UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

GILBERTE JILL KELLEY *et al.*,

Plaintiffs,

v.

THE FEDERAL BUREAU OF INVESTIGATION *et al.*,

Defendants.

Civil Action No. 13-cv-825 (ABJ)

DEFENDANTS' MOTION TO DISMISS COUNTS I THROUGH VII OF PLAINTIFFS' COMPLAINT

Pursuant to Rules 12(b)(1) and 12(b)(6) of the Federal Rules of Civil Procedure, defendants, the Federal Bureau of Investigation, Robert S. Mueller, III, in his official capacity as the Director of the FBI, the Department of Defense, and the United States of America respectfully move to dismiss Counts I through VII of plaintiffs' complaint, ECF No 1, for lack of subject matter jurisdiction and for failure to state a claim upon which relief can be granted. Points and authorities in support of defendants' motion are presented in the attached Memorandum in Support.

September 24, 2013

Respectfully Submitted,

STUART F. DELERY
Assistant Attorney General

JOHN R. TYLER
Assistant Branch Director

/s/ *Peter J. Phipps*
PETER J. PHIPPS (DC Bar #502904)
Senior Trial Counsel
U.S. Department of Justice, Civil Division

Federal Programs Branch
Tel: (202) 616-8482
Fax: (202) 616-8470
Email: peter.phipps@usdoj.gov

Mailing Address:
P.O. Box 883 Ben Franklin Station
Washington, DC 20044

Courier Address:
20 Massachusetts Ave., NW
Washington, DC 20001

Attorneys for Defendants

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

GILBERTE JILL KELLEY *et al.*,

Plaintiffs,

v.

THE FEDERAL BUREAU OF INVESTIGATION *et al.*,

Defendants.

Civil Action No. 13-cv-825 (ABJ)

MEMORANDUM IN SUPPORT OF DEFENDANTS' MOTION TO DISMISS COUNTS I THROUGH VII OF PLAINTIFFS' COMPLAINT

STUART F. DELERY
Assistant Attorney General

JOHN R. TYLER
Assistant Branch Director

PETER J. PHIPPS
Senior Trial Counsel
U.S. Department of Justice
Civil Division
Federal Programs Branch
P.O. Box 883, Ben Franklin Station
Washington, DC 20044
Tel: (202) 616-8482
Fax: (202) 616-8470
Email: peter.phipps@usdoj.gov

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

RULES

REGULATIONS

INTRODUCTION

The lengthy and narrative complaint filed by Jill Kelley and Scott Kelly is not a "short and plain statement" of claims. Fed. R. Civ. P. 8(a)(2). Nor does it demonstrate that "the pleader is entitled to relief." *Id.* Indeed, plaintiffs' complaint does not set forth facts, which when assumed true, would satisfy the substantive and procedural requirements of the two highly technical statutes, the Privacy Act and the Stored Communications Act, upon which plaintiffs base their claims. Because plaintiffs do not plausibly allege requisite elements of their claims against the Federal Bureau of Investigation and its Director in his official capacity (collectively, the "FBI"), the Department of Defense (the "DoD"), and the United States, Counts I through VII, the only counts for which plaintiffs have perfected service, should be dismissed.

Some of plaintiffs' claims fail on their face to establish necessary elements of this Court's subject matter jurisdiction. With respect to the named defendants, plaintiffs' complaint exceeds the scope of the relevant waivers of sovereign immunity. The United States cannot be sued under the Privacy Act, and federal agencies, including the FBI and the DoD, cannot be sued under the Stored Communications Act. Plaintiffs have also neglected a necessary prerequisite for a claim under the Stored Communications Act: presentment of the claim to the relevant federal agency. Without having alleged such a presentment, plaintiffs are jurisdictionally barred from litigating that claim here.

Beyond its jurisdictional deficiencies, the complaint fails to state necessary elements of plaintiffs' claims. Most broadly, Scott Kelley should be dismissed as a plaintiff because the complaint does not allege the maintenance of records about him. As statutorily defined, the term "record" has a specialized meaning, which lies at the foundation of plaintiffs' claims under the

Privacy Act and the Stored Communications Act. But because plaintiffs' do not plausibly allege facts to sustain that critical element, Scott Kelley's claims should be dismissed.

Plaintiffs' claims under the Privacy Act suffer from other shortcomings as well. By its structure, the Privacy Act provides location-based protections: only records within non-exempt systems of records are within its general coverage. Plaintiffs' allegations neglect that important requirement to their detriment. For instance, disclosure claims under the Privacy Act are governed by a rule of retrieval – to be actionable, disclosed information about an individual must have been retrieved from a protected system of records. But plaintiffs fail to make allegations to satisfy the retrieval rule, and that omission prevents plaintiffs from stating a claim for a wrongful disclosure. Plaintiffs' allegations also fail to account for the Privacy Act's other location-based protections. Specifically, the Privacy Act permits agencies to exempt certain of their record systems from several of the Privacy Act's requirements, and claims for improper maintenance and adverse determinations can be brought only with regard to non-exempt records. Both the FBI and the DoD have exempted several relevant systems of records from those obligations. But plaintiffs do not allege that the information upon which they base their claims was maintained in any non-exempt location. Nor do plaintiffs allege that the FBI or the DoD made an adverse determination about them based on records in a non-exempt location.

Plaintiffs' remaining counts fare no better. Plaintiffs premise two of their Privacy Act claims on the allegation that a sworn statement given by an FBI agent omitted a detail regarding Jill Kelley, and consequently, according to plaintiffs, the statement was inaccurate and incomplete. But plaintiffs do not establish that such information was relevant to the FBI's law enforcement investigation. As an irrelevant fact, that omission had no plausible impact on the accuracy or completeness of the FBI records, much less any records maintained by the DoD.

Plaintiffs also assert that the FBI and the DoD maintained records regarding their exercise of First Amendment rights in violation of the Privacy Act, but plaintiffs do not appreciate the broad scope of the law enforcement exception to that Privacy Act provision. Because the information at issue was related to law enforcement investigations that the FBI and the DoD were conducting, it was outside of the Privacy Act's protections. Finally, plaintiffs claim that the FBI and the DoD failed to establish Privacy Act safeguards, but the public record belies that claim: both the FBI and the DoD have promulgated numerous rules and regulations to safeguard Privacy Act protected information. In sum, in their lawsuit, plaintiffs seek to avail themselves of the highly technical protections provided by the Privacy Act, but their allegations, even when liberally construed, do not sustain the claims they attempt to bring.

FACTUAL BACKGROUND

As alleged in the Complaint, plaintiffs Jill Kelley and Scott Kelley reside in Tampa, Florida, which has an extensive military presence.[1] *See* Compl. ¶¶ 12, 19. Jill Kelley has volunteered to provide community outreach and support for the military community in Tampa, and over time, the Kelleys have become acquainted with a number of senior military leaders and their families, including General David H. Petraeus and General John R. Allen, Jr. *See id*. ¶¶ 20-22. The Kelleys interacted socially with those senior leaders on a regular basis, often sharing social news and personal reflections. *See id*. ¶ 22.

In May 2012, General John Allen received a strange email message that negatively referenced Jill Kelley. *See* Compl. ¶ 26. General Allen emailed Jill Kelley regarding the hostile message, which also contained specific non-public knowledge of an upcoming dinner with

[1] Consistent with the standard of review for facial jurisdictional challenges under Rule 12(b)(1) and for challenges to the sufficiency of a complaint's allegations under Rule 12(b)(6), this factual background recounts allegations from plaintiffs' complaint, which are assumed to be true for purposes of this motion.

several senior foreign intelligence, defense, and diplomatic officials. *See id*. ¶¶ 26-33. Because the email frightened the Kelleys personally and raised their concerns for the safety of senior military leaders, Jill Kelley contacted Fred Humphries, an FBI counterintelligence agent at nearby MacDill Air Force Base, with whom Jill Kelley had a social relationship. *See id*. ¶¶ 27, 28, 33.

In June, the Kelleys received similar emails at an email address they shared. *See* Compl. ¶¶ 29, 31. During that time, the Kelleys learned that General Allen and CIA Director General Petraeus were also receiving hostile emails. *See id*. ¶¶ 32. In an effort to learn the identity of the person sending the hostile emails, Jill Kelley met with FBI agents several times. *See id*. ¶¶ 34, 35, 41. The FBI initially requested limited access to the Kelleys' shared email account, and Jill Kelley consented to that request. *See id*. ¶¶ 35-36. The FBI later requested broader access to the Kelleys' shared email account, and Jill Kelley denied that request. *See id*. ¶ 37.

Around that time, the Kelleys became dissatisfied with the FBI and its investigation. The Kelleys believe that the FBI obtained additional email communications from their shared account and that Jill Kelley did not receive victim assistance or case updates that she was due. *See* Compl. ¶¶ 50, 53, 77-81. The Kelleys also suspect that the FBI investigation expanded and that the FBI was investigating whether Jill Kelley was having affairs with two different generals and an FBI agent. *See id*. ¶ 59. At one point, agent Humphries told the Kelleys that the FBI had asked and directed him to exclude an express denial of any sexual relationship with Jill Kelley in a sworn statement he provided, known as an FBI 302. *See id*. ¶¶ 61, 131, 151.

