

**UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA**

LAWANDA YORK,

Plaintiff,

v.

JOHN MCHUGH,
Secretary of the Army,

Defendant.

Civil Action No. 09-075 (BAH)
Judge Beryl A. Howell

MEMORANDUM OPINION

Plaintiff Lawanda York, a former employee of the U.S. Army Reserve, initiated this case after learning that personal medical information pertaining to her was placed by her supervisor on a shared network drive that could be accessed by other employees. The plaintiff is suing the Office of the Army Reserve¹ pursuant to the Privacy Act, 5 U.S.C. § 552a, to seek redress for the pain and embarrassment caused by the release of her private information. Pending before the Court is the defendant's motion for summary judgment, which argues that the plaintiff cannot establish a violation of the Privacy Act. For the reasons explained below, the Court agrees and the defendant's motion for summary judgment is GRANTED.

I. BACKGROUND

A. Factual Background

From May 2005 to March 2007, plaintiff Lawanda York was employed in the Office of the Chief of Army Reserve, Army Reserve Communications ("ARC") Directorate, Outreach Branch as a GS-13 Public Affairs Specialist. Def.'s Statement of Material Facts ("Def.'s SMF"), ECF No. 33-2, ¶ 1. On July 26, 2006, the plaintiff met with her supervisor, Lieutenant Colonel

¹ Pursuant to Rule 25(d), on March 22, 2010, the Court substituted John McHugh, in his official capacity as the Secretary of the Army, for Francis J. Harvey as a defendant in this action. Mem. Op., ECF No. 18, at 1 n.1.

Laurel Hubred, for counseling and to review the plaintiff's job description and basic responsibilities. *Id.* ¶ 4. During the course of the meeting, the plaintiff indicated that she had thoughts of suicide, was on anti-depressants, and made other statements regarding her mental condition that caused Lt. Col. Hubred concern. *Id.* ¶ 6. Following the meeting, Lt. Col. Hubred prepared a memorandum for her files and also sought guidance from her supervisor, Colonel Dorothy Perkins, on how to handle the situation. *Id.* ¶ 6.

Sometime thereafter, Colonel Perkins and Sheila Bailey, a human resources specialist, met with the plaintiff to discuss her mental health and the availability of Army counselors to assist the plaintiff.² *Id.* ¶ 9. Although the specifics of what transpired at that meeting are in dispute, after the meeting Colonel Perkins prepared a memorandum (the "Perkins Memo") detailing the subject of the meeting for her records. *Id.* ¶ 10. Colonel Perkins saved the Perkins Memo on her private workplace computer. *Id.*

On December 2, 2006, Colonel Perkins was deployed to Iraq for six months. *Id.* ¶ 11. In order to preserve the files and make them available to her supervisors while deployed, Colonel Perkins' complied with an order to move her electronic files from her computer to the ARC Directorate shared drive, known as the "J drive." *Id.* ¶ 13; Def.'s Second Mot. Summ. J., ECF No. 33, Ex. B, Dep. Col. Perkins, 20:11-21:18. Along with Colonel Perkins' other electronic files, the Perkins Memo and other documents with the plaintiff's name "York" in the filename were also placed on the J drive.³ Def.'s SMF, ¶ 14; Compl., Ex. 2. These files were contained in

² The parties dispute the exact dates of the meeting, the drafting of the subsequent memorandum of record, and the exact date on which files were uploaded onto the shared drive. *See* Pl.'s Reply to Def.'s Statement of Material Facts ("Pl.'s SMF"), ECF No. 36-4, at ¶¶ 7, 16. The exact dates of these events are immaterial for the purposes of the present motion. The Court will therefore discuss the facts underlying this case without referencing specific dates for the aforementioned events.

