relates to the ‘privilege’ at issue in this case [denial of plaintiff’s application], has been superceded by a subsequent amendment to the Social Security Act”); Stoianoff v. Comm’r of the DMV, 12 F. App’x 33, 35 (2d Cir. 2001) (finding that plaintiff’s Privacy Act claim would fail because 42 U.S.C. § 405(c)(2)(C)(i) “expressly authorizes states to require the disclosure of social security numbers in the administration of driver’s license programs” and further provides that “any federal law that conflicts with this section is ‘null, void, and of no effect’”); McElrath v. Califano, 615 F.2d 434, 440 (7th Cir. 1980) (finding disclosure of social security number required by regulation that implements Aid to Families with Dependent Children program do not violate Privacy Act); Green v. Philbrook, 576 F.2d 440, 445-46 (2d Cir. 1978) (finding that disclosure of children’s social security numbers required by state program that provided aid to families with children through federal funds did not violate Privacy Act); Ruiz v. Rhode Island, No. CV 16-507WES, 2020 WL 1989266, at *3 (D.R.I. Apr. 27, 2020) (concluding that state had legitimate reason to request social security number because it was required to comply with Medicare, Medicaid and SCHIP Extension Act); Lanzetta v. Woodmansee, 2013 WL 6498403 at *3 (M.D. Fla. Apr. 15, 2013) (dismissing claim that state tax collector’s office violated Section 7(a)(1) by requiring plaintiff to furnish his social security number in order to renew his motorcycle license on ground that such disclosure was mandated by Real ID Act of 2005); Dejeu v. Wash. State Dep’t of Labor and Indus., No. C13-5401RBL, 2013 WL 5437649, at *1-2 (W.D. Wash. Sept. 27, 2013) (finding that “State’s requirement that Plaintiff disclose his Social Security Number in order to register [with State as a contractor] does not violate the Privacy Act” as “[social security] information is statutorily required”); Rodriguez v. Lambert, No. 12-60844, 2012 WL 4838957, at *3 (S.D. Fla. Oct. 11, 2012) (discussing “Florida statute requiring workers to list their social security number” in relation to Section 7); Claugus v. Roosevelt Island Hous. Mgmt. Corp., No. 96CIV8155, 1999 WL 258275, at *4 (S.D.N.Y. Apr. 29, 1999) (considering housing management corporation to be state actor for Privacy Act purposes but finding that Privacy Act does not apply to income verification process for public housing program because of exception created by 42 U.S.C. § 405(c)(2)(C)(i)); In re Turner, 193 B.R. 548, 552-53 (Bankr. N.D. Cal. 1996) (holding that the Bankruptcy Code, 11 U.S.C. § 110(c) (2006), required disclosure of social security number, thus section 7(a) inapplicable; further holding that section 7(b) also was inapplicable “even assuming the [U.S. Trustee] or the clerk of the bankruptcy court were agencies” because no “request” had been made, and the notice requirements therefore not triggered; rather, because disclosure of social security number is required by statute, “the [U.S. Trustee] is enforcing a Congressional directive, not ‘requesting’ anyone’s SSN” and “[t]he clerk receives documents for filing but does not police their content or form or request that certain information be included”); In re Rausch, 197 B.R. 109, 120 (Bankr. D. Nev.

1996) (holding that the Privacy Act “inapplicable” because 11 U.S.C. § 110 “requires placing the SSN upon ‘documents for filing’”).

B. Exception for Laws and Regulations in Effect before January 1, 1975

Federal, state, and local agencies may deny an individual a right, benefit, or privilege provided by law because of such individual's refusal to disclose the individual's social security number if required under statute or regulation adopted prior to January 1, 1975, and used to verify the identity of an individual.

A second exception to the general provisions of section 7 is set out in subsection 7(a)(2)(B), which grandfathers statutes or regulations in effect before January 1, 1975, and provides that the prohibition on denying a benefit because of an individual's failure to provide a social security number does not apply to those statutes and regulations. See Schwier v. Cox, 439 F.3d 1285, 1285-86 (11th Cir. 2006) (holding that section 7(a)(2)(B) grandfather exception did not apply to Georgia voter registration procedures), aff'g 412 F. Supp. 2d 1266 (N.D. Ga. 2005), remanded by 340 F.3d at 1288-89 (explaining that although section 7 is uncodified, it is still present in the Statutes at Large and therefore is not “a dead letter”); McKay v. Thompson, 226 F.3d 752, 755 (6th Cir. 2000) (finding that Tennessee law requiring disclosure of social security number for voter registration fell within section 7(a)(2)'s exception for systems of records in existence prior to January 1, 1975, where disclosure was required under statute or regulation).

C. Federal, State, and Local Government Notice Requirements

Subsection 7(b) specifies the notice that Federal, State, and local agencies are required to give when requesting individuals' social security numbers.

Pursuant to subsection 7(b), an agency that requests that individuals disclose their social security numbers must notify individuals whether the disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it. See Crawford v. U.S. Trustee, 194 F.3d 954, 961-62 (9th Cir. 1999) (rejecting government's argument that because disclosure of plaintiff's social security number was expressly required by federal statute, section 7 was wholly inapplicable, stating that “§ 7(a)(2)(A)'s exclusion for federal statutes only pertains to the limitation recited in § 7(a)(1),” and holding that section 7(b) notice requirements had “no bearing on the public disclosure of [plaintiff's] social security number[] by the government,” which was only issue in dispute); Alcaraz v. Block, 746 F.2d 593, 608-09 (9th Cir. 1984) (finding section 7(b)'s notice provision satisfied where agency informed

“participants of the voluntariness of the disclosure, the source of authority for it and the possible uses to which the disclosed numbers may be put”); GeorgiaCarry.org, Inc. v. Metro. Atlanta Rapid Transit Auth., No. 1:09-CV-594, 2009 WL 5033444, at*9-10 (N.D. Ga. Dec. 14, 2009) (finding “one or both of the [transit authority police] officer Defendants violated section 7(b)” when officers “asked [plaintiff] for his identification, firearms license, and social security number But neither officer told [plaintiff] whether he had to provide his social security number, what authority they relied on in asking for the number, or what the number would be used for”); Szymecki, 2008 WL 4223620, at *9 (concluding that plaintiff stated claim under section 7 where he alleged that city threatened to arrest and incarcerate him if he did not provide his social security number and that city did not inform him why it needed number or how it would be used); Russell v. Bd. of Plumbing Exam’rs, 74 F. Supp. 2d 339, 347 (S.D.N.Y. 1999) (finding violation of section 7 and ordering injunctive relief where defendants neither informed applicants that providing social security number was optional nor provided statutory authority by which number was solicited, and no statutory authority existed); Greidinger v. Davis, 782 F. Supp. 1106, 1108-09 (E.D. Va. 1992) (finding violation of the Privacy Act where state did not provide timely notice in accordance with section 7(b) when collecting social security number for voter registration), rev’d & remanded on other grounds, 988 F.2d 1344 (4th Cir. 1993); Oakes v. IRS, No. 86-2804, 1987 WL 10227, at *1 (D.D.C. Apr. 16, 1987) (finding that agency requesting individual to disclose his social security number was required to inform individual in accordance with section 7(b) but was not required to publish notice in Federal Register); Doyle v. Wilson, 529 F. Supp. 1343, 1348-50 (D. Del. 1982) (finding section 7(b)’s requirements are not fulfilled when no affirmative effort is made to disclose information required under 7(b) “at or before the time the number is requested”); Doe v. Sharp, 491 F. Supp. 346, 347-50 (D. Mass. 1980) (following Green and McElrath regarding section 7(a); finding section 7(b) creates affirmative duty for agencies to inform applicant of uses to be made of social security numbers – “after-the-fact explanations” not sufficient); and Chambers v. Klein, 419 F. Supp. 569, 580 (D.N.J. 1976) (following Green, McElrath, and Doe v. Sharp regarding section 7(a); finding section 7(b) not violated where agency failed to notify applicants of for social security numbers because state had not begun using them pending full implementation of statute requiring their disclosure), aff’d, 564 F.2d 89 (3d Cir. 1977) (unpublished table decision). Cf. Gonzalez, 671 F.3d at 663-64 (concluding that qualified immunity shielded police officers from liability where officers had “asked [plaintiff] for his social security number” but “did not give him the information listed in § 7(b),” as “the officers’ obligation to make the disclosures specified in § 7(b) was not clearly established” at time of plaintiff’s arrest); Doe v. Herman, No. 297CV00043, 1999 WL 1000212, at *9 (W.D. Va. Oct. 29, 1999) (magistrate’s recommendation) (citing Doe v. Sharp and subsection (e)(3) for

proposition that “when an agency solicits a social security number it shall inform the individual of what use will be made of it”), adopted in pertinent part & rev’d in other part, (W.D. Va. July 24, 2000), aff’d in part, rev’d in part, & remanded, on other grounds sub nom. Doe v. Chao, 306 F.3d 170 (4th Cir. 2002), aff’d, 540 U.S. 615 (2004).

D. Causes of Action

Courts have split over whether section 7 provides a cause of action against agencies and, if it does, whether that action is limited to federal agencies.

Jurisdiction to enforce the social security number provision might appear questionable inasmuch as the Privacy Act does not expressly provide for a civil remedy against a nonfederal agency, or for injunctive relief outside of the access and amendment contexts. Courts of appeals in the Sixth and Ninth Circuit have held that section 7 of the Privacy Act applies exclusively to federal agencies and does not provide for causes of action against state and local entities. See Schmitt v. City of Detroit, 395 F.3d 327, 330-31 (6th Cir. 2005) (noting that it was “confronted by two provisions of the Privacy Act that contradict one another to some degree: the statutory definition, which unambiguously contemplates that the Privacy Act applies exclusively to federal agencies, and § 7(b), which by its terms includes state and local agencies within its ambit,” but after looking to legislative history, ultimately holding that Privacy Act applies only to federal agencies); Dittman v. Cal., 191 F.3d 1020, 1026 (9th Cir. 1999) (holding that Privacy Act provides no cause of action against a state licensing entity inasmuch as the private right of civil action created by subsection (g) “is specifically limited to actions against agencies of the United States Government”); Peterson v. Michigan, No. 11-12153, 2011 WL 3516030, at *1 (E.D. Mich. Aug. 11, 2011) (denying plaintiff’s motion to reconsider on grounds that § 7 does not apply to the State of Michigan); Dionicio v. Allison, No. 3:09-cv-00575, 2010 WL 3893816, at *18 (M.D. Tenn. Sept. 30, 2010) (citing Schmitt and granting summary judgment to defendants, agents of the Tennessee Alcohol & Beverage Commission who were sued in their individual and official capacities on grounds that “the civil remedies established by 5 U.S.C. § 552a(g) for violations of the Privacy Act of 1974 extend only to violations by federal agencies”); Treesh v. Cardaris, No. 2:10-CV-437, 2010 WL 3603553, at *3 (S.D. Ohio Sept. 9, 2010) (also citing Schmitt and finding that while the Privacy Act permits an individual to bring a civil action for disclosure of a social security number, that action may only be brought against a federal agency); Warner v. Twp. of S. Harrison, Civ. No. 09-6095, 2010 WL 3001969, at *4 (D.N.J. July 26, 2010) (dismissing plaintiff’s section 7(b) claim against Township because “Plaintiff’s real complaint is Defendants’ widespread, and apparently unjustifiable, dissemination of his

social security number to the public . . . [which is] not covered by Section 7(b), but instead by Section 3. . . . Section 3, however, does not apply to state and local agencies.”); but see Lawson v. Shelby Cnty., Tenn., 211 F.3d 331, 335 (6th Cir. 2000) (holding that “Congress never expressly abrogated state sovereign immunity under the Privacy Act”; however, permitting plaintiffs’ request for prospective injunctive relief [to enforce section 7 of the Privacy Act] against [state] officials” under Ex Parte Young, 209 U.S. 123 (1908)).