Despite their dissatisfaction with the FBI's investigation, the Kelleys do not claim to have received any similar hostile emails at any time after June 2012. *See id*. ¶ 39. Also, the Kelleys

later came to understand that the cyberstalker was Paula Broadwell, who in November 2012 was reported by the news media to have had an affair with General Petraeus. *See id*. ¶¶ 44, 67.

Shortly after the Petraeus-Broadwell affair was reported, Jill Kelley's name also appeared in the news as a recipient of harassing emails from Paula Broadwell. *See* Compl. ¶¶ 68-69. Several news media attributed knowledge of Jill Kelley's identity to unnamed governmental officials. *See id*. ¶¶ 68-71. A few days later in November 2012, the news media began reporting that there were large numbers of potentially inappropriate emails between General Allen and Jill Kelley. *See id*. ¶¶ 72-73. The news outlets again attributed those reports to unnamed governmental officials. *See id*. The Kelleys believe that governmental officials impermissibly leaked these pieces of information to the press. *See id*. ¶ 76.

In reaction to these events as alleged by the Kelleys in their complaint, the Kelleys have filed this lawsuit, in which they sue the FBI, the DoD, and the United States in Counts I through VII for alleged violations of the Privacy Act and the Stored Communications Act.

STATUTORY AND REGULATORY BACKGROUND

The Privacy Act of 1974

Congress enacted the Privacy Act in the wake of several notorious scandals in which the federal government officially collected, stored, and used the personal information of citizens. For example, the legislative history of the Privacy Act references the army's domestic spying program on political dissidents; the FBI's secret surveillance of the Urban League, the Southern Christian Leadership Conference, and persons who planned the first Earth Day; as well as the White House "plumbers," whose actions ultimately led to the Watergate scandal. *See* S. Rep. No. 93-1183 (Sept. 26, 1974), *reprinted in* LEGISLATIVE HISTORY OF THE PRIVACY ACT OF 1974 S. 3418 (PUBLIC LAW 93-579): SOURCE BOOK ON PRIVACY at 794-96 (hereafter "PRIVACY ACT SOURCE BOOK"); Statement of Senator Nelson (Nov. 21, 1974) *reprinted in* PRIVACY ACT

SOURCE BOOK at 794-96.[2] Adding to those congressional concerns was the realization that the increasing use of computers and sophisticated information technology had the potential to enable greater governmental intrusion into personal privacy. *See* Privacy Act of 1974, Pub. L. No. 93-579, § 2(A)(2) (Dec. 31, 1974). In response, Congress concluded that "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." *Id.* § 2(A)(5). In furtherance of that purpose, the Privacy Act protects personal privacy by "giv[ing] agencies detailed instructions for managing their records and provid[ing] for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements." *Doe v. Chao*, 540 U.S. 614, 618 (2004).

The Privacy Act achieves its goals through a series of highly technical provisions, which impose several requirements on federal agencies regarding the collection, use, maintenance, and dissemination of personal information. Those obligations include the duties to maintain only relevant and necessary records, *see* 5 U.S.C. § 552a(e)(1); to ensure that records used to make determinations about an individual or later disseminated satisfy certain informational quality standards, *see id.* § 552a(e)(5)-(6); to prohibit the collection of records describing how individuals exercise their First Amendment rights, *see id.* § 552a(e)(7); and to establish safeguards for the protection of personal information, *see id.* § 552a(e)(10). The Privacy Act also promotes transparency by providing a procedure through which individuals can gain access to agency records about them. *See id.* § 552a(d). Moreover, the Privacy Act prohibits the disclosure of personal information contained in agency records, subject to certain express exceptions. *See id.* § 552a(b). Critical to the present motion, the protections provided by the

[2] The PRIVACY ACT SOURCE BOOK is available online at http://www.loc.gov/rr/frd/Military_Law/LH_privacy_act-1974.html.

Privacy Act are also subject to two significant limitations: the system of records requirement and the ability of agencies to opt-out of certain Privacy Act requirements through exemption rules.

First, many of the Privacy Act's protections are location-based in that they apply only to records within a system of records. As statutorily defined, a "system of records" is a grouping of agency records from which information can be and is retrieved by an individual identifier:

> [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). Consistent with transparency concerns, an agency must provide notice in the Federal Register of each system of records it maintains along with certain details regarding the characteristics of the system of records, such as the categories of individuals on whom records are maintained in the system and the categories of records maintained in the system. *See id*. § 552a(e)(4). Several of the Privacy Act's provisions apply only to records maintained within a system of records. For example, the disclosure prohibitions, the limitation on maintaining relevant and necessary records, and the obligation to establish safeguards all apply only to records maintained within a system of records. *See Paige v. DEA*, 665 F.3d 1355, 1360 (D.C. Cir. 2012); *Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1123 (D.C. Cir. 2007); *Fisher v. Nat'l Inst. of Health*, 934 F. Supp. 464, 473 (D.D.C. 1996).

In addition to those location-based limits on its protections, the Privacy Act is confined by exemption rules. Specifically, the Privacy Act permits agencies to opt-out of several of its requirements though rulemaking. *See generally* 5 U.S.C. § 552a(j)-(k). For instance, in furtherance of law enforcement activities, agencies can exempt systems of records from several Privacy Act obligations. *See id.* § 552a(j)(2), (k)(2). And as relevant here, the FBI and the DoD

have exempted several of their law enforcement systems of records from the Privacy Act's requirements.[3]

As a means of redressing violations of its protections, the Privacy Act provides four civil remedies. The first three causes of action apply to the specific situations in which individuals seek the amendment of records, access to records, or damages resulting from adverse determinations based on records of low informational quality. *See* 5 U.S.C. § 552a(g)(1)(A)-(C). The fourth cause of action is a catchall, which permits individuals to sue for damages resulting from a violation of any other Privacy Act provision. *See id.* § 552(g)(1)(D). The catchall provision requires four elements in addition to those needed to demonstrate the underlying Privacy Act violation: (i) intentional and willful agency action; (ii) that proximately caused; (iii) an adverse effect on an individual; and (iv) that resulted in actual damages. *See* 5 U.S.C. § 552a(g)(a)(D), (g)(4); *see also Doe v. Chao*, 540 U.S. at 616 (requiring actual damages to recover); *Maydak v. United States*, 630 F.3d 166, 179-80 (D.C. Cir. 2010) (explaining the burden of proof on plaintiffs for the intentional and willful requirement); *Dickson v. Office of Personnel Mgmt.*, 828 F.2d 32, 37 (D.C. Cir. 1987) ("The adverse effect must be proximately caused by the Privacy Act violation."); *Albright v. United States*, 732 F.2d 181, 189 (D.C. Cir. 1984) ("The Act does not make the Government strictly liable for every affirmative or negligent action that might be said technically to violate the Privacy Act's provisions.").

The Stored Communications Act

The Stored Communications Act was enacted as Title II of the Electronic Communications Privacy Act ("ECPA"), Pub. L. No. 99-508, 100 Stat. 1848 (Oct. 21, 1986)

[3] The FBI's law enforcement exemptions are published as 28 C.F.R. § 16.96(a)(1), (c)(1), (e)(1), (g)(1), (j)(1), (l)(1), (n)(1), (p)(1), (r)(1), & (t)(1). The law enforcement exemptions for the DoD's Office of Inspector General are published at 32 C.F.R. § 312.12(d), (e), & (f).

(codified as amended at 18 U.S.C. §§ 2701-12). As its name suggests, the Act addresses several matters related to stored electronic communications. For instance, it sets forth criminal penalties for the unlawful access to stored communications. *See* 18 U.S.C. § 2701. It also prohibits entities that provide an electronic communication service to the public from disclosing the contents of a communication that they store. *See id.* § 2702. The Stored Communications Act also sets forth the warrant, subpoena, and notice procedures through which governmental entities can gain access to stored electronic communications or compel the creation of backup preservations of such communications. *See id.* §§ 2703-05.

As amended through the Patriot Act, the Stored Communications Act provides civil recoveries against the United States for violations of its terms. *See* Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001, Pub. L. No. 107-56, 115 Stat. 272 (Oct. 26, 2001). Specifically, a plaintiff injured by a violation of Stored Communications Act may sue the United States for the greater of $10,000 or actual damages, as well as reasonably incurred litigation costs. *See* 18 U.S.C. § 2712(a). Those remedies are exclusive of all others against the United States, and thus attorney's fees, injunctive relief, and punitive damages are not available against the United States for violations of the Stored Communications Act. *See id*. § 2712(d); *see also id*. § 2708. Procedurally, the Stored Communications Act adopts the presentment requirements of the Federal Tort Claims Act, which prohibit civil suits absent the exhaustion of administrative remedies. *See id*. § 2712(b)(1); *see also GAF Corp. v. United States*, 818 F.2d 901, 919 (D.C. Cir. 1987) (explaining the presentment obligations under the Federal Tort Claims Act). Federal law enforcement activities take precedence over the civil remedy provisions of the Stored Communication Act, and upon motion of the United States, any civil suit against the United States must be stayed if a court

determines that "civil discovery will adversely affect the ability of the Government to conduct a related investigation or the prosecution of a related criminal case." 18 U.S.C. § 2712(e)(1). However, if a Court determines that a federal agency violated any provision of the Act, then that agency is required to initiate a proceeding to determine whether or not disciplinary action is warranted against a federal officer or employee. *See id*. § 2712(c).

ARGUMENT

Plaintiffs' complaint should be dismissed in its entirety – partially on jurisdictional grounds under Rule 12(b)(1), and the remainder for a failure to state a claim for relief under Rule 12(b)(6).