³ The exact number of documents relating to the plaintiff on the shared J drive is unclear. While the exhibits attached to the Complaint indicate that there were approximately eleven documents on the shared drive, the plaintiff alleges in her deposition that fifteen such files existed. *See* Compl., Ex. 2; Def.'s Second Mot. Summ. J., ECF No.

a sub-folder called “COL Perkins’ files,” and were not indexed or grouped in any particular manner. Def.’s SMF, ¶ 15. The documents concerning the plaintiff were mixed in with all of the other documents in the “COL Perkins’ files” folder, and were not otherwise separated or distinguished. *Id.* ¶ 15.

The shared J drive on which the Perkins Memo was uploaded is accessible only to those Army Reserve employees who are given permission to access the drive, which both parties agree includes at least the other members of the ARC staff. *Id.* ¶ 16; Pl.’s SMF ¶ 16; *see also* Decl. Felicia Davis Batte, ECF No. 6-2, ¶ 4 (indicating that the shared drive is only accessible to those who “can authenticate to the Army Reserve domain”). The defendant asserts that there is “no indication that any individual with access to the J drive accessed this document or any other documents concerning Plaintiff other than Plaintiff herself and Ms. Linda Moore who was asked by Plaintiff to access the document.” Def.’s SMF ¶ 17. The plaintiff disputes the defendant’s characterization of the facts. Although she cannot identify any individual who viewed the files containing her private information, the plaintiff states that Master Sergeant Rodriguez, another Army Reserve employee, must have known about the Perkins Memo because “around January 2007” he told her: “You know, people know your business. You really should check into it.” Pl.’s SMF ¶ 17; Pl.’s Opp’n Mot. Summ. J., ECF No. 36, at 6-7. Neither party contends or provides any direct testimony from any individual who claims to have accessed the files containing the plaintiff’s personal information, with the exception of Linda Moore who accessed the files after the plaintiff discovered them and upon the plaintiff’s request.

On March 14, 2007, the plaintiff conducted a search for the term “standards” on the shared J drive in order to find documents relating to a work assignment. Def.’s Second Mot.

33, Ex. A, Dep. Lawanda York, 17:20-18:8, 24:25-25:6. The particular number of documents is not relevant to determining whether the plaintiff has alleged a violation of the Privacy Act, but the Court notes that the number of documents was not voluminous.

Summ. J., ECF No. 33, Ex. A, Dep. Lawanda York, 22:16-23:6. The search yielded a number of documents, including documents relating to the plaintiff's comments to Col. Perkins. *Id.* Upon learning that documents referencing the plaintiff's personal medical and mental health were on the shared J drive, the plaintiff instructed Ms. Moore, a work colleague, to "[s]ee if you can find anything on me on the shared drive" in order to confirm that the documents were accessible by other employees, which they were. *Id.* at 25:20-25:25.

After learning that her personal information was accessible to other employees, the plaintiff states that she became visibly upset and physically ill. Compl. ¶¶ 13-16. According to the plaintiff, the trauma resulting from the alleged disclosure of her personal information caused her to miss work and contact her therapist, who became concerned for her well-being and prescribed her medication. *Id.*

On March 15, 2007, the plaintiff sent an email to multiple ARC personnel demanding that the documents pertaining to her be removed from the J drive. Pl.'s SMF ¶ 18; Def.'s SMF ¶ 18. That same day, the files were removed and placed on a compact disk for Colonel Perkins' use upon her return from Iraq. Pl.'s SMF ¶¶ 19, 20.

B. Procedural History

On January 9, 2009, the plaintiff filed a Complaint against the U.S. Army Reserve, alleging that the disclosure of her personal medical information violated the Privacy Act. *See* 5 U.S.C §§ 552a(b), (g)(1)(D). The plaintiff alleges this alleged wrongful disclosure "humiliated and embarrassed" her and negatively affected her medical health. In redress for her injuries, the plaintiff seeks "actual damages," plus attorney's fees and costs. Compl. at 4.