Other courts, including the Seventh and Eleventh Circuit Courts of Appeals, have reached the opposite conclusion, however, and have held that the remedial scheme of section 3 of the Privacy Act, which applies strictly to federal agencies, does not apply to section 7, which by its express terms applies to federal, state, and local agencies. See Schwier v. Cox, 340 F.3d 1284, 1292 (11th Cir. 2003); see also Gonzalez v. Vill. of W. Milwaukee, 671 F.3d 649, 661-63 (7th Cir. 2012). In Schwier, the court concluded that “Congress created an ‘unambiguously conferred right’ in section 7 of the Privacy Act,” and it reasoned that section 7 may be enforced under 42 U.S.C. § 1983, which “provides a private right of action whenever an individual has been deprived of any constitutional or statutory federal right under color of state law” as “the remedial scheme of section 3 provides no basis for concluding that Congress intended to preclude private remedies under § 1983 for violations of section 7.” Schwier, 340 F.3d at 1289-90, 1292. Following the Eleventh Circuit’s reasoning in Schwier, the Seventh Circuit in Gonzalez found “no conflict between §§ 3 and 7 [of the Privacy Act]” as “it seems clear that when § 3(a)(1) defines agencies as federal agencies ‘for purposes of this section,’ it refers only to § 3 Accordingly, there is no need to look beyond the unambiguous text of § 7 to determine its applicability. By its express terms, § 7 applies to federal, state, and local agencies.” Gonzalez, 671 F.3d at 662. See also Lanzetta v. Woodmansee, No. 2:13-cv-276, 2013 WL 1610508, at *2 (following Schwier and stating “[a]n individual may also pursue enforcement of his privacy rights under Section 7 of the Privacy Act pursuant to [42 U.S.C. § 1983]; Ingerman v. Del. River Port Auth., 630 F. Supp. 2d 426, 445 (D.N.J. 2009) (ruling that Delaware River Port Authority’s requirement that social security number had to be submitted to receive a senior citizen “E-Z Pass” violated section 7, which was enforceable under Ex Parte Young); Szymecki v. Norfolk, No. 2:08cv142, 2008 WL 4223620, at *9 (E.D. Va. Sept. 11, 2008) (concluding that “because Section 7 confers a legal right on individuals and because Congress did not specifically foreclose a remedy under [42 U.S.C.] § 1983 for violations of Section 7 . . . violations of Section 7 are enforceable under § 1983”); Stollenwerk v. Miller, No. 04-5510, 2006 WL 463393, at *3-7 (E.D. Pa. Feb. 24, 2006) (concluding that state statute requiring submission of social security number to purchase a handgun was invalid, as section 7 is enforceable under 42 U.S.C. § 1983); Libertarian Party v. Ehrler, 776

F. Supp. 1200, 1209 (E.D. Ky. 1991) (requiring that voter include social security number on signature petition violates Privacy Act); cf. Lawson v. Shelby Cnty., Tenn., 211 F.3d at 335 (permitting plaintiffs' request for prospective injunctive relief [to enforce section 7 of the Privacy Act] against [state] officials" under Ex Parte Young, 209 U.S. 123 (1908)); Greidinger v. Almand, 30 F. Supp. 3d 413, 426-27 (D. Md. 2014) (noting that private right of action has been recognized in certain circumstances even though question of whether "an individual has an implied private right of action under 42 U.S.C. § 1983 for the violation of section 7 of the Federal Privacy Act is an open question in the Fourth Circuit") (citing White v. Cain, 2:10-CV-01182, 2011 WL 1087489, at *7 (S.D. W. Va. Mar. 21, 2011)). Contra Treesh, 2010 WL 3603553, at *3 ("[E]ven if disclosure of plaintiff's medical information somehow violated the Privacy Act, [plaintiff] still fails to state a federal claim" because "section 1983 cannot be used to redress violations of the Privacy Act."); Bush v. Lancaster Bureau of Police, No. 07-3172, 2008 WL 3930290, at *7-8 (E.D. Pa. Aug. 28, 2008) (concluding that "Plaintiff cannot state a claim under [42 U.S.C. § 1983] for a violation of subsection (b) of section 7 of the Privacy Act" because "[u]pon review of th[e] statutory language, the court cannot conclude that Congress created an 'unambiguously conferred right'" for individuals).

Other courts also have recognized implied remedies for alleged violations of section 7. See Ky. Rest. Concepts, Inc. v. City of Louisville, Jefferson Cnty. Ky., 209 F. Supp. 2d 672, 687 (W.D. Ky. 2002) (recognizing disagreement but finding that municipality may request social security numbers in adult entertainment applications as part of its regulatory scheme, but also finding that city did not offer any argument that regulation met any of exceptions to enforcement of Privacy Act); McKay v. Altobello, No. 96-3458, 1997 WL 266717, at *1-3, 5 (E.D. La. May 16, 1997) (finding that Commissioner of elections could not require social security numbers from prospective voters as prerequisite to vote because state law did not specifically mention them among items that would sufficiently establish identity); Yeager v. Hackensack Water Co., 615 F. Supp. 1087, 1090-92 (D.N.J. 1985) (concluding that section 7(b) creates implied right of action, in this case against private company whose actions were imputed to state, that "[i]n the absence of a cause of action to enforce section 7(b) in the federal courts, said action would provide an empty right with no means of enforcement. Such would clearly frustrate the intent of Congress.") (citing Greater Cleveland Welfare Rights Org. v. Bauer, 462 F. Supp. 1313, 1319-20 (N.D. Ohio 1978); Wolman v. United States, 501 F. Supp. 310, 311 (D.D.C. 1980) (finding reliance on Section 3 of the Privacy Act to prevent court from exercising injunctive power misplaced and that "traditional equity powers of the Court must be exercised in these circumstances in the absence of any indication from Congress of an intention to limit the Court's inherent power to enforce the law"), remanded, 675 F.2d 1341

(D.C. Cir. 1982) (unpublished table decision), on remand, 542 F. Supp. 84, 85-86 (D.D.C. 1982); Greater Cleveland Welfare Rights Org. v. Bauer, 462 F. Supp. 1313, 1320-21 (N.D. Ohio 1978) (concluding “that Section 7(b) affords plaintiffs an implied right of action for prospective relief”).

Section 7 does not provide for a civil remedy against individuals or private entities. White, No. 2:10-cv-01182, 2011 WL 1087489, at *6-7 (dismissing claim brought against police officer alleging that officer violated section 7 by “requesting the plaintiff’s Social Security Number without providing the plaintiff with adequate information” on ground that “the Privacy Act is not applicable to individuals”); Krebs v. Rutgers, 797 F. Supp. 1246, 1256 (D.N.J. 1992) (finding Rutgers is not a state agency or government-controlled corporation subject to Privacy Act and could not distribute class rosters that listed students by name and social security number).

GOVERNMENT CONTRACTORS

“(1) When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section [Sept. 27, 1995], shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under section 3711(e) of Title 31 shall not be considered a contractor for the purposes of this section.” 5 U.S.C. § 552a(m)(1)-(2)

Comment:

Generally, subsection (m) extends the requirements of the Privacy Act to contractors who maintain a system of records to accomplish the agency’s functions. See generally Pennsylvania Higher Educ. Assistance Agency v. Perez, No. 3:18-CV-1114 (MPS), 2020 WL 2079634, at *12 (D. Conn. Apr. 30, 2020) (citing subsection (m) to conclude that contractor “had no more right to disclose the documents than an employee of the [agency] would have had.”); cf. Boggs v. Se. Tidewater Opportunity Project, No. CIV. A. 2:96CV196, 1996 WL 274381, at *2 (E.D. Va. May 22, 1996) (finding subsection (m) inapplicable where contractor was community action agency that was not “in the business of keeping records for federal agencies” as is required under subsection (m)).

The Federal Acquisition Regulation provides language that must be inserted in solicitations and contracts “[w]hen the design, development, or operation of a system of records on individuals is required to accomplish an agency function.” 48 C.F.R. § 24.104 (2020); see also id. § 52.224-1 to -2. The regulation defines “operation of a system of records” as “performance of any of the activities associated with maintaining the system of records, including the collection, use, and dissemination of records.” Id. at § 52.224-2(c)(1). But cf. Koch v. Schapiro, 777 F. Supp. 2d 86, 91 (D.D.C. 2011) (concluding, in context of claim brought under Rehabilitation Act, that “a contract to investigate complaints of discrimination by employees of the agency on behalf of the [agency’s] EEO Office” is “not a contract for the design or development of a system of records” and therefore is “not the type of contract covered by 48 C.F.R. pt. 24”).

Additionally, see the discussion of subsection (b)(1), “Twelve Exceptions to “No Disclosure without Consent, Conditions Of Disclosure to Third Parties, Need to

Know Within Agency” above, regarding whether contractors are “employees” of an agency for purposes of disclosing a record in a system of records under that subsection.

Even when subsection (m) is applicable, the agency – not the contractor – remains the only proper defendant in a Privacy Act civil lawsuit. *See, e.g., Repetto v. Magellan Health Servs.*, No. 12-4108, 2013 WL 1176470, at *5-6 (D.N.J. Mar. 19, 2013) (rejecting plaintiff’s claims that §subsection (m) permits Privacy Act claims against corporations contracting with government and finding that, had “Congress wanted government contractors to be subject to suit for violations, it could have included word ‘remedies’ in § 552a(m). Instead, Congress deliberately ensured that only agencies were subjects of requirements and remedies, but only extended the Act’s requirements to the government contractors.”); *Patterson v. Austin Med. Ctr.*, No. 97-1241, 1998 WL 35276064, at *2 (D. Minn. Jan. 28, 1998) (finding subsection (m) “does not create a private cause of action against a government contractor for violations of the Act”), *aff’d*, 163 F.3d 602 (8th Cir. Sept. 11, 1998) (unpublished table case); *Adelman v. Discover Card Servs.*, 915 F. Supp. 1163, 1166 (D. Utah 1996) (finding that “a strict construction of ‘employee of the United States’ cannot include employees of state agencies administering a federal program,” and also finding that limited waiver of sovereign immunity afforded by § 552a(g)(1) applies only to federal agencies). *Contra Shannon v. Gen. Elec. Co.*, 812 F. Supp. 308, 315, n.5 (N.D.N.Y. 1993) (noting that “[t]here is no dispute that GE is subject to the requirements of the Privacy Act, inasmuch as it falls within the definition of ‘agency’”).