In a motion to dismiss under Rule 12(b)(1), the moving party may raise facial or factual challenges to the court's subject matter jurisdiction. *See Erby v. United States*, 424 F. Supp. 2d 180, 182 (D.D.C. 2006). Under either challenge, it is presumed that a plaintiff's action lies outside of a court's limited jurisdiction. *See Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994). The jurisdictional challenges presented here are facial and require no additional factual development. The standard for a facial challenge mirrors that of Rule 12(b)(6) – in evaluating its subject matter jurisdiction, a court construes the allegations in a light most favorable to the non-moving party. *See Agrocomplect AD v. Republic of Iraq*, 524 F. Supp. 2d 16, 21 (D.D.C. 2007); *Flynn v. Ohio Bldg. Restoration, Inc.*, 260 F. Supp. 2d 156, 162 (D.D.C. 2003); *Loughlin v. United States*, 230 F. Supp. 2d 26, 35 (D.D.C. 2002).

While not jurisdictional, a motion to dismiss under Rule 12(b)(6) tests the legal sufficiency of a complaint's factual allegations under a plausibility standard. As articulated by the Supreme Court "[t]o survive a motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007));

see also Rollins v. Wackenhut Servs., Inc., 703 F.3d 122, 129 (D.C. Cir. 2012). To survive a Rule 12(b)(6) motion, a plaintiff must present "more than a sheer possibility that a defendant has acted unlawfully," *Iqbal*, 556 U.S. at 678, and the complaint will fail if it does not contain "more than labels and conclusions." *Twombly*, 550 U.S. at 555. Similarly, "a formulaic recitation of the elements of a cause of action will not do." *Id.*; *see also Kowal v. MCI Commc'ns Corp., Inc.*, 16 F.3d 1271, 1275 (D.C. Cir. 1994) (explaining that Rule 12(b)(6) pleading standard applies only to factual allegations and does not apply to "legal conclusions cast in the form of factual allegations"); *Nat'l ATM Council, Inc. v. Visa, Inc.*, 922 F. Supp. 2d 73, 79 (D.D.C. 2013).

I. THE COMPLAINT NAMES THE WRONG PARTIES AS DEFENDANTS IN ITS CLAIMS UNDER THE PRIVACY ACT AND THE STORED COMMUNICATIONS ACT

In Counts I through VII, plaintiffs mistakenly attempt to pursue Privacy Act and Stored Communications Act claims against three defendants. For the reasons stated below, however, the United States should be dismissed from the Privacy Act counts, and the FBI and the DoD should be dismissed from the Stored Communications Act counts.

A. The United States Should Be Dismissed from the Privacy Act Claims.

Plaintiffs' Privacy Act claims implicate only federal agencies. For instance, the civil remedy provisions in subsection (g) of the Privacy Act waive sovereign immunity only for claims against federal agencies. *See* 5 U.S.C. § 552a(g); *Sussman*, 494 F.3d at 1123. In addition, the disclosure prohibitions upon which plaintiffs base Count I govern federal agency action. *See* 5 U.S.C. § 552a(b). Similarly, the requirements for agency recordkeeping that form the basis of Counts II through VI apply only to federal agencies. *See id.* § 552a(e).

The term "agency" as used in the Privacy Act does not include the United States. In defining the term "agency," the Privacy Act incorporates the meaning supplied in the Freedom of

Information Act, which builds off of the definition of "agency" in the Administrative Procedure Act. *See* 5 U.S.C. § 552a(a)(1); *id.* §552(f)(1); *id.* § 551(a). Taken together, these provisions define the term "agency" for Privacy Act purposes as "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency." *Id.* § 552(f)(1); *see also id.* § 551(a) (excluding from the definition of "agency" entities such as Congress, the courts of the United States, and governments of the territories or possessions of the United States). That definition does not include the United States. Nor should that formulation be read to encompass the United States because waivers of sovereign immunity must be "unequivocally expressed in statutory text," and any ambiguity is narrowly construed in favor of the sovereign. *Lane v. Peña*, 518 U.S. 187, 192 (1996); *see also Sussman*, 494 F.3d at 1123 (construing the Privacy Act's waiver of sovereign immunity narrowly); *United W. Bank v. Office of Thrift Supervision*, 793 F. Supp. 2d 357, 361 (D.D.C. 2011). The United States, therefore, does not constitute an "agency" under the Privacy Act. *See Mumme v. U.S. Dep't of Labor*, 150 F. Supp. 2d 162, 169 (D. Me. 2001) (explaining that "a claimant bringing a Privacy Act claim must bring suit against a particular agency, not the entire United States," and that "the United States cannot be a defendant pursuant to . . . Privacy Act claims"); *Sheppard v. Revell*, 2010 WL 3672261, at *2 (E.D.N.C. 2010) ("The United States is not a proper party in an action brought pursuant to the Privacy Act."). Because the waiver of sovereign immunity is of jurisdictional significance, claims outside of such a waiver should be dismissed. *See United States v. Mitchell*, 463 U.S. 206, 212 (1983) ("It is axiomatic that the United States may not be sued without its consent and that the existence of consent is a prerequisite for jurisdiction."); *Scurlock v. Lappin*, 870 F. Supp. 2d 116, 119 (D.D.C. 2012)

("The Court lacks subject matter jurisdiction over claims against the United States unless it has waived sovereign immunity."). For that reason, the United States should be dismissed from Counts I through VI for a lack of subject matter jurisdiction.

B. The FBI and the DoD Should Be Dismissed from the Stored Communications Act Claim.

Unlike the Privacy Act, the waiver of sovereign immunity in the Stored Communication Act does not permit actions against federal agencies. Instead, the Stored Communications Act permits suits against the United States, but it requires the relevant federal agency to reimburse the treasury for the amount of the award. *See* 18 U.S.C. § 2712(a) (permitting a civil action "in United States District Court *against the United States* to recover money damages" (emphasis added)); *id.* § 2712(b)(5) (requiring a federal agency or department to reimburse the federal treasury of the amount of the award). Those terms act as waivers of sovereign immunity, and as such they define the extent to which the United States and its agencies can be sued for damages. *See United States v. Sherwood*, 312 U.S. 584, 586 (1941); *Bartlett v. Bowen*, 816 F.2d 695, 718-19 (D.C. Cir. 1987); *Williams v. Connor*, 522 F. Supp. 2d 92, 98 (D.D.C. 2007). Because waivers of sovereign immunity must be strictly construed, the Stored Communications Act permits suit only against the United States, and not against federal agencies or officers. *See Lane v. Peña*, 518 U.S. at 192; *Sussman*, 494 F.3d at 1123; *United W. Bank*, 793 F. Supp. 2d at 361. Consequently, the FBI and DoD should be dismissed from Count VII for a lack of subject matter jurisdiction.

II. PLAINTIFF SCOTT KELLEY FAILS TO STATE A CLAIM FOR RELIEF BECAUSE HE DOES NOT ALLEGE THAT DEFENDANTS MAINTAINED RECORDS ABOUT HIM.

All of plaintiff Scott Kelly's claims under the Privacy Act and the Stored Communication Act should be dismissed. The conceptual foundation of both of these Acts is the protection of agency "records." Consistent with the centrality of that term, each of plaintiffs' Privacy Act

counts is premised on agency action with respect to the maintenance or the protection of agency "records." Likewise, the Stored Communications Act incorporates the Privacy Act definition of "record" into its disclosure prohibition. *See* 18 U.S.C. § 2707(g). Despite the ubiquity of the concept of agency "records" in the Acts, the complaint fails to allege facts that support the inference that defendants maintained any "record" about Scott Kelley. Without such an allegation, Scott Kelley fails to state a claim for relief for Counts I through VII.

As defined in the Privacy Act, the term "record" has a specialized meaning:

> [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). Under that formulation, for information maintained by an agency to constitute a "record," two elements must be satisfied. There must be (i) information about an individual and (ii) it must contain the individual's name or the identifying number, symbol, or other identifying particular assigned to the individual. *See Tobey v. NLRB*, 40 F.3d 469, 471 (D.C. Cir. 1994); *Houghton v. U.S. Dep't of State*, 875 F. Supp. 2d 22, 34-35 (D.D.C. 2012); *Fisher*, 934 F. Supp. at 468. The D.C. Circuit has emphasized that information with only a personal identifier does not constitute a record; the information must also be about the individual: "for an assemblage of data to qualify as [an individual's] records, it must not only contain his name or other identifying particulars but also be 'about' him." *Sussman*, 494 F.3d at 1121; *see also* Office of Management and Budget Privacy Act Implementation: Guidelines and Responsibilities 40 Fed. Reg. 28,948, 28,951 (July 9, 1975) (explaining that the term record "[m]eans any item of information about an individual that includes an individual identifier"). To be "about" an individual, the information "must actually describe him in some way." *Sussman*,

494 F.3d at 1121; *McCready v. Nicholson*, 465 F.3d 1, 9 (D.C. Cir. 2006); *Tobey*, 40 F.3d at 472. It is not sufficient that the information "simply 'applies to him'" in some way. *Tobey*, 40 F.3d at 472. Nor does information that merely contains an individual's name and address constitute information "about" that individual. *See Fisher*, 934 F. Supp. at 471. The allegations in the complaint fail to satisfy the two elements for an agency "record" with respect to Scott Kelley.