In response to the Complaint, on April 6, 2009, the defendant moved to dismiss this action, or, in the alternative, for summary judgment, arguing that (1) the protections of the

Privacy Act do not apply because the shared J drive was not a “system of records”; (2) the plaintiff failed to allege actual disclosure; and (3) the plaintiff’s alleged injuries were not caused by any such disclosure. Def.’s Mot. Dismiss, ECF No. 6. On March 22, 2010, the Court denied the defendant’s motion to dismiss and denied without prejudice the defendant’s motion for summary judgment. Mem. Op., ECF No. 18 (Kollar-Kotelly, J.). Specifically, the Court withheld judgment on whether the J drive was a “system of records” within the meaning of the Privacy Act, stating that “this issue cannot be resolved without resorting to matters outside the pleadings” and the plaintiff was entitled to a period of discovery to gather evidence to substantiate her claim. *Id.* at 9. The Court also held that plaintiff had sufficiently alleged actual disclosure of her medical information and a resulting injury. *Id.* at 9-10.

Following denial of the defendant’s motion to dismiss, on May 25, 2010, the Court directed the parties, in accordance with the parties’ request in the Joint Meet and Confer Report, to complete discovery by October 25, 2010. ECF Nos. 20-21. The Court granted the parties’ request to extend the discovery deadline three times, and the parties ultimately completed discovery on March 15, 2011.

On June 8, 2011, the defendant filed a renewed motion for summary judgment, arguing again that (1) the shared J drive does not constitute a “system of records” under the Privacy Act; (2) the plaintiff cannot prove actual disclosure of the Perkins Memo; (3) there is no causation between the plaintiff’s alleged injuries and actual disclosure; and (4) there is no evidence that the defendant willfully or intentionally disclosed the plaintiff’s records. Def.’s Second Mot. Summ. J., ECF No. 33, at 1. This motion is pending before the Court.

As explained below, the Court agrees that the plaintiff cannot establish a claim under the Privacy Act. Accordingly, the defendant's motion for summary judgment is GRANTED and judgment is entered in favor of the defendant.

II. LEGAL STANDARD

Pursuant to Rule 56 of the Federal Rules of Civil Procedure, summary judgment shall be granted "if the movant shows that there is no genuine dispute as to any material fact and the movant is entitled to judgment as a matter of law." FED. R. CIV P. 56(a); *Anderson v. Liberty Lobby*, 477 U.S. 242, 247 (1986); *Estate of Parsons v. Palestinian Auth.*, 651 F.3d 118, 123 (D.C. Cir. 2011); *Tao v. Freeh*, 27 F.3d 635, 638 (D.C. Cir. 1994). "The mere existence of *some* alleged factual dispute between the parties," however, will not defeat summary judgment; "the requirement is that there be no *genuine* issue of *material* fact." *Holcomb v. Powell*, 433 F.3d 889, 895 (D.C. Cir. 2006) (citing *Anderson*, 477 U.S. at 247-48) (emphasis in original).

The burden is on the moving party to demonstrate the absence of a "genuine issue of material fact." *Anderson*, 477 U.S. at 248. Thus, in ruling on a motion for summary judgment, the Court must draw all justifiable inferences in favor of the nonmoving party, and shall accept the nonmoving party's evidence as true. *Id.*; *Estate of Parsons*, 651 F.3d at 123; *Tao*, 27 F.3d at 638. That said, the plaintiff still bears the burden of setting forth sufficient evidence to raise a triable issue of material fact as to each element of his claim. *See Matsushita Elec. Indus. Co. v. Zenith Radio Corp.*, 475 U.S. 574, 587 (1986) (while the movant bears the initial responsibility of identifying those portions of the record that demonstrate the absence of a genuine issue of material fact, the burden shifts to the non-movant to "come forward with 'specific facts showing that there is a *genuine issue for trial*.'") (citing FED. R. CIV. P. 56(e)) (emphasis in original). "The nonmoving party cannot defeat summary judgment by simply showing that there is some