For additional guidance concerning this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,951, 975-76, https://www.justice.gov/paoverview_omb-75, and the legislative debate reported at 120 Cong. Rec. at 40,408, reprinted in Source Book at 866, https://www.justice.gov/opcl/paoverview_sourcebook.

MAILING LISTS

“An individual’s name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.” 5 U.S.C. § 552a(n).

Comment:

For a decision discussing this provision, see Disabled Officer’s Ass’n v. Rumsfeld, 428 F. Supp. 454, 459 (D.D.C. 1977), aff’d, 574 F.2d 636 (D.C. Cir. 1978) (unpublished table decision). In this case, the court ordered the Department of Defense to release names and addresses of retired disabled officers to the association. The court’s analysis centered on Exemption (b)(6) of the FOIA, but the court also found that subsection (n) did not apply because the agency was not selling or renting the information, and the FOIA required disclosure. For a further discussion of this provision, see OMB 1975 Guidelines, 40 Fed. Reg. at 28,976, https://www.justice.gov/paoverview_omb-75.

ARCHIVAL RECORDS AND NEW SYSTEMS AND MATCHING PROVISIONS

“(1)(1) Archival records.--Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

...

(r) Report on new systems and matching programs.--Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals.” 5 U.S.C. §§ 552a(l), (r).

Comments:

The Privacy Act contains provisions addressing archival records. See 5 U.S.C. § 552a(l); see also OMB 1975 Guidelines, 40 Fed. Reg. at 28,974-75, https://www.justice.gov/paoverview_omb-75. It also includes reporting requirements for new record systems and matching programs, see 5 U.S.C. § 552a(r).

TEXT OF THE PRIVACY ACT OF 1974, AS AMENDED

5 U.S.C § 552a (2018)

THE PRIVACY ACT OF 1974

5 U.S.C. § 552a (2018)

As Amended

§ 552a. Records maintained on individuals

(a) DEFINITIONS. — For purposes of this section —

- (1) the term “agency” means agency as defined in section 552(e)¹ of this title;
- (2) the term “individual” means a citizen of the United States or an alien lawfully admitted for permanent residence;
- (3) the term “maintain” includes maintain, collect, use, or disseminate;
- (4) the term “record” means any 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;
- (5) the term “system of records” means 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;
- (6) the term “statistical record” means a record in a system of records maintained for statistical research or reporting purposes only and not used in whole or in part in making any determination about an identifiable individual, except as provided by section 8 of title 13;
- (7) the term “routine use” means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected;
- (8) the term “matching program” —
 - (A) means any computerized comparison of —

¹ See References in Text note below.

OVERVIEW OF THE PRIVACY ACT

(i) two or more automated systems of records or a system of records with non-Federal records for the purpose of—

(I) establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or

(II) recouping payments or delinquent debts under such Federal benefit programs, or

(ii) two or more automated Federal personnel or payroll systems of records or a system of Federal personnel or payroll records with non-Federal records,

(B) but does not include—

(i) matches performed to produce aggregate statistical data without any personal identifiers;

(ii) matches performed to support any research or statistical project, the specific data of which may not be used to make decisions concerning the rights, benefits, or privileges of specific individuals;

(iii) matches performed, by an agency (or component thereof) which performs as its principal function any activity pertaining to the enforcement of criminal laws, subsequent to the initiation of a specific criminal or civil law enforcement investigation of a named person or persons for the purpose of gathering evidence against such person or persons;

(iv) matches of tax information (I) pursuant to section 6103(d) of the Internal Revenue Code of 1986, (II) for purposes of tax administration as defined in section 6103(b)(4) of such Code, (III) for the purpose of intercepting a tax refund due an individual under authority granted by section 404(e), 464, or 1137 of the Social Security Act; or (IV) for the purpose of intercepting a tax refund due an individual under any other tax refund intercept program authorized by statute which has been determined by the Director of the Office of Management and Budget to contain verification, notice, and hearing requirements that are substantially similar to the procedures in section 1137 of the Social Security Act;

(v) matches—

(I) using records predominantly relating to Federal personnel, that are performed for routine administrative purposes (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)); or

(II) conducted by an agency using only records from systems of records maintained by that agency;

if the purpose of the match is not to take any adverse financial, personnel, disciplinary, or other adverse action against Federal personnel;

(vi) matches performed for foreign counterintelligence purposes or to produce background checks for security clearances of Federal personnel or Federal contractor personnel;

(vii) matches performed incident to a levy described in section 6103(k)(8) of the Internal Revenue Code of 1986;

(viii) matches performed pursuant to section 202(x)(3) or 1611(e)(1) of the Social Security Act (42 U.S.C. 402(x)(3), 1382(e)(1));

(ix) matches performed by the Secretary of Health and Human Services or the Inspector General of the Department of Health and Human Services with respect to potential fraud, waste, and abuse, including matches of a system of records with non-Federal records; or

(x) matches performed pursuant to section 3(d)(4) of the Achieving a Better Life Experience Act of 2014;¹

(9) the term “recipient agency” means any agency, or contractor thereof, receiving records contained in a system of records from a source agency for use in a matching program;

(10) the term “non-Federal agency” means any State or local government, or agency thereof, which receives records contained in a system of records from a source agency for use in a matching program;

(11) the term “source agency” means any agency which discloses records contained in a system of records to be used in a matching program, or any State or local government, or agency thereof, which discloses records to be used in a matching program;

(12) the term “Federal benefit program” means any program administered or funded by the Federal Government, or by any agent or State on behalf of the Federal Government, providing cash or in-kind assistance in the form of payments, grants, loans, or loan guarantees to individuals; and

(13) the term “Federal personnel” means officers and employees of the Government of the United States, members of the uniformed services (including members of the Reserve Components), individuals entitled to receive immediate or deferred retirement benefits under any retirement program of the Government of the United States (including survivor benefits).

(b) CONDITIONS OF DISCLOSURE. — 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, unless disclosure of the record would be —

(1) to those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties;

(2) required under section 552 of this title;

(3) for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section;

(4) to the Bureau of the Census for purposes of planning or carrying out a census or survey or related activity pursuant to the provisions of title 13;

(5) to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable;

(6) to the National Archives and Records Administration as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, or for evaluation by the Archivist of the United States or the designee of the Archivist to determine whether the record has such value;

(7) to another agency or to an instrumentality of any governmental jurisdiction within or under the control of the United States for a civil or criminal law enforcement activity if the activity is authorized by law, and if the head of the agency or instrumentality has made a written request to the agency which

OVERVIEW OF THE PRIVACY ACT

maintains the record specifying the particular portion desired and the law enforcement activity for which the record is sought;

(8) to a person pursuant to a showing of compelling circumstances affecting the health or safety of an individual if upon such disclosure notification is transmitted to the last known address of such individual;

(9) to either House of Congress, or, to the extent of matter within its jurisdiction, any committee or subcommittee thereof, any joint committee of Congress or subcommittee of any such joint committee;

(10) to the Comptroller General, or any of his authorized representatives, in the course of the performance of the duties of the Government Accountability Office;

(11) pursuant to the order of a court of competent jurisdiction; or

(12) to a consumer reporting agency in accordance with section 3711(e) of title 31.

(c) ACCOUNTING OF CERTAIN DISCLOSURES. — Each agency, with respect to each system of records under its control, shall —

(1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of-

(A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and

(B) the name and address of the person or agency to whom the disclosure is made;

(2) retain the accounting made under paragraph (1) of this subsection for at least five years or the life of the record, whichever is longer, after the disclosure for which the accounting is made;

(3) except for disclosures made under subsection (b)(7) of this section, make the accounting made under paragraph (1) of this subsection available to the individual named in the record at his request; and

(4) inform any person or other agency about any correction or notation of dispute made by the agency in accordance with subsection (d) of this section of any record that has been disclosed to the person or agency if an accounting of the disclosure was made.

OVERVIEW OF THE PRIVACY ACT

(d) ACCESS TO RECORDS. — Each agency that maintains a system of records shall —

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

(2) permit the individual to request amendment of a record pertaining to him and —

(A) not later than 10 days (excluding Saturdays, Sundays, and legal public holidays) after the date of receipt of such request, acknowledge in writing such receipt; and

(B) promptly, either —

(i) make any correction of any portion thereof which the individual believes is not accurate, relevant, timely, or complete; or

(ii) inform the individual of its refusal to amend the record in accordance with his request, the reason for the refusal, the procedures established by the agency for the individual to request a review of that refusal by the head of the agency or an officer designated by the head of the agency, and the name and business address of that official;

(3) permit the individual who disagrees with the refusal of the agency to amend his record to request a review of such refusal, and not later than 30 days (excluding Saturdays, Sundays, and legal public holidays) from the date on which the individual requests such review, complete such review and make a final determination unless, for good cause shown, the head of the agency extends such 30-day period; and if, after his review, the reviewing official also refuses to amend the record in accordance with the request, permit the individual to file with the agency a concise statement setting forth the reasons for his disagreement with the refusal of the agency, and notify the individual of the provisions for judicial review of the reviewing official's determination under subsection (g)(1)(A) of this section;

(4) in any disclosure, containing information about which the individual has filed a statement of disagreement, occurring after the filing of the statement

OVERVIEW OF THE PRIVACY ACT

under paragraph (3) of this subsection, clearly note any portion of the record which is disputed and provide copies of the statement and, if the agency deems it appropriate, copies of a concise statement of the reasons of the agency for not making the amendments requested, to persons or other agencies to whom the disputed record has been disclosed; and

(5) nothing in this section shall allow an individual access to any information compiled in reasonable anticipation of a civil action or proceeding.