First, the complaint does not identify any content maintained by either the FBI or the DoD that is "about" Scott Kelley. The complaint alleges that defendants collected emails sent from an email account that Scott and Jill Kelley shared. *See, e.g.*, Compl. ¶¶ 6, 46, 53. But without more, those statements do not indicate that the email communications were "about" Scott Kelley. If an individual's name and address do not suffice to make a document "about" that individual, *see Fisher*, 934 F. Supp. at 471, then a mere mention of an email address certainly cannot have that effect. Put simply, nothing in the complaint indicates that the email communications actually describe Scott Kelley in some way and therefore come within the meaning of a "record" under the Privacy Act. *See Sussman*, 494 F.3d at 1121. Without such an allegation, plaintiffs cannot satisfy the required element that a record be "about an individual."

Plaintiffs also fail to satisfy the second "record" element. The documents that defendants allegedly maintained related to Scott Kelley were email communications from an email address that he shares with Jill Kelley. But those emails are not alleged to have any identifying particulars assigned to Scott Kelley. Notably, the complaint does not aver that Scott Kelley was mentioned by name, identifying number, or symbol in any email communications allegedly maintained by defendants. The only possible identifier for Scott Kelley as alleged in the complaint is the email addresses that he shares with Jill Kelley. But an email address is not a name, identifying number, or symbol. Nor is a shared email address some "other identifying

particular assigned to an individual," since a common email account is by its very nature shared rather than individually assigned.

In sum, Scott Kelley fails to state a claim under Counts I through VII because the complaint does not allege that defendants maintained any documents "about" Scott Kelley, and it does not allege that the any documents maintained by defendants contain any identifying particular assigned to Scott Kelley.

III. PLAINTIFFS CANNOT PROCEED WITH CLAIMS UNDER THE STORED COMMUNICATIONS ACT BECAUSE THEY DO NOT ALLEGE A PRESENTMENT OF THOSE CLAIMS.

The provisions in the Stored Communication Act that permit civil suits against the United States incorporate certain of the procedural requirements of the Federal Tort Claims Act (the "FTCA"). Relevant here is that the Stored Communications Act contains a presentment requirement, which requires a potential plaintiff to present claims to appropriate federal agency for consideration:

> Any action against the United States under this section may be commenced only after a claim is presented to the appropriate department or agency under the procedures of the Federal Tort Claims Act, as set forth in title 28, United States Code.

18 U.S.C. § 2712(b)(1). From that text, the Stored Communication Act imposes the same presentment requirements as the FTCA, which requires a plaintiff to file with the appropriate Federal agency "(1) a written statement sufficiently describing the injury to enable the agency to begin its own investigation, and (2) a sum-certain damages claim." *GAF Corp.*, 818 F.2d at 919; *see also* 28 U.S.C. § 2675(a). After making such a presentment, a potential plaintiff cannot initiate a civil action until the agency has denied the claims or the expiration of six months since the date of presentment. *See* 28 U.S.C. § 2675(a). The FTCA's presentment requirement is jurisdictional, and a complaint that does not allege a presentment of claims should be dismissed for lack of subject matter jurisdiction. *See McNeil v. United States*, 508 U.S. 106, 113 (1993)

("The FTCA bars claimants from bringing suit in federal court until they have exhausted their administrative remedies."); *Upshaw v. United States*, 669 F. Supp. 2d 32, 45 (D.D.C. 2009) (dismissing a case for lack of subject matter jurisdiction where plaintiff did not plead presentment claims to the appropriate federal agency); *Bell v. Library of Congress*, 539 F. Supp. 2d 411, 413 (D.D.C. 2008) (same).

Here, plaintiffs fail to allege that they presented their Stored Communications Act claims to either the FBI or to the DoD. The complaint does not allege that plaintiffs filed a written statement sufficiently describing the injury and a sum-certain damages claim. Without having done so, plaintiffs are unable to avail themselves of this Court's jurisdiction under the Stored Communications Act, and Count VII must be dismissed.[4]

IV. PLAINTIFFS DO NOT ALLEGE FACTS NECESSARY FOR THEIR PRIVACY ACT CLAIMS.

A. Plaintiffs' Disclosure Claim under the Privacy Act Fails Because the Complaint Does Not Satisfy the Retrieval Rule.

Plaintiffs allege in Count I that the FBI and the DoD impermissibly shared information with members of the press and media outlets. *See* Compl. ¶¶ 105-17. Based on those allegations, plaintiffs pursue an unauthorized disclosure claim under subsection (b) of the Privacy Act, through the catchall civil remedy provision. *See* 5 U.S.C. § 552a(b), (g)(1)(D), (g)(4). Plaintiffs' claim should be dismissed because the complaint lacks allegations that defendants violated the "retrieval rule."

The retrieval rule is a necessary element of unauthorized disclosure claims under the Privacy Act. Specifically, for a disclosure to be unlawful, the information disclosed must first be retrieved from a record that is retrievable by a plaintiffs' name and that is contained within an

[4] Because the United States cannot be sued under the Privacy Act, and because plaintiffs have not exhausted their Stored Communications Act claims, the United States should be dismissed as a party from this lawsuit.

agency's system of records, and not from some independent source. *See Paige*, 665 F.3d at 1360 (rejecting a disclosure claim where the information released was not retrieved from a system of records); *Sussman*, 494 F.3d at 1123 (explaining that to be unlawful, the disclosures had to be materials from records about a plaintiff that were retrieved by plaintiff's name); *Fisher*, 934 F. Supp. at 473 ("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." (quotation omitted)). This is so because the Privacy Act's prohibition on unauthorized disclosures applies only to records maintained within an agency's system of records. *See* 5 U.S.C § 552a(a)(5); *see McCready*, 465 F.3d at 9 ("The key limitation in the Act's definition of 'system of records' is its use of 'retrieved.'"). Beyond its textual grounding, the retrieval rule is justified for two additional reasons: (1) the imposition of liability on federal agencies for the disclosure of independently acquired information would impose an intolerable burden, and (2) abandoning the retrieval rule would exceed the relevant purpose of the Privacy Act, which was to preclude information in a system of records from serving as the *source* of personal information about a person. *See Doe v. U.S. Dep't of Treasury*, 706 F. Supp. 2d 1, 7 (D.D.C. 2009). Accordingly, through the retrieval rule, agencies are excluded from liability for the release of information that has not been actually retrieved from records within a Privacy Act system of records. *See Cloonan v. Holder*, 768 F. Supp. 2d 154, 164 (D.D.C. 2011) ("[A]n agency official who discloses information that he or she acquired from non-record sources – such as observation, office emails, discussions with co-workers and the 'rumor mill' – does not violate the Privacy Act in doing so, even if the information disclosed is also contained in agency records."). Here, plaintiffs' allegations do not satisfy the retrieval rule.

Plaintiffs do not aver that any disclosed information about them was retrieved from a record within a system of records. Plaintiffs do allege in a general fashion that information regarding them was contained in a system of records:

> Information regarding the Kelleys and their report to the FBI of threatening and harassing cyberstalking is maintained within one or more Privacy Act systems of records retrievable by use of the Kelleys' name or by some identifying number, symbol or other identifying particular assigned to Plaintiffs.

Compl. ¶¶ 106, 119, 129, 148; *see also* ¶¶ 139, 159 (making the same allegation but "upon information and belief"). But because that allegation does not allege a retrieval of a record about plaintiffs within a system of records, it does not satisfy the retrieval rule. Plaintiffs later allege, upon information and belief, that the FBI and the DoD shared records regarding the Kelleys with the media:

> [O]n one or more occasions since the Kelleys first reported the threatening and criminal actions of the cyber stalker, the FBI shared records on the Kelleys with the DOD, and both shared those records with the media.

Compl. ¶ 109. Even if taken as true, that alleged record sharing does not satisfy the retrieval rule for the same reason – it contains no suggestion that any of the shared records were retrieved from a protected system of records, and not some other location. *Cf., e.g.*, Compl. ¶ 178 (alleging that some information gathered from the FBI's alleged searching of their email was "not then collected and maintained as a record in a system of governmental records"). The complaint does allege, again upon information and belief, that information retrieved from a protected system of records was disseminated:

> [T]he FBI, DOD, and the United States, through numerous employees, unlawfully and without regard to the foreseeable and certain consequences of association with the unfolding national scandal of Petraeus' extramarital affair, disseminated information, including that which was inaccurate, derogatory, and irrelevant, from within a protected system of records, to media members and other third parties who were not authorized to receive such information.

Compl. ¶ 111. But a bare allegation of a retrieval *untethered to records about plaintiffs* cannot sustain an unauthorized disclosure claim. This is so for two reasons. First, to satisfy the retrieval rule, a plaintiff must allege that the "improperly disclosed materials [were] located in records retrievable by [his or her] name as opposed to someone else's name," and paragraph 111 does not allege that. *Sussman*, 494 F.3d at 1123. Second, the Privacy Act does not create third-party privacy rights, and thus an allegedly illegal disclosure of information about other individuals could not form the basis of plaintiffs' disclosure claim. *See id*.

Put simply, without stating that the allegedly disclosed information was actually retrieved from records that were retrievable by plaintiffs' names from a system of records, the unauthorized disclosure count fails. *See York v. McHugh*, 850 F. Supp. 2d 305, 313 (D.D.C. 2012) ("Although it may appear counterintuitive, the Privacy Act does not protect against disclosure of all records containing personal or private information."). Because plaintiffs' allegations do not satisfy the retrieval rule, Count I should be dismissed for failure to state a claim for relief.

B. Plaintiffs Fail to State a Claim for the Unlawful Maintenance of Records.

In Count II, plaintiffs claim that the FBI and the DoD maintained records that were irrelevant and unnecessary for the accomplishment of a legitimate purpose of either agency. *See* Compl. ¶¶ 118-27. Based on those allegations, plaintiffs seek damages for a violation of subsection (e)(1) of the Privacy Act through the catch-all civil remedy provisions in subsection (g). *See* 5 U.S.C. § 552a(e)(1), (g)(1)(D), (g)(4). Plaintiffs fail to state a claim for relief, however. The FBI and the DoD have exempted several of their record systems from the requirements of subsection (e)(1), but plaintiffs do not aver that the alleged (e)(1) violation (the

maintenance of irrelevant or unnecessary records in a system of records) occurred in a system of records that was subject to the requirements of subsection (e)(1).

Subsection (e)(1) of the Privacy Act restricts the scope of the records that federal agencies maintain. Specifically, it limits a federal agency to maintaining only records relevant and necessary to a legitimate purpose of that agency:

> Each agency that maintains a system of records shall --
> maintain in its records only such information about an individual as is relevant and necessary to accomplish a purpose of the agency required to be accomplished by statute or by executive order of the President

5 U.S.C. § 552a(e)(1); *see also Reuber v. United States*, 829 F.2d 133, 138 (D.C. Cir. 1987). This requirement applies only to records maintained within an agency's system of records. *See Maydak v. United States*, 363 F.3d 512, 518 (D.C. Cir. 2004). As explained by the Privacy Act Guidelines, subsection (e)(1) "does not require that each agency conduct a detailed review of the contents of each record in its possession." 40 Fed. Reg. at 28,961. Instead, the Privacy Act Guidelines direct agencies to "consider the relevance of, and necessity for, the general categories of information maintained. . . ." *Id.*

These obligations imposed by the Privacy Act are "not absolute," and "[t]he Act permits agencies to exempt certain systems of records from some of its requirements." *Doe v. FBI*, 936 F.2d 1346, 1351 (D.C. Cir. 1991). Agencies, or components of agencies, that are engaged in criminal law enforcement as their principal function may promulgate rules to exempt systems of records related to criminal investigations from the requirements of subsection (e)(1). *See* 5 U.S.C. § 552a(j)(2). On the basis of its law enforcement functions, the FBI has exercised that option to exempt several of its systems of records from subsection (e)(1). For example, the FBI has exempted its Central Records System, which contains investigative, personnel, applicant,

administrative, and general files. *See* 28 C.F.R. § 16.96(a)(1); *see also id.* § 16.96(c)(1), (e)(1), (g)(1), (j)(1), (*l*)(1), (n)(1), (p)(1), (r)(1), (t)(1). The FBI made that exemption for four reasons:

> (i) It is not possible in all instances to determine relevancy or necessity of specific information in the early stages of a criminal or other investigation.
>
> (ii) Relevance and necessity are questions of judgment and timing; what appears relevant and necessary when collected ultimately may be deemed unnecessary. It is only after the information is assessed that its relevancy and necessity in a specific investigative activity can be established.
>
> (iii) In any investigation the FBI might obtain information concerning violations of law not under its jurisdiction, but in the interest of effective law enforcement, dissemination will be made to the agency charged with enforcing such law.
>
> (iv) In interviewing individuals or obtaining other forms of evidence during an investigation, information could be obtained, the nature of which would leave in doubt its relevancy and necessity. Such information, however, could be relevant to another investigation or to an investigative activity under the jurisdiction of another agency.

See 28 C.F.R. § 16.96(a)(3).

The Privacy Act also permits all agencies to exempt systems of records from the maintenance of subsection (e)(1) for other law enforcement purposes as well. *See* 5 U.S.C. § 552a(k)(2). Consistent with that authority, the DoD has exempted some of its systems of records from subsection (e)(1), including, for instance, an investigatory file system of the DoD Inspector General's Office, known as the Senior Official and Reprisal Investigation Case System, also referred to as CIG-15. *See* 32 C.F.R. § 312.12(f); *see also id.* § 312.12(d), (e). The DoD justified that exemption on several grounds:

> because the nature of the criminal and/or civil investigative function creates unique problems in prescribing a specific parameter in a particular case with respect to what information is relevant or necessary. Also, due to OIG's close liaison and working relationships with other Federal, state, local and foreign country law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

See 32 C.F.R. § 312.12(f)(6).

Due to those exempted systems of records, plaintiffs' allegations do not state a claim for relief. No claim exists under subsection (e)(1) for records maintained in systems of records that are exempted from subsection (e)(1). *See Sieverding v. U.S. Dep't of Justice*, 693 F. Supp. 2d 93, 102-03 (D.D.C. 2010); *cf. Arnold v. U.S. Secret Serv.*, 524 F. Supp. 2d 65, 67 (D.D.C. 2007) (dismissing a claim under subsection (e)(5) related to an exempt system of records). And here, plaintiffs have not alleged that the FBI or the DoD maintained records in a system of records subject to the requirements of subsection (e)(1). Without such an allegation, plaintiffs fail to state a claim for relief under subsection (e)(1).

C. Plaintiffs' Allegations Do Not Constitute a Claim of an Adverse Determination Based on Inaccurate or Incomplete Records.

In Count III, plaintiffs assert that the FBI and the DoD violated subsection (e)(5) of the Privacy Act by making determinations based on records that were inaccurate and incomplete. *See* Compl. ¶¶ 128-37. The basis for this count is the notion that the FBI dissuaded agent Fred Humphries "from providing a complete and accurate record on Mrs. Kelley." *Id.* ¶ 131. As alleged by plaintiffs, agent Humphries provided a sworn statement, known as an FBI 302, in connection with the cyberstalking investigation, and as part of that statement he wanted to deny expressly that he had sexual relations with Jill Kelley. *See id.* ¶ 61. According to plaintiffs, the FBI directed or asked agent Humphries not to include such a denial in his sworn statement. *See id.* (alleging that "the FBI directed Agent Humphries to remove a statement in his sworn 302 declaration addressing, and flatly denying, the accusation that he had any sort of sexual contact or relationship with Mrs. Kelley"); *id.* ¶ 131 (alleging that the FBI "asked that the agent eliminate information in the record"). Plaintiffs further allege that, because the Humphries 302 lacked an explicit disavowal of a sexual relationship with Jill Kelley, it was inaccurate and

incomplete. *See id.* ¶¶ 131, 133. Plaintiffs claim that those alleged defects caused the FBI to deny victim assistance services to plaintiffs and to treat them as the subjects of the investigation and not as crime victims. *See id*. ¶ 132. As explained below, plaintiffs' allegations do not state a plausible claim for relief under subsection (e)(5), and Count III should be dismissed.

The Privacy Act provides a remedy for situations in which agency determinations are unfairly made due to inaccurate, irrelevant, untimely, or incomplete records. Through subsection (e)(5), the Privacy Act imposes an obligation on agencies to ensure the integrity of records used to make determinations by requiring that federal agencies

> maintain all records which are used by the agency in making any determination about an 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). To pursue a damages claim under subsection (e)(5), a plaintiff must proceed under the remedy provisions in subsection (g)(1)(C). *See Deters v. U.S. Parole Comm'n*, 85 F.3d 655, 660-61 & n.5 (D.C. Cir. 1996) ("[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)."); *Thompson v. Dep't of State*, 400 F. Supp. 2d 1, 8 (D.D.C. 2005) (explaining that subsection (g)(1)(C) "provides the exclusive damages remedy for violations of subsection (e)(5)"). Subsection (g)(1)(C) permits a civil suit when an agency does not

> 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 . . . .

5 U.S.C. § 552a(g)(1)(C). The provisions in subsections (e)(5) and (g)(1)(C) extend to agency records that are not maintained in a system of records. *See Gerlich v. U.S. Dep't of Justice*, 711 F.3d 161, 169 (D.C. Cir. 2013) ("The obligations the Privacy Act established in subsection (e)(5) therefore apply even when the agency does not maintain the records at issue in

its system of records."); *McCready*, 465 F.3d at 12 (explaining that "subsection (g)(1)(C) applies to any record, and not any record within a system of records" (quotations and emphasis omitted)). To recover damages under subsection (g)(1)(C), a plaintiff must also allege that the adverse agency determination was committed with an intentional or willful mental state, and that it was the proximate cause of actual damages. *See* 5 U.S.C. § 552a(g)(4). The protections and civil remedy provided by subsections (e)(5) and (g)(1)(C) are not absolute, however, and they are subject to exceptions. For instance, subsection (j)(2) of the Privacy Act permits agencies (or components of agencies) with law enforcement responsibilities as their principal function to exempt law-enforcement systems of records that they maintain from the scope of subsection (e)(5). *See* 5 U.S.C. § 552a(j)(2).