(e) AGENCY REQUIREMENTS. — Each agency that maintains a system of records shall —

(1) maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President;

(2) collect information to the greatest extent practicable directly from the subject individual when the information may result in adverse determinations about an individual's rights, benefits, and privileges under Federal programs;

(3) inform each individual whom it asks to supply information, on the form which it uses to collect the information or on a separate form that can be retained by the individual —

(A) the authority (whether granted by statute, or by executive order of the President) which authorizes the solicitation of the information and whether disclosure of such information is mandatory or voluntary;

(B) the principal purpose or purposes for which the information is intended to be used;

(C) the routine uses which may be made of the information, as published pursuant to paragraph (4)(D) of this subsection; and

(D) the effects on him, if any, of not providing all or any part of the requested information;

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include —

(A) the name and location of the system;

(B) the categories of individuals on whom records are maintained in the system;

OVERVIEW OF THE PRIVACY ACT

- (C) the categories of records maintained in the system;
 - (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
 - (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
 - (F) the title and business address of the agency official who is responsible for the system of records;
 - (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
 - (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
 - (I) the categories of sources of records in the system;
- (5) maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination;
- (6) prior to disseminating any record about an individual to any person other than an agency, unless the dissemination is made pursuant to subsection (b)(2) of this section, make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes;
- (7) maintain no record describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity;
- (8) make reasonable efforts to serve notice on an individual when any record on such individual is made available to any person under compulsory legal process when such process becomes a matter of public record;
- (9) establish rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of this section, including any other rules and procedures adopted pursuant to this section and the penalties for noncompliance;

OVERVIEW OF THE PRIVACY ACT

(10) establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained;

(11) at least 30 days prior to publication of information under paragraph (4)(D) of this subsection, publish in the Federal Register notice of any new use or intended use of the information in the system, and provide an opportunity for interested persons to submit written data, views, or arguments to the agency; and

(12) if such agency is a recipient agency or a source agency in a matching program with a non-Federal agency, with respect to any establishment or revision of a matching program, at least 30 days prior to conducting such program, publish in the Federal Register notice of such establishment or revision.

(f) AGENCY RULES.—In order to carry out the provisions of this section, each agency that maintains a system of records shall promulgate rules, in accordance with the requirements (including general notice) of section 553 of this title, which shall—

(1) establish procedures whereby an individual can be notified in response to his request if any system of records named by the individual contains a record pertaining to him;

(2) define reasonable times, places, and requirements for identifying an individual who requests his record or information pertaining to him before the agency shall make the record or information available to the individual;

(3) establish procedures for the disclosure to an individual upon his request of his record or information pertaining to him, including special procedure, if deemed necessary, for the disclosure to an individual of medical records, including psychological records, pertaining to him;

(4) establish procedures for reviewing a request from an individual concerning the amendment of any record or information pertaining to the individual, for making a determination on the request, for an appeal within the agency of an initial adverse agency determination, and for whatever additional means may be necessary for each individual to be able to exercise fully his rights under this section; and

(5) establish fees to be charged, if any, to any individual for making copies of his record, excluding the cost of any search for and review of the record. The Office of the Federal Register shall biennially compile and publish the rules promulgated under this subsection and agency notices published under subsection (e)(4) of this section in a form available to the public at low cost.

(g)

(1) CIVIL REMEDIES.—Whenever any agency

(A) makes a determination under subsection (d)(3) of this section not to amend an individual's record in accordance with his request, or fails to make such review in conformity with that subsection;

(B) refuses to comply with an individual request under subsection (d)(1) of this section;

(C) fails to maintain any record concerning any individual with such accuracy, relevance, timeliness, and completeness as is necessary to assure fairness in any determination relating to the qualifications, character, rights, or opportunities of, or benefits to the individual that may be made on the basis of such record, and consequently a determination is made which is adverse to the individual; or

(D) fails to comply with any other provision of this section, or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual,

the individual may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters under the provisions of this subsection.

(2)

(A) In any suit brought under the provisions of subsection (g)(1)(A) of this section, the court may order the agency to amend the individual's record in accordance with his request or in such other way as the court may direct. In such a case the court shall determine the matter de novo.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(3)

(A) In any suit brought under the provisions of subsection (g)(1)(B) of this section, the court may enjoin the agency from withholding the records and order the production to the complainant of any agency records improperly withheld from him. In such a case the court shall determine the matter *de novo*, and may examine the contents of any agency records *in camera* to determine whether the records or any portion thereof may be withheld under any of the exemptions set forth in subsection (k) of this section, and the burden is on the agency to sustain its action.

(B) The court may assess against the United States reasonable attorney fees and other litigation costs reasonably incurred in any case under this paragraph in which the complainant has substantially prevailed.

(4) In any suit brought under the provisions of subsection (g)(1)(C) or (D) of this section in which the court determines that the agency acted in a manner which was intentional or willful, the United States shall be liable to the individual in an amount equal to the sum of—

(A) actual damages sustained by the individual as a result of the refusal or failure, but in no case shall a person entitled to recovery receive less than the sum of \$1,000; and

(B) the costs of the action together with reasonable attorney fees as determined by the court.

(5) An action to enforce any liability created under this section may be brought in the district court of the United States in the district in which the complainant resides, or has his principal place of business, or in which the agency records are situated, or in the District of Columbia, without regard to the amount in controversy, within two years from the date on which the cause of action arises, except that where an agency has materially and willfully misrepresented any information required under this section to be disclosed to an individual and the information so misrepresented is material to establishment of the liability of the agency to the individual under this section, the action may be brought at any time within two years after discovery by the individual of the misrepresentation. Nothing in this section shall be construed to authorize any civil action by reason of any injury sustained as the result of a disclosure of a record prior to September 27, 1975.

(h) RIGHTS OF LEGAL GUARDIAN.—For the purposes of this section, the parent of any minor, or the legal guardian of any individual who has been declared to be

incompetent due to physical or mental incapacity or age by a court of competent jurisdiction, may act on behalf of the individual.

(i)

(1) **CRIMINAL PENALTIES.**— Any officer or employee of an agency, who by virtue of his employment or official position, has possession of, or access to, agency records which contain individually identifiable information the disclosure of which is prohibited by this section or by rules or regulations established thereunder, and who knowing that disclosure of the specific material is so prohibited, willfully discloses the material in any manner to any person or agency not entitled to receive it, shall be guilty of a misdemeanor and fined not more than \$5,000.

(2) Any officer or employee of any agency who willfully maintains a system of records without meeting the notice requirements of subsection (e)(4) of this section shall be guilty of a misdemeanor and fined not more than \$5,000.

(3) Any person who knowingly and willfully requests or obtains any record concerning an individual from an agency under false pretenses shall be guilty of a misdemeanor and fined not more than \$5,000.

(j) **GENERAL EXEMPTIONS.**— The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from any part of this section except subsections (b), (c)(1) and (2), (e)(4)(A) through (F), (e)(6), (7), (9), (10), and (11), and (i) if the system of records is —

(1) maintained by the Central Intelligence Agency; or

(2) maintained by an agency or component thereof which performs as its principal function any activity pertaining to the enforcement of criminal laws, including police efforts to prevent, control, or reduce crime or to apprehend criminals, and the activities of prosecutors, courts, correctional, probation, pardon, or parole authorities, and which consists of (A) information compiled for the purpose of identifying individual criminal offenders and alleged offenders and consisting only of identifying data and notations of arrests, the nature and disposition of criminal charges, sentencing, confinement, release, and parole and probation status; (B) information compiled for the purpose of a criminal investigation, including reports of informants and investigators, and associated with an identifiable individual; or (C) reports identifiable to an individual compiled at any stage of the process of enforcement of the criminal laws from arrest or indictment through release from supervision

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(k) SPECIFIC EXEMPTIONS. — The head of any agency may promulgate rules, in accordance with the requirements (including general notice) of sections 553(b)(1), (2), and (3), (c), and (e) of this title, to exempt any system of records within the agency from subsections (c)(3), (d), (e)(1), (e)(4)(G), (H), and (I) and (f) of this section if the system of records is—

- (1) subject to the provisions of section 552(b)(1) of this title;
- (2) investigatory material compiled for law enforcement purposes, other than material within the scope of subsection (j)(2) of this section: Provided, however, That if any individual is denied any right, privilege, or benefit that he would otherwise be entitled by Federal law, or for which he would otherwise be eligible, as a result of the maintenance of such material, such material shall be provided to such individual, except to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;
- (3) maintained in connection with providing protective services to the President of the United States or other individuals pursuant to section 3056 of title 18;
- (4) required by statute to be maintained and used solely as statistical records;
- (5) investigatory material compiled solely for the purpose of determining suitability, eligibility, or qualifications for Federal civilian employment, military service, Federal contracts, or access to classified information, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence;
- (6) testing or examination material used solely to determine individual qualifications for appointment or promotion in the Federal service the disclosure of which would compromise the objectivity or fairness of the testing or examination process; or

OVERVIEW OF THE PRIVACY ACT

(7) evaluation material used to determine potential for promotion in the armed services, but only to the extent that the disclosure of such material would reveal the identity of a source who furnished information to the Government under an express promise that the identity of the source would be held in confidence, or, prior to the effective date of this section, under an implied promise that the identity of the source would be held in confidence.

At the time rules are adopted under this subsection, the agency shall include in the statement required under section 553(c) of this title, the reasons why the system of records is to be exempted from a provision of this section.

(l)

(1) ARCHIVAL RECORDS.—Each agency record which is accepted by the Archivist of the United States for storage, processing, and servicing in accordance with section 3103 of title 44 shall, for the purposes of this section, be considered to be maintained by the agency which deposited the record and shall be subject to the provisions of this section. The Archivist of the United States shall not disclose the record except to the agency which maintains the record, or under rules established by that agency which are not inconsistent with the provisions of this section.

(2) Each agency record pertaining to an identifiable individual which was transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, prior to the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall not be subject to the provisions of this section, except that a statement generally describing such records (modeled after the requirements relating to records subject to subsections (e)(4)(A) through (G) of this section) shall be published in the Federal Register.

(3) Each agency record pertaining to an identifiable individual which is transferred to the National Archives of the United States as a record which has sufficient historical or other value to warrant its continued preservation by the United States Government, on or after the effective date of this section, shall, for the purposes of this section, be considered to be maintained by the National Archives and shall be exempt from the requirements of this section except subsections (e)(4)(A) through (G) and (e)(9) of this section.

(m)

(1) GOVERNMENT CONTRACTORS.—When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system. For purposes of subsection (i) of this section any such contractor and any employee of such contractor, if such contract is agreed to on or after the effective date of this section, shall be considered to be an employee of an agency.

(2) A consumer reporting agency to which a record is disclosed under section 3711(e) of title 31 shall not be considered a contractor for the purposes of this section.

(n) MAILING LISTS.—An individual's name and address may not be sold or rented by an agency unless such action is specifically authorized by law. This provision shall not be construed to require the withholding of names and addresses otherwise permitted to be made public.