Thus, altogether, to state a civil claim for relief under subsection (e)(5), a complaint must contain six allegations: (i) an intentional and willful; (ii) adverse determination; (iii) proximately caused by; (iv) a failure by an agency to maintain accurate, relevant, timely, and complete records; (v) in a non-exempt location; (vi) which resulted in actual damages. *See* 5 U.S.C. § 552a(g)(1)(c), (g)(4); *Chambers v. U.S. Dep't of Interior*, 568 F.3d 998, 1007 (D.C. Cir. 2009); *Deters*, 85 F.3d at 657; *see also Doe v. Chao*, 540 U.S. at 616 (requiring actual damages to recover); *Allmon v. Fed. Bureau of Prisons*, 605 F. Supp. 2d 1, 6 (D.D.C. 2009) (dismissing a complaint where there was no allegation that the records at issue were located in a non-exempt system of records); *Conklin v. U.S. Bureau of Prisons*, 514 F. Supp. 2d 1, 6 (D.D.C. 2007) (same). Plaintiffs do not allege several of these elements, and therefore Count III should be dismissed.

At the outset, Plaintiffs fail to allege facts sufficient to satisfy the adverse determination element with respect to the DoD. Plaintiffs identify two potentially adverse determinations: the

FBI's denial of victim assistance services and relatedly, the FBI's treatment of plaintiffs as the subjects of an investigation and not as victims. *See* Compl. ¶ 132. Notably absent from these allegations is any mention of the DoD, much less a statement that the DoD made an adverse determination with respect to either plaintiff. For that reason, plaintiffs fail to state a claim under subsections (e)(5) and (g)(1)(C) against the DoD.

In addition, a claim that the FBI did not provide victim assistance services cannot serve as a legally cognizable basis for a Privacy Act claim under subsection (e)(5). As noted above, subsection (g)(1)(C) of the Privacy Act permits a damages remedy under subsection (e)(5) when an agency fails to maintain a record about an individual that is accurate and relevant in order "to assure fairness in any determination relating to . . . rights . . . or benefits to the individual that may be made on the basis of such record . . ." 5 U.S.C. § 552a(g)(1)(C). Congress, however, has made clear under the Crime Victims' Rights Act, *see* Pub. L. No. 108-405, tit. I (Oct. 30, 2004) (codified at 18 U.S.C. § 3771), that a failure to provide victim assistance cannot form the basis of a damages claim:

> Nothing in this chapter shall be construed to authorize a cause of action for damages or to create, to enlarge, or to imply any duty or obligation to any victim or other person for the breach of which the United States or any of its officers or employees could be held liable in damages.

18 U.S.C. § 3771(d)(6). Consequently, plaintiffs fail to state a claim under subsection (e)(5) due to the FBI's alleged non-provision of victim assistance.

Plaintiffs' additional allegation that the FBI converted their status from victims to subjects is not a cognizable adverse determination under the Privacy Act. Deep-rooted policy concerns caution against courts probing the details of the criminal investigatory process:

> The powers of criminal investigation are committed to the Executive branch. The balance between the Executive and Judicial branches would be profoundly upset if the Judiciary assumed superintendence over the law enforcement activities of

> the Executive branch upon nothing more than a vague fear or suspicion that its officers will be unfaithful to their oaths or unequal to their responsibility.

Reporters Comm. for Freedom of Press v. Am. Tel. & Tel. Co., 593 F.2d 1030, 1065 (D.C. Cir. 1978). Moreover, multiple circuits have acknowledged that "[c]ourts should go very slowly before staking out rules that will deter government agents from the proper performance of their investigative duties." *United States v. Connell*, 960 F.2d 191, 196 (1st Cir. 1992); *see also United States v. Barth*, 990 F.2d 422, 425 (8th Cir. 1993) (same). Here, however, to evaluate when, why, and on the basis of what records the FBI allegedly began treating plaintiffs as suspects would do exactly that, by forcing the parties and the Court to reconstruct the smallest details of a sensitive law enforcement investigation. Accordingly, even if plaintiffs' allegation is assumed to be true, *i.e.*, that they were somehow converted to the subjects of a criminal investigation, there is no basis in precedent for concluding that such an allegation, without more, rises to the level of an adverse determination under the Privacy Act.

In addition, the complaint does not plausibly allege that the Humphries 302 is inaccurate or incomplete. Such an allegation is fundamental to a claim under subsections (e)(5) and (g)(1)(C). *See Chambers*, 568 F.3d at 1007 ("Central to a cause of action under subsection (g)(1)(C) is the existence of an adverse agency determination resulting from inaccurate agency records."); *Toolasprashad v. Bureau of Prisons*, 286 F.3d 576, 583 (D.C. Cir. 2002); *Doe v. U.S. Dep't of Justice*, 660 F. Supp. 2d 31, 43 (D.D.C. 2009) (dismissing a claim under subsection (e)(5) where the complaint did not allege any inaccuracy in agency information); *Djenasevic v. Exec. U.S. Attorney's Office*, 579 F. Supp. 2d 129 (D.D.C. 2008) (rejecting claim under subsection (e)(5) where there was no inaccurate, irrelevant, untimely, or incomplete record); *see also Thompson*, 400 F. Supp. 2d. at 19 (explaining that to make out a damages claim under subsection (e)(5), "the alleged adverse determination must result from the inaccuracy of records,

not the mere existence of records"). Although plaintiffs allege that the Humphries 302 lacked an express disavowal of a sexual relationship between agent Humphries and Jill Kelley, that omission does not render the 302 inaccurate or incomplete. Rather, as the Privacy Act Guidelines advise, "[a]gencies must limit their records to those elements of information which clearly bear on the determination(s) for which the records are intended to be used, and assure that all elements necessary to the determinations are present before the determination is made." 40 Fed. Reg. at 28,965. Moreover, the alleged determinations here (to deny victim services and to make plaintiffs the subjects of the investigation) did not depend in any way on the alleged non-sexual nature of Jill Kelley's relationship with agent Humphries. Therefore, even assuming the truth of plaintiffs' allegations, it is appropriate that the Humphries 302 made no mention of those immaterial matters, and the exclusion of such irrelevant statements does render the Humphries 302 inaccurate or incomplete.

Plaintiffs' claim under subsection (e)(5) also fails because the complaint does not allege that defendants relied on information in systems of records covered by subsection (e)(5) to make any determination regarding plaintiffs. With respect to the DoD, plaintiffs do not allege that the DoD ever maintained a copy of the Humphries 302, much less that DoD maintained that statement in a covered system of records. Plaintiffs' claims against the FBI fail as well because the FBI has exempted several of its systems of records from the requirements of subsection (e)(5), under the authority provided by subsection (j)(2). *See* 5 U.S.C. § 552a(j)(2). The FBI has exempted its Central Records System and several other systems of records from the requirements of subsection (e)(5). *See* 28 C.F.R. § 16.96(a)(1); *see also id.* § 16.96(c)(1), (e)(1), (g)(1), (j)(1), (*l*)(1), (n)(1), (p)(1), (r)(1), (t)(1). The FBI explains that the Central Records System is exempted from subsection (e)(5) because law enforcement investigations are dynamic,

and strict adherence to the requirements of subsection (e)(5) would impede the investigatory process:

> [I]n the collection of information for law enforcement purposes it is impossible to determine in advance what information is accurate, relevant, timely and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light. The restrictions imposed by subsection (e)(5) would limit the ability of trained investigators and intelligence analysts to exercise their judgment in reporting on investigations and impede the development of criminal intelligence necessary for effective law enforcement. In addition, because many of these records come from other federal, state, local, joint, foreign, tribal, and international agencies, it is administratively impossible to ensure compliance with this provision.

28 C.F.R. § 16.96(b)(6). Due to the presence of these exempt systems of records, to state a claim against the FBI, plaintiffs must allege that the record at issue – the Humphries 302 – was maintained by the FBI in a non-exempt location. *See Allmon*, 605 F. Supp. 2d at 6 (dismissing a complaint where there was no allegation that the records at issue were located in a non-exempt system of records); *Arnold*, 524 F. Supp. 2d at 67 (same) *Conklin*, 514 F. Supp. 2d at 6 (same). Plaintiffs make no such allegation, and therefore they do not state a claim against the FBI under subsection (e)(5).

D. Plaintiffs Do Not State a Claim for Failing to Assure Accuracy and Completeness of Records Prior to Their Alleged Dissemination.

In Count V, plaintiffs claim that defendants violated subsection (e)(6) of the Privacy Act by failing to assure the accuracy and completeness of records before disseminating them. *See* Compl. ¶¶ 147-57. As with Count III, plaintiffs' subsection (e)(6) claim rests on the alleged contents of a sworn declaration, an FBI 302, provided by FBI agent Fred Humphries in connection with the FBI's investigation of Jill Kelley's cyberstalking complaint. *See id*. ¶¶ 61, 151. Plaintiffs assert that the Humphries FBI 302 is inaccurate and incomplete because it did not state affirmatively that agent Humphries had no sexual relationship with Jill Kelley. *See id.* Even if taken as true, those allegations do not state a claim under subsection (e)(6).

Subsection (e)(6) requires that agencies take reasonable efforts to assure the accuracy, completeness, timeliness, and relevance of agency records prior to their dissemination:

> Each agency that maintains a system of records shall . . . 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.

5 U.S.C. § 552a(e)(6). Subsection (e)(6) applies only to records contained within a system of records. *See Krieger v. U.S. Dep't of Justice*, 529 F. Supp. 2d 29, 50, 55 (D.D.C. 2008); *see also McCready v. Nicholson*, 465 F.3d at 12, 12 n.6. Based on those principles, a violation of subsection (e)(6) consists of three elements: (i) dissemination of a record about the plaintiff to a person other than an agency or a FOIA requestor; (ii) retrieved from a system of records; (iii) without having undertaken reasonable efforts to assure that the record is accurate, complete, timely, and relevant for agency purposes. *See* 5 U.S.C. § 552a(e)(6); *McCready*, 465 F.3d at 8 n.4 (clarifying that subsection (e)(6) does not apply to disseminations made pursuant to the Freedom of Information Act); *Thompson*, 400 F. Supp. 2d. at 21 (explaining that subsection (e)(6) "does not apply when information is disclosed within the agency or to another agency"); *see generally* 40 Fed. Reg. at 28,965 (acknowledging exceptions for dissemination to another agency or to a FOIA requestor). Plaintiffs fail to allege those elements.

First, plaintiffs fail to allege any dissemination of the Humphries 302. Plaintiffs *do* allege that several pieces of information regarding Jill Kelley were allegedly communicated to the press, *see, e.g.*, Compl. ¶¶ 68-73, but they do not allege that the Humphries 302 or its contents were provided to anyone outside of the FBI. Without such an allegation, plaintiffs fail to allege the dissemination element required for a claim under subsection (e)(6) against the FBI. *See Thompson*, 400 F. Supp. 2d. at 22 (rejecting a subsection (e)(6) claim where there was no dissemination outside of a federal agency). That void in plaintiffs' allegation extends to the

DoD. Plaintiffs do not allege that the DoD received the Humphries 302, nor do they allege that the DoD disseminated any record in violation of subsection (e)(6).

Relatedly, plaintiffs fail to satisfy the retrieval rule. They do not allege that the Humphries 302 was retrievable by either plaintiff's name, much less that it was actually retrieved from a system of records.

Finally, and as explained above, plaintiffs' allegations are insufficient to establish that the Humphries sworn statement is inaccurate or incomplete. The lack of express denial of sexual relations between Humphries and Jill Kelley does not make the FBI 302, provided in the context of a cyberstalking investigation, inaccurate or incomplete. To the contrary, such a statement would be irrelevant to the cyberstalking investigation, and would not belong in Humphries's sworn statement. Accordingly, the complaint does not sufficiently allege that the FBI maintained an inaccurate or incomplete record, much less that the FBI failed to take reasonable efforts to assure the accuracy and completeness of that record.

E. Plaintiffs Fail to State a Claim for Maintaining Records that Describe the Exercise of First Amendment Rights Because Any Such Records Would Be Covered by the Law Enforcement Exception.

Count IV alleges that the FBI and the DoD illegally maintained records describing how plaintiffs exercised their First Amendment rights. Based on those allegations, plaintiffs sue for a violation of subsection (e)(7) of the Privacy Act, proceeding under the catch-all civil remedy provisions in subsection (g)(1)(D). *See* 5 U.S.C. § 552a(g)(1)(D); *see also Doe v. FBI*, 936 F.2d at 1360 (explaining that a claim under subsection (e)(7) is actionable only under the catch-all civil remedy provision in subsection (g)(1)(D)). Plaintiffs' claim fails because the alleged information that the FBI and the DoD maintained related to authorized law enforcement activities, and would therefore be exempted from subsection (e)(7).

1. Subsection (e)(7) is limited by the law enforcement exception.

Subsection (e)(7) of the Privacy Act generally prohibits federal agencies from maintaining records that describe how an individual exercises First Amendment rights:

> Each agency that maintains a system of records shall . . . 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). The D.C. Circuit has held that subsection (e)(7) applies to records outside of systems of records. *See Gerlich*, 711 F.3d at 169 ("The obligations imposed by subsection (e)(7) are not limited to records maintained in a system of records."); *see also Albright v. United States*, 631 F.2d 915, 918-19 (D.C. Cir. 1980).

The scope of subsection (e)(7)'s applicability, although broad, is subject to the law enforcement exception. *See Maydak*, 363 F.3d at 517 ("Although the Privacy Act does not define 'law enforcement activity,' we have interpreted the phrase broadly."); *Sieverding*, 693 F. Supp. 2d at 105. The exception covers many forms of federal investigations, including information gathered as part of any authorized criminal, intelligence, or administrative investigation. *See Nagel v. U.S. Dep't of Health, Educ. & Welfare*, 725 F.2d 1438, 1441 n.3 (D.C. Cir. 1984). In addition, the exception extends to all persons associated with the investigation – including crime victims – and not merely to the target of the investigation. *See J. Roderick MacArthur Found. v. FBI*, 102 F.3d 600, 602 (D.C. Cir. 1996). Moreover, by its plain text, the law enforcement exception is not limited to only law enforcement investigations, but rather it encompasses any "authorized law enforcement activity." *See* 5 U.S.C. § 552a(e)(7); *J. Roderick MacArthur Found.*, 102 F.3d at 602. Accordingly, the law enforcement exception extends to matters that are not under active investigation and to matters that are not a current law enforcement necessity. *See J. Roderick MacArthur Found.*, 102 F.3d at 602, 603.

2. The law enforcement exception precludes plaintiffs' claim under subsection (e)(7).

Even assuming the truth of plaintiffs' allegation that either the FBI or the DoD maintained records describing how plaintiffs exercised their First Amendment rights, any such records would come within the law enforcement exception. According to the complaint, both the FBI and the DoD were engaged in law enforcement activity that implicated Jill Kelley's emails. For instance, plaintiffs allege that the FBI was investigating Jill Kelley's report that she was receiving cyberstalking threats through email. *See, e.g.*, Compl. ¶¶ 33, 35, 41. The complaint also alleges that the DoD was investigating whether General Allen had an inappropriate relationship with Jill Kelley. *See, e.g., id.* ¶¶ 72, 74, 75. Based on those allegations, the collection of information regarding Jill Kelley's email correspondence was related to either the FBI's cyberstalking investigation or the DoD's investigation of General Allen's conduct. And criminal investigations and administrative investigations constitute authorized law enforcement activities for purposes of the law enforcement exception. *See Nagel*, 725 F.2d at 1441 n.3. Therefore, any collection and maintenance of information for those investigations would be well within the law enforcement exception. *See Doe v. FBI*, 936 F.2d at 1361 (finding no violation of subsection (e)(7) where the records at issue constituted "the underlying investigative records in the FBI's files"); *Scott v. Conley*, -- F. Supp. 2d --, 2013 WL 1409310, at *16 (D.D.C. Apr. 9, 2013) (requiring allegations that an agency had no valid law enforcement reason for the records as a prerequisite to stating a claim under subsection (e)(7)). Consequently, Count IV should be dismissed for failure to state a claim for relief.

F. Plaintiffs Do Not State a Claim for Relief against the FBI and the DoD for Failure to Establish Privacy Act Safeguards.

In count VI, plaintiffs allege that FBI and DoD violated subsection (e)(10) of the Privacy Act by failing to establish safeguards to ensure the security and confidentiality of records. *See* Compl. ¶¶ 158-68. Plaintiffs' allegations simply repeat, verbatim at times, the text of the Privacy Act. *See, e.g., id*. ¶ 161 (quoting the text of subsection (e)(10), but only upon information and belief); *id.* ¶ 167 (alleging in conclusory fashion, and only upon information and belief, that the federal government "acted intentionally and/or willfully in violation of the Kelleys' privacy rights"). Those parroted allegations, by themselves, are insufficient to state a claim for relief. Neither formulaic recitations of the elements of an offense nor conclusory allegations satisfy the pleading standards. *See Twombly*, 550 U.S. at 555; *Kowal*, 16 F.3d at 1275; *Nat'l ATM Council*, 922 F. Supp. 2d at 79. Plaintiffs' allegations are weakened further still because they are based on "information and belief," a convention not recognized in the rules of civil procedure. *Cf.* Fed. R. Civ. P. 8(a) (setting forth the standards for pleading a claim). While "information and belief" allegations are sometimes permitted, it is often due to the presence of additional factual allegations that support the reliability or the plausibility of the professed information and belief. *See, e.g., Jefferson v. Collins*, 905 F. Supp. 2d 269, 288-89 (D.D.C. 2012); *Robertson v. Cartinhour*, 867 F. Supp. 2d 37, 59 n.57 (D.D.C. 2012). Here, however, there is no plausible basis for plaintiffs' allegations because as matters within judicial notice, the FBI and the DoD have in fact established numerous Privacy Act safeguards. Thus, as elaborated below, plaintiffs do not state a claim for a violation of subsection (e)(10).

Subsection (e)(10) requires that agencies establish safeguards for Privacy Act systems of records. Specifically, subsection (e)(10) requires each agency that maintains a system of records to

> 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). As its text indicates, subsection (e)(10) imposes an obligation to *establish safeguards*, but not to *safeguard* all Privacy Act protected information – other more specific provisions of the Privacy Act govern the safeguarding of Privacy Act protected information, such as the disclosure prohibition in subsection (b). The requirement to establish safeguards in subsection (e)(10) applies only to an agency's systems of records, and not to every record that an agency maintains. *See Gerlich*, 711 F.3d at 167; *Maydak*, 363 F.3d at 518 (explaining that the obligation to implement Privacy Act safeguards in subsection (e)(10) does not apply to all records, but only to systems of records); *see also* 40 Fed. Reg. at 28,966. And where an agency has preexisting safeguards in place, a plaintiff must identify a safeguard that the agency should have established but did not. *See Doe v. U.S. Dep't of Justice*, 660 F. Supp. 2d 31, 43 (D.D.C. 2009); *Chambers*, 568 F.3d at 1007 n.7. In addition, the Privacy Act does not provide a specific civil claim for damages resulting from a violation of subsection (e)(10), and therefore plaintiffs' claim for failing to establish safeguards can proceed only under the Privacy Act's catchall provision, which requires an allegation of intentional and willful agency action. *See* 5 U.S.C. § 552a(g)(1)(D) & (g)(4).