(o) MATCHING AGREEMENTS.—

(1) No record which is contained in a system of records may be disclosed to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written agreement between the source agency and the recipient agency or non-Federal agency specifying—

(A) the purpose and legal authority for conducting the program;

(B) the justification for the program and the anticipated results, including a specific estimate of any savings;

(C) a description of the records that will be matched, including each data element that will be used, the approximate number of records that will be matched, and the projected starting and completion dates of the matching program;

(D) procedures for providing individualized notice at the time of application, and notice periodically thereafter as directed by the Data Integrity Board of such agency (subject to guidance provided by the Director of the Office of Management and Budget pursuant to subsection (v)), to—

(i) applicants for and recipients of financial assistance or payments under Federal benefit programs, and

OVERVIEW OF THE PRIVACY ACT

- (ii) applicants for and holders of positions as Federal personnel, that any information provided by such applicants, recipients, holders, and individuals may be subject to verification through matching programs;
 - (E) procedures for verifying information produced in such matching program as required by subsection (p);
 - (F) procedures for the retention and timely destruction of identifiable records created by a recipient agency or non-Federal agency in such matching program;
 - (G) procedures for ensuring the administrative, technical, and physical security of the records matched and the results of such programs;
 - (H) prohibitions on duplication and redisclosure of records provided by the source agency within or outside the recipient agency or the non-Federal agency, except where required by law or essential to the conduct of the matching program;
 - (I) procedures governing the use by a recipient agency or non-Federal agency of records provided in a matching program by a source agency, including procedures governing return of the records to the source agency or destruction of records used in such program;
 - (J) information on assessments that have been made on the accuracy of the records that will be used in such matching program; and
 - (K) that the Comptroller General may have access to all records of a recipient agency or a non-Federal agency that the Comptroller General deems necessary in order to monitor or verify compliance with the agreement.
- (2)
- (A) A copy of each agreement entered into pursuant to paragraph (1) shall—
 - (i) be transmitted to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives; and
 - (ii) be available upon request to the public.

OVERVIEW OF THE PRIVACY ACT

(B) No such agreement shall be effective until 30 days after the date on which such a copy is transmitted pursuant to subparagraph (A)(i).

(C) Such an agreement shall remain in effect only for such period, not to exceed 18 months, as the Data Integrity Board of the agency determines is appropriate in light of the purposes, and length of time necessary for the conduct, of the matching program.

(D) Within 3 months prior to the expiration of such an agreement pursuant to subparagraph (C), the Data Integrity Board of the agency may, without additional review, renew the matching agreement for a current, ongoing matching program for not more than one additional year if—

(i) such program will be conducted without any change; and

(ii) each party to the agreement certifies to the Board in writing that the program has been conducted in compliance with the agreement.

(p) VERIFICATION AND OPPORTUNITY TO CONTEST FINDINGS. —

(l) In order to protect any individual whose records are used in a matching program, no recipient agency, non-Federal agency, or source agency may suspend, terminate, reduce, or make a final denial of any financial assistance or payment under a Federal benefit program to such individual, or take other adverse action against such individual, as a result of information produced by such matching program, until—

(A)

(i) the agency has independently verified the information; or

(ii) the Data Integrity Board of the agency, or in the case of a non-Federal agency the Data Integrity Board of the source agency, determines in accordance with guidance issued by the Director of the Office of Management and Budget that—

(I) the information is limited to identification and amount of benefits paid by the source agency under a Federal benefit program; and

(II) there is a high degree of confidence that the information provided to the recipient agency is accurate;

OVERVIEW OF THE PRIVACY ACT

(B) the individual receives a notice from the agency containing a statement of its findings and informing the individual of the opportunity to contest such findings; and

(C)

(i) the expiration of any time period established for the program by statute or regulation for the individual to respond to that notice; or

(ii) in the case of a program for which no such period is established, the end of the 30-day period beginning on the date on which notice under subparagraph (B) is mailed or otherwise provided to the individual.

(2) Independent verification referred to in paragraph (1) requires investigation and confirmation of specific information relating to an individual that is used as a basis for an adverse action against the individual, including where applicable investigation and confirmation of—

(A) the amount of any asset or income involved;

(B) whether such individual actually has or had access to such asset or income for such individual's own use; and

(C) the period or periods when the individual actually had such asset or income.

(3) Notwithstanding paragraph (1), an agency may take any appropriate action otherwise prohibited by such paragraph if the agency determines that the public health or public safety may be adversely affected or significantly threatened during any notice period required by such paragraph.

(q) SANCTIONS.—

(1) Notwithstanding any other provision of law, no source agency may disclose any record which is contained in a system of records to a recipient agency or non-Federal agency for a matching program if such source agency has reason to believe that the requirements of subsection (p), or any matching agreement entered into pursuant to subsection (o), or both, are not being met by such recipient agency.

(2) No source agency may renew a matching agreement unless—

(A) the recipient agency or non-Federal agency has certified that it has complied with the provisions of that agreement; and

(B) the source agency has no reason to believe that the certification is inaccurate.

(r) REPORT ON NEW SYSTEMS AND MATCHING PROGRAMS.—Each agency that proposes to establish or make a significant change in a system of records or a matching program shall provide adequate advance notice of any such proposal (in duplicate) to the Committee on Government Operations of the House of Representatives, the Committee on Governmental Affairs of the Senate, and the Office of Management and Budget in order to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals.

(s) BIENNIAL REPORT.—The President shall biennially submit to the Speaker of the House of Representatives and the President pro tempore of the Senate a report—

(1) describing the actions of the Director of the Office of Management and Budget pursuant to section 6 of the Privacy Act of 1974 during the preceding 2 years;

(2) describing the exercise of individual rights of access and amendment under this section during such years;

(3) identifying changes in or additions to systems of records;

(4) containing such other information concerning administration of this section as may be necessary or useful to the Congress in reviewing the effectiveness of this section in carrying out the purposes of the Privacy Act of 1974.

(t)

(1) EFFECT OF OTHER LAWS.—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 otherwise accessible to such individual under the provisions of section 552 of this title.

(u) DATA INTEGRITY BOARDS.—

(1) Every agency conducting or participating in a matching program shall establish a Data Integrity Board to oversee and coordinate among the various components of such agency the agency's implementation of this section.

OVERVIEW OF THE PRIVACY ACT

(2) Each Data Integrity Board shall consist of senior officials designated by the head of the agency, and shall include any senior official designated by the head of the agency as responsible for implementation of this section, and the inspector general of the agency, if any. The inspector general shall not serve as chairman of the Data Integrity Board.

(3) Each Data Integrity Board—

(A) shall review, approve, and maintain all written agreements for receipt or disclosure of agency records for matching programs to ensure compliance with subsection (o), and all relevant statutes, regulations, and guidelines;

(B) shall review all matching programs in which the agency has participated during the year, either as a source agency or recipient agency, determine compliance with applicable laws, regulations, guidelines, and agency agreements, and assess the costs and benefits of such programs;

(C) shall review all recurring matching programs in which the agency has participated during the year, either as a source agency or recipient agency, for continued justification for such disclosures;

(D) shall compile an annual report, which shall be submitted to the head of the agency and the Office of Management and Budget and made available to the public on request, describing the matching activities of the agency, including—

(i) matching programs in which the agency has participated as a source agency or recipient agency;

(ii) matching agreements proposed under subsection (o) that were disapproved by the Board;

(iii) any changes in membership or structure of the Board in the preceding year;

(iv) the reasons for any waiver of the requirement in paragraph (4) of this section for completion and submission of a cost-benefit analysis prior to the approval of a matching program;

(v) any violations of matching agreements that have been alleged or identified and any corrective action taken; and

(vi) any other information required by the Director of the Office of Management and Budget to be included in such report;

(E) shall serve as a clearinghouse for receiving and providing information on the accuracy, completeness, and reliability of records used in matching programs;

(F) shall provide interpretation and guidance to agency components and personnel on the requirements of this section for matching programs;

(G) shall review agency recordkeeping and disposal policies and practices for matching programs to assure compliance with this section; and

(H) may review and report on any agency matching activities that are not matching programs.

(4)

(A) Except as provided in subparagraphs (B) and (C), a Data Integrity Board shall not approve any written agreement for a matching program unless the agency has completed and submitted to such Board a cost-benefit analysis of the proposed program and such analysis demonstrates that the program is likely to be cost effective.²

(B) The Board may waive the requirements of subparagraph (A) of this paragraph if it determines in writing, in accordance with guidelines prescribed by the Director of the Office of Management and Budget, that a cost-benefit analysis is not required.

(C) A cost-benefit analysis shall not be required under subparagraph (A) prior to the initial approval of a written agreement for a matching program that is specifically required by statute. Any subsequent written agreement for such a program shall not be approved by the Data Integrity Board unless the agency has submitted a cost-benefit analysis of the program as conducted under the preceding approval of such agreement.

(5)

(A) If a matching agreement is disapproved by a Data Integrity Board, any party to such agreement may appeal the disapproval to the Director of the Office of Management and Budget. Timely notice of the filing of such an appeal shall be provided by the Director of the Office of Management and Budget to the Committee on Governmental Affairs of the Senate and the Committee on Government Operations of the House of Representatives.

² So in original. Probably should be “cost-effective.”

(B) The Director of the Office of Management and Budget may approve a matching agreement notwithstanding the disapproval of a Data Integrity Board if the Director determines that-

- (i) the matching program will be consistent with all applicable legal, regulatory, and policy requirements;
- (ii) there is adequate evidence that the matching agreement will be cost-effective; and
- (iii) the matching program is in the public interest.

(C) The decision of the Director to approve a matching agreement shall not take effect until 30 days after it is reported to committees described in subparagraph (A).

(D) If the Data Integrity Board and the Director of the Office of Management and Budget disapprove a matching program proposed by the inspector general of an agency, the inspector general may report the disapproval to the head of the agency and to the Congress.

(6) In the reports required by paragraph (3)(D), agency matching activities that are not matching programs may be reported on an aggregate basis, if and to the extent necessary to protect ongoing law enforcement or counterintelligence investigations.

(v) OFFICE OF MANAGEMENT AND BUDGET RESPONSIBILITIES. — The Director of the Office of Management and Budget shall—

- (1) develop and, after notice and opportunity for public comment, prescribe guidelines and regulations for the use of agencies in implementing the provisions of this section; and
- (2) provide continuing assistance to and oversight of the implementation of this section by agencies.

(w) APPLICABILITY TO BUREAU OF CONSUMER FINANCIAL PROTECTION. — Except as provided in the Consumer Financial Protection Act of 2010, this section shall apply with respect to the Bureau of Consumer Financial Protection.

(Added Pub. L. 93-579, § 3, Dec. 31, 1974, 88 Stat. 1897; amended Pub. L. 94-183, § 2(2), Dec. 31, 1975, 89 Stat. 1057; Pub. L. 97-365, § 2, Oct. 25, 1982, 96 Stat. 1749; Pub. L. 97-375, title II, § 201(a), (b), Dec. 21, 1982, 96 Stat. 1821; Pub. L. 97-452, § 2(a)(1), Jan. 12, 1983, 96 Stat. 2478; Pub. L. 98-477, § 2(c), Oct. 15, 1984, 98 Stat. 2211; Pub. L. 98-497, title I, § 107(g), Oct. 19, 1984, 98 Stat. 2292; Pub. L. 100-503, §§ 2-6(a), 7, 8, Oct.