Measured against these standards, plaintiffs fail to state a claim for a violation of subsection (e)(10). Nor can they, as both the FBI and the DoD have established Privacy Act safeguards. In specific part, the Department of Justice has promulgated regulations mandating the implementation of security requirements for systems of records by all of its components, including the FBI:

> (a) Each component shall establish administrative and physical controls to prevent unauthorized access to its systems of records, to prevent unauthorized disclosure of records, and to prevent physical damage to or destruction of records. The stringency of these controls shall correspond to the sensitivity of the records that the controls protect. At a minimum, each component's administrative and physical controls shall ensure that:
>
> (1) Records are protected from public view;
>
> (2) The area in which records are kept is supervised during business hours to prevent unauthorized persons from having access to them;
>
> (3) Records are inaccessible to unauthorized persons outside of business hours; and
>
> (4) Records are not disclosed to unauthorized persons or under unauthorized circumstances in either oral or written form.
>
> (b) Each component shall have procedures that restrict access to records to only those individuals within the Department who must have access to those records in order to perform their duties and that prevent inadvertent disclosure of records.

28 C.F.R. § 16.51; *see also id.* § 16.54 (setting forth employee standards of conduct with respect to information protected by the Privacy Act). Courts in this District have repeatedly acknowledged the adequacy of these safeguards in rejecting claims that the FBI failed to establish Privacy Act safeguards. *See, e.g., Doe v. U.S. Dep't of Justice*, 660 F. Supp. 2d 31, 43 (D.D.C. 2009); *Krieger v. U.S. Dep't of Justice*, 529 F. Supp. 2d 29, 54-55 (D.D.C. 2008). In addition to the regulatory safeguards, each of the FBI's systems of records has specific safeguarding provisions published in the Federal Register. For instance, the FBI's system of records for investigative, personnel, applicant, administrative, and general files – known as the Central Records System – contains additional published safeguards as well:

> Records are maintained in a restricted area and are accessed only by agency personnel. All FBI employees receive a complete background investigation prior to being hired. All employees are cautioned about divulging confidential information or any information contained in FBI files. Failure to abide by this provision violates Department of Justice regulations and may violate certain statutes providing maximum severe penalties of a ten thousand dollar fine or 10

> years imprisonment or both. Employees who resign or retire are also cautioned about divulging information acquired in the jobs. Registered mail is used to transmit routine hard copy records between field offices. Highly classified records are hand carried by Special Agents or personnel of the Armed Forces Courier Service. Highly classified or sensitive privacy information, which is electronically transmitted between field offices, is transmitted in encrypted form to prevent interception and interpretation. Information transmitted in teletype form is placed in the main files of both the receiving and transmitting field offices. Field offices involved in certain complicated investigative matters may be provided with on-line access to the duplicative computerized information which is maintained for them on disk storage in the FBI Computer Center in Washington, DC, and this computerized data is also transmitted in encrypted form.

63 Fed. Reg. 8659, 8683 (Feb. 20, 1998). Through measures such as these, the adequacy of which plaintiffs do not contest, the FBI has established safeguards for the protection of information protected by the Privacy Act.

The DoD has also enacted comprehensive Privacy Act safeguards. For instance, the DoD has established a Defense Privacy Office whose responsibilities include ensuring that "[a]ppropriate procedures and safeguards shall be developed, implemented, and maintained to protect personal information when it is stored in either a manual and/or automated system of records or transferred by electronic or non-electronic means." *See* DoD Directive No. 5400.11 at § E4.4.2.9.2 (May 8, 2007, as amended Sept. 1, 2011) (available at http://www.dtic.mil/whs/directives/corres/pdf/540011p.pdf). In addition, the DoD has promulgated regulations that impose responsibility on each component for the protection of Privacy Act records:

> C1.4.1. General Responsibilities. DoD Components shall establish appropriate administrative, technical and physical safeguards to ensure that the records in each system of records are protected from unauthorized access, alteration, or disclosure and that their confidentiality is preserved and protected. Records shall be protected against reasonably anticipated threats or hazards that could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual about whom information is kept.

C1.4.2. Minimum Standards

C1.4.2.1. Tailor system safeguards to conform to the type of records in the system, the sensitivity of the personal information stored, the storage medium used and, to a degree, the number of records maintained.

C1.4.2.2. Treat all unclassified records that contain personal information that normally would be withheld from the public under Freedom of Information Exemption Numbers 6 and 7, chapter 3 of Reference (d) as "For Official Use Only (FOUO)," and safeguard them accordingly, in accordance with DoD 5200.1-R (Reference (h)), even if they are not actually marked "FOUO."

C1.4.2.3. Personal information that does not meet the criteria discussed in paragraph C1.4.2.2 of this Chapter shall be accorded protection commensurate with the nature and type of information involved.

C1.4.2.4. Special administrative, physical, and technical procedures are required to protect data that is stored or processed in an IT system to protect against threats unique to an automated environment. See Appendix 1.

C1.4.2.5. Tailor safeguards specifically to the vulnerabilities of the system.

See DoD Privacy Program, DoD 5400.11-R, at C1.4 (May 14, 2007) (available online at www.dtic.mil/whs/directives/corres/pdf/540011r.pdf). The DoD has also implemented safeguards for its thousand-plus systems of records. *See* http://dpclo.defense.gov/privacy/SORNs/component/DOD_Component_Notices.html (listing system of records notice for DoD components). For instance, the DoD has published safeguards for a system of records within the Inspector General's Office – referred to as CIG-15 – which contains information related to administrative investigations of senior officials related to violations of laws, rules, or regulations or mismanagement. Those safeguards limit the persons who may access the records and provide physical and technical protections:

> Records are maintained in locked rooms accessible only to Office of the Deputy Inspector General for Investigations personnel having official need-to-know and [the] electronic data system is password protected.

73 Fed. Reg. 61,085, 61,089 (Oct. 15, 2008). These measures demonstrate that the DoD has established Privacy Act safeguards, and plaintiffs allege no deficiency in those efforts. Consequently, plaintiffs fail to state a claim for a violation of subsection (e)(10).

In addition, plaintiffs do not adequately allege that the FBI or the DoD acted intentionally or willfully. To satisfy that element, plaintiffs would have to allege facts that the FBI and the DoD acted with flagrant disregard for individuals' privacy rights in not establishing certain Privacy Act safeguards. *See Albright*, 732 F.2d at 189; *see also Maydak*, 630 F.3d at 180. This element presents "a high standard, requiring a showing of 'something greater than gross negligence' on the agency's part." *Djenasevic*, 579 F. Supp. 2d at 136 (quoting *Tijerina v. Walters*, 821 F.2d 789, 799 (D.C. Cir. 1987)); *see also Hurt v. D.C. Court Servs. & Offender Supervision Agency*, 827 F. Supp. 2d 16, 20 (D.D.C. 2011) (characterizing the Privacy Act's intentional and willful element as "a high hurdle to clear"). Under this standard, a plaintiff must allege agency action that is "so 'patently egregious and unlawful' that anyone undertaking the conduct should have known it 'unlawful.'" *Laningham v. U.S. Navy*, 813 F.2d 1236, 1242 (D.C.Cir.1987) (quoting *Wisdom v. Dep't of Hous. & Urban Dev.*, 713 F.2d 422, 425 (8th Cir.1983)). Where a complaint lacks such allegations, it should be dismissed. *See, e.g., Scott v. Conley*, -- F. Supp. 2d --, 2013 WL 1409310, at *16 (D.D.C. Apr. 9, 2013) (dismissing a Privacy Act claim for damages where the allegations did not satisfy the intentional and willful standard); *McIntyre v. Fulwood*, 892 F. Supp. 2d 209, 218 (D.D.C. 2012) (same); *Djenasevic*, 579 F. Supp. 2d at 136 (same). The complaint does not meet that standard because plaintiffs do not provide any facts suggesting that the FBI and the DoD – despite promulgating numerous Privacy Act safeguards – flagrantly disregarded privacy rights by not establishing any

(unspecified) safeguard. On that basis as well, Count VI should be dismissed for failure to state a claim.

CONCLUSION

For the foregoing reasons, Counts I through VII of plaintiffs' complaint, the only counts for which plaintiffs have perfected service, should be dismissed, partially for a lack of subject matter jurisdiction and the remainder for a failure to state a claim for relief.

September 24, 2013

Respectfully Submitted,

STUART F. DELERY
Assistant Attorney General

JOHN R. TYLER
Assistant Branch Director

/s/ *Peter J. Phipps*
PETER J. PHIPPS (DC Bar #502904)
Senior Trial Counsel
U.S. Department of Justice, Civil Division
Federal Programs Branch
Tel: (202) 616-8482
Fax: (202) 616-8470
Email: peter.phipps@usdoj.gov

Mailing Address:
P.O. Box 883 Ben Franklin Station
Washington, DC 20044

Courier Address:
20 Massachusetts Ave., NW
Washington, DC 20001

Attorneys for Defendants