18, 1988, 102 Stat. 2507-2514; Pub. L. 101-508, title VII, § 7201(b)(1), Nov. 5, 1990, 104 Stat. 1388-334; Pub. L. 103-66, title XIII, § 13581(c), Aug. 10, 1993, 107 Stat. 611; Pub. L. 104-193, title I, § 110(w), Aug. 22, 1996, 110 Stat. 2175; Pub. L. 104-226, § 1(b)(3), Oct. 2, 1996, 110 Stat. 3033; Pub. L. 104-316, title I, § 115(g)(2)(B), Oct. 19, 1996, 110 Stat. 3835; Pub. L. 105-34, title X, § 1026(b)(2), Aug. 5, 1997, 111 Stat. 925; Pub. L. 105-362, title XIII, § 1301(d), Nov. 10, 1998, 112 Stat. 3293; Pub. L. 106-170, title IV, § 402(a)(2), Dec. 17, 1999, 113 Stat. 1908; Pub. L. 108-271, § 8(b), July 7, 2004, 118 Stat. 814; Pub. L. 111-148, title VI, § 6402(b)(2), Mar. 23, 2010, 124 Stat. 756; Pub. L. 111-203, title X, § 1082, July 21, 2010, 124 Stat. 2080; Pub. L. 113-295, div. B, title I, § 102(d), Dec. 19, 2014, 128 Stat. 4062.)

REFERENCES IN TEXT

Section 552(e) of this title, referred to in subsec. (a)(1), was redesignated section 552(f) of this title by section 1802(b) of Pub. L. 99-570.

Section 6103 of the Internal Revenue Code of 1986, referred to in subsec. (a)(8)(B)(iv), (vii), is classified to section 6103 of Title 26, Internal Revenue Code.

Sections 404, 464, and 1137 of the Social Security Act, referred to in subsec. (a)(8)(B)(iv), are classified to sections 604, 664, and 1320b-7, respectively, of Title 42, The Public Health and Welfare.

The Achieving a Better Life Experience Act of 2014, referred to in subsec. (a)(8)(B)(x), probably means Pub. L. 113-295, div. B, Dec. 19, 2014, 128 Stat. 4056, known as the Stephen Beck, Jr., Achieving a Better Life Experience Act of 2014 or the Stephen Beck, Jr., ABLE Act of 2014. The Act does not contain a section 3.

For effective date of this section, referred to in subsecs. (k)(2), (5), (7), (1)(2), (3), and (in), see Effective Date note below.

Section 6 of the Privacy Act of 1974, referred to in subsec. (s)(1), is section 6 of Pub. L. 93-579, which was set out below and was repealed by section 6(c) of Pub. L. 100-503.

For classification of the Privacy Act of 1974, referred to in subsec. (s)(4), see Short Title note below.

The Consumer Financial Protection Act of 2010, referred to in subsec. (w), is title X of Pub. L. 111-203, July 21, 2010, 124 Stat. 1955, which enacted subchapter V (§ 5481 et seq.) of chapter 53 of Title 12, Banks and Banking, and enacted and amended numerous other sections and notes in the Code. For complete classification of this Act to the Code, see Short Title note set out under section 5301 of Title 12 and Tables.

CODIFICATION

Section 552a of former Title 5, Executive Departments and Government Officers and Employees, was transferred to section 2244 of Title 7, Agriculture.

AMENDMENTS

2014—Subsec. (a)(8)(B)(x). Pub. L. 113-295 added cl. (x).

2010—Subsec. (a)(8)(B)(ix). Pub. L. 111-148 added cl. (ix).

Subsec. (w). Pub. L. 111-203 added subsec. (w).

2004—Subsec. (b)(10). Pub. L. 108-271 substituted "Government Accountability Office" for "General Accounting Office".

1999—Subsec. (a)(8)(B)(viii). Pub. L. 106-170 added cl. (viii).

1998—Subsec. (u)(6), (7). Pub. L. 105-362 redesignated par. (7) as (6), substituted "paragraph (3)(D)" for "paragraphs (3)(D) and (6)", and struck out former par. (6) which read as follows: "The Director of the Office of Management and Budget shall, annually during the first 3 years after the date of enactment of this subsection and biennially thereafter, consolidate in a report to the Congress the information contained in the reports from the various Data Integrity Boards under paragraph (3)(D) Such report shall include detailed information about costs and benefits of matching programs that are conducted during the period covered by such consolidated report, and shall identify each waiver granted by a Data Integrity Board of the requirement for completion and submission of a cost-benefit analysis and the reasons for granting the waiver."

1997—Subsec. (a)(8)(B)(vii). Pub. L. 105-34 added cl. (vii).

1996—Subsec. (a)(8)(B)(iv)(III). Pub. L. 104-193 substituted "section 404(e), 464," for "section 464".

Subsec. (a)(8)(B)(v) to (vii). Pub. L. 104-226 inserted "or" at end of cl. (v), struck out "or" at end of cl. (vi), and struck out cl. (vii) which read as follows: "matches performed pursuant to section 6103(1)(12) of the Internal Revenue Code of 1986 and section 1144 of the Social Security Act;"

Subsecs. (b)(12), (m)(2). Pub. L. 104-316 substituted "3711(e)" for "3711(f)".

1993—Subsec. (a)(8)(B)(vii). Pub. L. 103-66 added cl. (vii).

1990—Subsec. (p). Pub. L. 101-508 amended subsec. (p) generally, restating former pars. (1) and (3) as par. (1), adding provisions relating to Data Integrity Boards, and restating former pars. (2) and (4) as (2) and (3), respectively.

1988—Subsec. (a)(8) to (13). Pub. L. 100-503, § 5, added pars. (8) to (13).

Subsec. (e)(12). Pub. L. 100-503, § 3(a), added par. (12).

Subsec. (f). Pub. L. 100-503, §7, substituted “biennially” for “annually” in last sentence.

Subsecs. (0) to (q). Pub. L. 100-503, § 2(2), added subsecs. (o) to (q). Former subsecs. (o) to (q) redesignated (r) to (t), respectively.

Subsec. (r). Pub. L. 100-503, § 3(b), inserted “and matching programs” in heading and amended text generally. Prior to amendment, text read as follows: “Each agency shall provide adequate advance notice to Congress and the Office of Management and Budget of any proposal to establish or alter any system of records in order to permit an evaluation of the probable or potential effect of such proposal on the privacy and other personal or property rights of individuals or the disclosure of information relating to such individuals, and its effect on the preservation of the constitutional principles of federalism and separation of powers.”

Pub. L. 100-503, § 2(1), redesignated former subsec. (o) as (r).

Subsec. (s). Pub. L. 100-503, § 8, substituted “Biennial” for “Annual” in heading, “biennially submit” for “annually submit” in introductory provisions, “preceding 2 years” for “preceding year” in par. (1), and “such years” for “such year” in par. (2).

Pub. L. 100-503, § 2(1), redesignated former subsec. (p) as (s).

Subsec. (t). Pub. L. 100-503, § 2(1), redesignated former subsec. (q) as (t).

Subsec. (u). Pub. L. 100-503, § 4, added subsec. (u).

Subsec. (v). Pub. L. 100-503, § 6(a), added subsec. (v).

1984—Subsec. (b)(6). Pub. L. 98-497, § 107(g)(1), substituted “National Archives and Records Administration” for “National Archives of the United States”, and “Archivist of the United States or the designee of the Archivist” for “Administrator of General Services or his designee”.

Subsec. (1)(1). Pub. L. 98-497, §107(g)(2), substituted “Archivist of the United States” for “Administrator of General Services” in two places.

Subsec. (q). Pub. L. 98-477 designated existing provisions as par. (1) and added par. (2).

1983—Subsec. (b)(12). Pub. L. 97-452 substituted “section 3711(f) of title 31” for “section 3(d) of the Federal Claims Collection Act of 1966 (31 U.S.C. 952(d))”.

Subsec. (m)(2). Pub. L. 97-452 substituted “section 3711(f) of title 31” for “section 3(d) of the Federal Claims Collection

Act of 1966 (31 U.S.C. 952(d))”.

1982-Subsec. (b)(12). Pub. L. 97-365, § 2(a), added par. (12).

Subsec. (e)(4). Pub. L. 97-375, §201(a), substituted “upon establishment or revision” for “at least annually” after

“Federal Register”.

Subsec. (m). Pub. L. 97-365, § 2(b), designated existing provisions as par. (1) and added par. (2).

Subsec. (p). Pub. L. 97-375, § 201(b), substituted provisions requiring annual submission of a report by the President to the Speaker of the House and President pro tempore of the Senate relating to the Director of the Office of Management and Budget, individual rights of access, changes or additions to systems of records, and other necessary or useful information, for provisions which had directed the President to submit to the Speaker of the House and the President of the Senate, by June 30 of each calendar year, a consolidated report, separately listing for each Federal agency the number of records contained in any system of records which were exempted from the application of this section under the provisions of subsections (j) and (k) of this section during the preceding calendar year, and the reasons for the exemptions, and such other information as indicate efforts to administer fully this section.

1975—Subsec. (g)(5). Pub. L. 94-183 substituted “to September 27, 1975” for “to the effective date of this section”.

CHANGE OF NAME

Committee on Governmental Affairs of Senate changed to Committee on Homeland Security and Governmental Affairs of Senate, effective Jan. 4, 2005, by Senate Resolution No. 445, One Hundred Eighth Congress, Oct. 9, 2004.

Committee on Government Operations of House of Representatives treated as referring to Committee on Government Reform and Oversight of House of

Representatives by section 1(a) of Pub. L. 104-14, set out as a note preceding section 21 of Title 2, The Congress. Committee on Government Reform and Oversight of House of Representatives changed to Committee on Government Reform of House of Representatives by House Resolution No. 5, One Hundred Sixth Congress, Jan. 6, 1999. Committee on Government Reform of House of Representatives changed to Committee on Oversight and Government Reform of House of Representatives by House Resolution No. 6, One Hundred Tenth Congress, Jan. 5, 2007.

EFFECTIVE DATE OF 2014 AMENDMENT

Pub. L. 113-295, div. B, title I, § 102(f)(1), Dec. 19, 2014, 128 Stat. 4062, provided that: “The amendments made by this section [enacting section 529A of Title 26, Internal Revenue Code, and amending this section, section 5517 of Title 12, Banks and Banking, and sections 26, 877A, 4965, 4973, and 6693 of Title 26] shall apply to taxable years beginning after December 31, 2014.”

EFFECTIVE DATE OF 2010 AMENDMENT

Pub. L. 111-203, title X, § 1082, July 21, 2010, 124 Stat. 2080, provided that the amendment made by section 1082 is effective on July 21, 2010.

Pub. L. 111-203, title X, §1100H, July 21, 2010, 124 Stat. 2113, provided that: “Except as otherwise provided in this subtitle [subtitle H (§§ 1081-1100H) of title X of Pub. L. 111-203, see Tables for classification] and the amendments made by this subtitle, this subtitle and the amendments made by this subtitle, other than sections 1081 [amending section 8G of Pub. L. 95-452, set out in the Appendix to this title, and enacting provisions set out as a note under section 8G of Pub. L. 95-452] and 1082 [amending this section and enacting provisions set out as a note under this section], shall become effective on the designated transfer date.”

[The term “designated transfer date” is defined in section 5481(9) of Title 12, Banks and Banking, as the date established under section 5582 of Title 12, which is July 21, 2011.]

EFFECTIVE DATE OF 1999 AMENDMENT

Amendment by Pub. L. 106-170 applicable to individuals whose period of confinement in an institution commences on or after the first day of the fourth month beginning after December 1999, see section 402(a)(4) of Pub. L. 106-170, set out as a note under section 402 of Title 42, The Public Health and Welfare.

EFFECTIVE DATE OF 1997 AMENDMENT

Amendment by Pub. L. 105-34 applicable to levies issued after Aug. 5, 1997, see section 1026(c) of Pub. L. 105-34, set out as a note under section 6103 of Title 26, Internal Revenue Code.

EFFECTIVE DATE OF 1996 AMENDMENT

Amendment by Pub. L. 104-193 effective July 1, 1997, with transition rules relating to State options to accelerate such date, rules relating to claims, actions, and proceedings commenced before such date, rules relating to closing out of accounts for terminated or substantially modified programs and continuance in office of Assistant Secretary for Family Support, and provisions relating to termination of entitlement under AFDC program, see section 116 of Pub. L. 104-193, as amended, set out as an Effective Date note under section 601 of Title 42, The Public Health and Welfare.

EFFECTIVE DATE OF 1993 AMENDMENT

Amendment by Pub. L. 103-66 effective Jan. 1, 1994, see section 13581(d) of Pub. L. 103-66, set out as a note under section 1395y of Title 42, The Public Health and Welfare.

EFFECTIVE DATE OF 1988 AMENDMENT

Pub. L. 100-503, § 10, Oct. 18, 1988, 102 Stat. 2514, as amended by Pub. L. 101-56, § 2, July 19, 1989, 103 Stat. 149, provided that:

“(a) IN GENERAL. — Except as provided in subsections (b) and (c), the amendments made by this Act [amending this section and repealing provisions set out as a note below] shall take effect 9 months after the date of enactment of this Act [Oct. 18, 1988].

“(b) EXCEPTIONS. — The amendment made by sections 3(b), 6, 7, and 8 of this Act [amending this section and repealing provisions set out as a note below] shall take effect upon enactment.

“(c) EFFECTIVE DATE DELAYED FOR EXISTING PROGRAMS. — In the case of any matching program (as defined in section 552a(a)(8) of title 5, United States Code, as added by section 5 of this Act) in operation before June 1, 1989, the amendments made by this Act (other than the amendments described in subsection (b)) shall take effect January 1, 1990, if-

“(1) such matching program is identified by an agency as being in operation before June 1, 1989; and

“(2) such identification is—

“(A) submitted by the agency to the Committee on Governmental Affairs of the Senate, the Committee on Government Operations of the House of Representatives, and the Office of Management and Budget before August 1, 1989, in a report which contains a schedule showing the dates on which the agency expects to have such matching program in compliance with the amendments made by this Act, and

“(B) published by the Office of Management and Budget in the Federal Register, before September 15, 1989.”

EFFECTIVE DATE OF 1984 AMENDMENT

Amendment by Pub. L. 98-497 effective Apr. 1, 1985, see section 301 of Pub. L. 98-497, set out as a note under section 2102 of Title 44, Public Printing and Documents.

EFFECTIVE DATE

Pub. L. 93-579, §8, Dec. 31, 1974, 88 Stat. 1910, provided that: “The provisions of this Act [enacting this section and provisions set out as notes under this section] shall be effective on and after the date of enactment [Dec. 31, 1974], except that the amendments made by sections 3 and 4 [enacting this section and amending analysis preceding section 500 of this title] shall become effective 270 days following the day on which this Act is enacted.”

SHORT TITLE OF 1990 AMENDMENT

Pub. L. 101-508, title VII, § 7201(a), Nov. 5, 1990, 104 Stat. 1388-334, provided that: “This section [amending this section and enacting provisions set out as notes below] may be cited as the ‘Computer Matching and Privacy Protection Amendments of 1990’.”

SHORT TITLE OF 1989 AMENDMENT

Pub. L. 101-56, § 1, July 19, 1989, 103 Stat. 149, provided that: “This Act [amending section 10 of Pub. L. 100-503, set out as a note above] may be cited as the ‘Computer Matching and Privacy Protection Act Amendments of 1989’.”

SHORT TITLE OF 1988 AMENDMENT

Pub. L. 100-503, § 1, Oct. 18, 1988, 102 Stat. 2507, provided that: “This Act [amending this section, enacting provisions set out as notes above and below, and repealing provisions set out as a note below] may be cited as the ‘Computer Matching and Privacy Protection Act of 1988’.”

SHORT TITLE OF 1974 AMENDMENT

Pub. L. 93-579, §1, Dec. 31, 1974, 88 Stat. 1896, provided: “That this Act [enacting this section and provisions set out as notes under this section] may be cited as the ‘Privacy Act of 1974’.”

SHORT TITLE

This section is popularly known as the “Privacy Act” and the “Privacy Act of 1974”.

TERMINATION OF REPORTING REQUIREMENTS

For termination, effective May 15, 2000, of reporting provisions in subsec. (s) of this section, see section 3003 of Pub. L. 104-66, as amended, set out as a note under section 1113 of Title 31, Money and Finance, and page 31 of House Document No. 103-7.

DELEGATION OF FUNCTIONS

Functions of Director of Office of Management and Budget under this section delegated to Administrator for Office of Information and Regulatory Affairs by section 3 of Pub. L. 96-511, Dec. 11, 1980, 94 Stat. 2825, set out as a note under section 3503 of Title 44, Public Printing and Documents.

EXTENSION OF PRIVACY ACT REMEDIES TO CITIZENS OF DESIGNATED COUNTRIES

Pub. L. 114-126, Feb. 24, 2016, 130 Stat. 282, provided that:

“SECTION 1. SHORT TITLE.

“This Act may be cited as the ‘Judicial Redress Act of 2015’.

“SEC. 2. EXTENSION OF PRIVACY ACT REMEDIES TO CITIZENS OF DESIGNATED COUNTRIES.

“(a) CIVIL ACTION; CIVIL REMEDIES.-With respect to covered records, a covered person may bring a civil action against an agency and obtain civil remedies, in the same manner, to the same extent, and subject to the same limitations, including exemptions and exceptions, as an individual may bring and obtain with respect to records under—

“(1) section 552a(g)(1)(D) of title 5, United States Code, but only with respect to disclosures intentionally or willfully made in violation of section 552a(b) of such title; and

OVERVIEW OF THE PRIVACY ACT

“(2) subparagraphs (A) and (B) of section 552a(g)(1) of title 5, United States Code, but such an action may only be brought against a designated Federal agency or component.

“(b) EXCLUSIVE REMEDIES.-The remedies set forth in subsection (a) are the exclusive remedies available to a covered person under this section.

“(c) APPLICATION OF THE PRIVACY ACT WITH RESPECT TO A COVERED PERSON.—For purposes of a civil action described in subsection (a), a covered person shall have the same rights, and be subject to the same limitations, including exemptions and exceptions, as an individual has and is subject to under section 552a of title 5, United States Code, when pursuing the civil remedies described in paragraphs (1) and (2) of subsection (a).

“(d) DESIGNATION OF COVERED COUNTRY.-

“(1) IN GENERAL.-The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, designate a foreign country or regional economic integration organization, or member country of such organization, as a ‘covered country’ for purposes of this section if—

“(A)(i) the country or regional economic integration organization, or member country of such organization, has entered into an agreement with the United States that provides for appropriate privacy protections for information shared for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses; or

“(ii) the Attorney General has determined that the country or regional economic integration organization, or member country of such organization, has effectively shared information with the United States for the purpose of preventing, investigating, detecting, or prosecuting criminal offenses and has appropriate privacy protections for such shared information;

“(B) the country or regional economic integration organization, or member country of such organization, permits the transfer of personal data for commercial purposes between the territory of that country or regional economic organization and the territory of the United States, through an agreement with the United States or otherwise; and

“(C) the Attorney General has certified that the policies regarding the transfer of personal data for commercial purposes and related actions of

the country or regional economic integration organization, or member country of such organization, do not materially impede the national security interests of the United States.

“(2) REMOVAL OF DESIGNATION. — The Attorney General may, with the concurrence of the Secretary of State, the Secretary of the Treasury, and the Secretary of Homeland Security, revoke the designation of a foreign country or regional economic integration organization, or member country of such organization, as a ‘covered country’ if the Attorney General determines that such designated ‘covered country’ —

“(A) is not complying with the agreement described under paragraph (1)(A)(i);

“(B) no longer meets the requirements for designation under paragraph (1)(A)(ii);

“(C) fails to meet the requirements under paragraph (1)(B);

“(D) no longer meets the requirements for certification under paragraph (1)(C); or

“(E) impedes the transfer of information (for purposes of reporting or preventing unlawful activity) to the United States by a private entity or person.

“(e) DESIGNATION OF DESIGNATED FEDERAL AGENCY OR COMPONENT. —

“(1) IN GENERAL. — The Attorney General shall determine whether an agency or component thereof is a ‘designated Federal agency or component’ for purposes of this section. The Attorney General shall not designate any agency or component thereof other than the Department of Justice or a component of the Department of Justice without the concurrence of the head of the relevant agency, or of the agency to which the component belongs.

“(2) REQUIREMENTS FOR DESIGNATION. — The Attorney General may determine that an agency or component of an agency is a ‘designated Federal agency or component’ for purposes of this section, if—

“(A) the Attorney General determines that information exchanged by such agency with a covered country is within the scope of an agreement referred to in subsection (d)(1)(A); or

“(B) with respect to a country or regional economic integration organization, or member country of such organization, that has been

designated as a ‘covered country’ under subsection (d)(1)(B), the Attorney General determines that designating such agency or component thereof is in the law enforcement interests of the United States.

“(f) FEDERAL REGISTER REQUIREMENT; NONREVIEWABLE DETERMINATION. — The Attorney General shall publish each determination made under subsections (d) and (e). Such determination shall not be subject to judicial or administrative review.

“(g) JURISDICTION.—The United States District Court for the District of Columbia shall have exclusive jurisdiction over any claim arising under this section.

“(h) DEFINITIONS. — In this Act:

“(1) AGENCY.—The term ‘agency’ has the meaning given that term in section 552(f) of title 5, United States Code.

“(2) COVERED COUNTRY. — The term ‘covered country’ means a country or regional economic integration organization, or member country of such organization, designated in accordance with subsection (d).

“(3) COVERED PERSON.—The term ‘covered person’ means a natural person (other than an individual) who is a citizen of a covered country.

“(4) COVERED RECORD.—The term ‘covered record’ has the same meaning for a covered person as a record has for an individual under section 552a of title 5, United States Code, once the covered record is transferred —

“(A) by a public authority of, or private entity within, a country or regional economic organization, or member country of such organization, which at the time the record is transferred is a covered country; and

“(B) to a designated Federal agency or component for purposes of preventing, investigating, detecting, or prosecuting criminal offenses.

“(5) DESIGNATED FEDERAL AGENCY OR COMPONENT. — The term ‘designated Federal agency or component’ means a Federal agency or component of an agency designated in accordance with subsection (e).

“(6) INDIVIDUAL. — The term ‘individual’ has the meaning given that term in section 552a(a)(2) of title 5, United States Code.

“(i) PRESERVATION OF PRIVILEGES. — Nothing in this section shall be construed to waive any applicable privilege or require the disclosure of classified information.

Upon an agency's request, the district court shall review in camera and ex parte any submission by the agency in connection with this subsection.

“(j) EFFECTIVE DATE.—This Act shall take effect 90 days after the date of the enactment of this Act [Feb. 24, 2016].”

PUBLICATION OF GUIDANCE UNDER SUBSECTION (p)(1)(A)(ii)

Pub. L. 101-508, title VII, § 7201(b)(2), Nov. 5, 1990, 104 Stat. 1388-334, provided that: “Not later than 90 days after the date of the enactment of this Act [Nov. 5, 1990], the Director of the Office of Management and Budget shall publish guidance under subsection (p)(1)(A)(ii) of section 552a of title 5, United States Code, as amended by this Act.”

LIMITATION ON APPLICATION OF VERIFICATION REQUIREMENT

Pub. L. 101-508, title VII, § 7201(c), Nov. 5, 1990, 104 Stat. 1388-335, provided that: “Section 552a(p)(1)(A)(ii)(II) of title 5, United States Code, as amended by section 2 [probably means section 7201(b)(1) of Pub. L. 101-508], shall not apply to a program referred to in paragraph (1), (2), or (4) of section 1137(b) of the Social Security Act (42 U.S.C. 1320b-7), until the earlier of—

“(1) the date on which the Data Integrity Board of the Federal agency which administers that program determines that there is not a high degree of confidence that information provided by that agency under Federal matching programs is accurate; or

“(2) 30 days after the date of publication of guidance under section 2(b) [probably means section 7201(b)(2) of Pub. L. 101-508, set out as a note above].”

**EFFECTIVE DATE DELAYED FOR CERTAIN EDUCATION BENEFITS
COMPUTER MATCHING PROGRAMS**

Pub. L. 101-366, title II, § 206(d), Aug. 15, 1990, 104 Stat. 442, provided that:

“(1) In the case of computer matching programs between the Department of Veterans Affairs and the Department of Defense in the administration of education benefits programs under chapters 30 and 32 of title 38 and chapter 106 of title 10, United States Code, the amendments made to section 552a of title 5, United States Code, by the Computer Matching and Privacy Protection Act of 1988 [Pub. L. 100-503] (other than the amendments made by section 10(b) of that Act) [see Effective Date of 1988 Amendment note above] shall take effect on October 1, 1990.

“(2) For purposes of this subsection, the term ‘matching program’ has the same meaning provided in section 552a(a)(8) of title 5, United States Code.”

IMPLEMENTATION GUIDANCE FOR 1988 AMENDMENTS

Pub. L. 100-503, § 6(b), Oct. 18, 1988, 102 Stat. 2513, provided that: “The Director shall, pursuant to section 552a(v) of title 5, United States Code, develop guidelines and regulations for the use of agencies in implementing the amendments made by this Act [amending this section and repealing provisions set out as a note below] not later than 8 months after the date of enactment of this Act [Oct. 18, 1988].”

CONSTRUCTION OF 1988 AMENDMENTS

Pub. L. 10--503, § 9, Oct. 18, 1988, 102 Stat. 2514, provided that: “Nothing in the amendments made by this Act [amending this section and repealing provisions set out as a note below] shall be construed to authorize—

“(1) the establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies;

“(2) the direct linking of computerized systems of records maintained by Federal agencies;

“(3) the computer matching of records not otherwise authorized by law; or

“(4) the disclosure of records for computer matching except to a Federal, State, or local agency.”

CONGRESSIONAL FINDINGS AND STATEMENT OF PURPOSE

Pub. L. 93-579, § 2, Dec. 31, 1974, 88 Stat. 1896, provided that:

“(a) The Congress finds that—

“(1) the privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies;

“(2) the increasing use of computers and sophisticated information technology, while essential to the efficient operations of the Government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information;

“(3) the opportunities for an individual to secure employment, insurance, and credit, and his right to due process, and other legal protections are endangered by the misuse of certain information systems;

“(4) the right to privacy is a personal and fundamental right protected by the Constitution of the United States; and

“(5) in order to protect the privacy of individuals identified in information systems maintained by Federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies.

“(b) The purpose of this Act [enacting this section and provisions set out as notes under this section] is to provide certain safeguards for an individual against an invasion of personal privacy by requiring Federal agencies, except as otherwise provided by law, to-

“(1) permit an individual to determine what records pertaining to him are collected, maintained, used, or disseminated by such agencies;

“(2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent;

“(3) permit an individual to gain access to information pertaining to him in Federal agency records, to have a copy made of all or any portion thereof, and to correct or amend such records;

“(4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information;

“(5) permit exemptions from the requirements with respect to records provided in this Act only in those cases where there is an important public policy need for such exemption as has been determined by specific statutory authority; and

“(6) be subject to civil suit for any damages which occur as a result of willful or intentional action which violates any individual’s rights under this Act.”

PRIVACY PROTECTION STUDY COMMISSION

Pub. L. 93-579, § 5, Dec. 31, 1974, 88 Stat. 1905, as amended by Pub. L. 95-38, June 1, 1977, 91 Stat. 179, which established the Privacy Protection Study Commission and provided that the Commission study data banks, automated data processing programs and information systems of governmental, regional and private organizations to determine standards and procedures in force for protection of

personal information, that the Commission report to the President and Congress the extent to which requirements and principles of section 552a of title 5 should be applied to the information practices of those organizations, and that it make other legislative recommendations to protect the privacy of individuals while meeting the legitimate informational needs of government and society, ceased to exist on September 30, 1977, pursuant to section 5(g) of Pub. L. 93-579.

GUIDELINES AND REGULATIONS FOR MAINTENANCE OF PRIVACY AND PROTECTION OF RECORDS OF INDIVIDUALS

Pub. L. 93-579, § 6, Dec. 31, 1974, 88 Stat. 1909, which provided that the Office of Management and Budget shall develop guidelines and regulations for use of agencies in implementing provisions of this section and provide continuing assistance to and oversight of the implementation of the provisions of such section by agencies, was repealed by Pub. L. 100-503, § 6(c), Oct. 18, 1988, 102 Stat. 2513.

DISCLOSURE OF SOCIAL SECURITY NUMBER

Pub. L. 93-579, §7, Dec. 31, 1974, 88 Stat. 1909, provided that:

“(a)(1) It shall be unlawful for any Federal, State or local government agency to deny to any individual any right, benefit, or privilege provided by law because of such individual’s refusal to disclose his social security account number.

“(2) the [The] provisions of paragraph (1) of this subsection shall not apply with respect to-

“(A) any disclosure which is required by Federal statute, or

“(B) the disclosure of a social security number to any Federal, State, or local agency maintaining a system of records in existence and operating before January 1, 1975, if such disclosure was required under statute or regulation adopted prior to such date to verify the identity of an individual.

“(b) Any Federal, State, or local government agency which requests an individual to disclose his social security account number shall inform that individual whether that disclosure is mandatory or voluntary, by what statutory or other authority such number is solicited, and what uses will be made of it.”

AUTHORIZATION OF APPROPRIATIONS TO PRIVACY PROTECTION STUDY COMMISSION

Pub. L. 93-579, § 9, Dec. 31, 1974, 88 Stat. 1910, as amended by Pub. L. 94-394, Sept. 3, 1976, 90 Stat. 1198, authorized appropriations for the period beginning July 1, 1975, and ending on September 30, 1977.

Ex. ORD. NO. 9397. NUMBERING SYSTEM FOR FEDERAL ACCOUNTS
RELATING TO INDIVIDUAL PERSONS

Ex. Ord. No. 9397, Nov. 22, 1943, 8 F.R. 16095, as amended by Ex. Ord. No. 13478, § 2, Nov. 18, 2008, 73 F.R. 70239, provided:

WHEREAS certain Federal agencies from time to time require in the administration of their activities a system of numerical identification of accounts of individual persons; and

WHEREAS some seventy million persons have heretofore been assigned account numbers pursuant to the Social Security Act; and

WHEREAS a large percentage of Federal employees have already been assigned account numbers pursuant to the Social Security Act; and

WHEREAS it is desirable in the interest of economy and orderly administration that the Federal Government move towards the use of a single, unduplicated numerical identification system of accounts and avoid the unnecessary establishment of additional systems:

NOW, THEREFORE, by virtue of the authority vested in me as President of the United States, it is hereby ordered as follows:

1. Hereafter any Federal department, establishment, or agency may, whenever the head thereof finds it advisable to establish a new system of permanent account numbers pertaining to individual persons, utilize the Social Security Act account numbers assigned pursuant to title 20, section 422.103 of the Code of Federal Regulations and pursuant to paragraph 2 of this order.
2. The Social Security Administration shall provide for the assignment of an account number to each person who is required by any Federal agency to have such a number but who has not previously been assigned such number by the Administration. The Administration may accomplish this purpose by (a) assigning such numbers to individual persons, (b) assigning blocks of numbers to Federal agencies for reassignment to individual persons, or (c) making such other arrangements for the assignment of numbers as it may deem appropriate.
3. The Social Security Administration shall furnish, upon request of any Federal agency utilizing the numerical identification system of accounts provided for in this order, the account number pertaining to any person with whom such agency has an account or the name and other identifying data pertaining to any account number of any such person.

OVERVIEW OF THE PRIVACY ACT

4. The Social Security Administration and each Federal agency shall maintain the confidential character of information relating to individual persons obtained pursuant to the provisions of this order.
5. There shall be transferred to the Social Security Administration, from time to time, such amounts as the Director of the Office of Management and Budget shall determine to be required for reimbursement by any Federal agency for the services rendered by the Administration pursuant to the provisions of this order.
6. This order shall be implemented in accordance with applicable law and subject to the availability of appropriations.
7. This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity, by any party against the United States, its departments, agencies, instrumentalities, or entities, its officers, employees, or agents, or any other person.
8. This order shall be published in the Federal Register.

CLASSIFIED NATIONAL SECURITY INFORMATION

For provisions relating to a response to a request for information under this section when the fact of its existence or nonexistence is itself classified or when it was originally classified by another agency, see Ex. Ord. No. 13526, § 3.6, Dec. 29, 2009, 75 F.R. 718, set out as a note under section 3161 of Title 50, War and National Defense.