metaphysical doubt as to material facts.” *Moore v. Hartman*, 571 F.3d 62, 66 (D.C. Cir. 2009) (quoting *Matsushita Elec. Indus.*, 475 U.S. at 586). Instead, the non-moving party must show that a genuine factual issue exists by, *inter alia*, citing to particular parts of materials in the record, including depositions, documents, and affidavits or declarations; or “showing that the materials cited do not establish the absence or presence of a genuine dispute” FED. R. CIV. P. 56(c)(1). For a factual dispute to be “genuine,” the non-moving party must demonstrate more than “the mere existence of a scintilla of evidence” in support of its position, and it cannot simply rely on allegations or conclusory statements. *Estate of Parsons*, 651 F.3d at 123 (quoting *Anderson*, 477 U.S. at 255); *Ass’n of Flight Attendants-CWA v. U.S. Dep’t of Transp.*, 564 F.3d 462, 465-66 (D.C. Cir. 2009). Indeed, conclusory assertions offered without any factual basis in the record cannot create a genuine dispute. *See Ass’n of Flight Attendants*, 564 F.3d at 465 (“[A]lthough, as a rule, statements made by the party opposing a motion for summary judgment must be accepted as true for the purpose of ruling on that motion, some statements are so conclusory as to come within an exception to that rule.”).

Additionally, only disputes over “material” facts will preclude the Court from entering summary judgment. *Holcomb*, 433 F.3d at 895 (citing *Anderson*, 477 U.S. at 248). “A fact is ‘material’ if a dispute over it might affect the outcome of a suit under governing law; factual disputes that are ‘irrelevant or unnecessary’ do not affect the summary judgment determination.” *Id.* “If material facts are at issue, or, though undisputed, are susceptible to divergent inferences, summary judgment is not available.” *Moore*, 571 F.3d at 66. When there are no genuine issues of material fact, however, the moving party is entitled to judgment as a matter of law if the nonmoving party, after an adequate time for discovery, “fails to make a showing sufficient to establish the existence of an element essential to that party’s case, and on which that party will

bear the burden of proof at trial.” *Holcomb*, 433 F.3d at 895 (quoting *Celotex Corp. v. Catrett*, 477 U.S. 317, 322 (1986)).

III. DISCUSSION

The plaintiff alleges that by placing information pertaining to her medical and mental condition on the shared J drive, the defendant violated the Privacy Act. The defendant argues, however, that the plaintiff cannot demonstrate that the defendant violated the provisions of the Privacy Act because, *inter alia*, the shared J drive on which the Perkins Memo and related documents concerning the plaintiff were placed is not a “system of records,” and that the plaintiff cannot demonstrate actual disclosure of her confidential information.⁴ While there is no dispute that the defendant unfortunately handled highly personal and confidential information relating to the plaintiff in a manner that made it available for other employees to view, the Court agrees that this action did not violate the Privacy Act.

A. The Privacy Act

The Privacy Act, 5 U.S.C. § 552a, “safeguards the public from unwarranted collection, maintenance, use and dissemination of personal information contained in agency records . . . by allowing an individual to participate in ensuring that his records are accurate and properly used.” *Cloonan v. Holder*, No. 08-cv-700, 2011 WL 782028, at *6 (D.D.C. Mar. 8, 2011) (quoting *Henke v. Dep’t of Commerce*, 83 F.3d 1453, 1456 (D.C. Cir. 1996)). “To accomplish this goal, the Act ‘gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government’s part to comply with

⁴ The defendant further argues that the plaintiff’s Privacy Act claim fails because, absent any actual disclosure, the plaintiff cannot establish causation between such disclosure and her alleged injuries. In addition, the defendant contends that there is no evidence that the defendant willfully or intentionally disclosed the plaintiff’s records. Def.’s Second Mot. Summ. J, ECF No. 33, at 11-14. The Court need not evaluate, however, whether these requirements for a Privacy Act violation are met since the plaintiff cannot demonstrate that the shared J drive is a system of records or that actual disclosure of any confidential information occurred. In any event, the Court notes that the defendant’s assertion that Col. Perkins uploaded the documents to the shared J drive pursuant to an order from her superiors would not necessarily foreclose inquiry into whether her act was willful or intentional.

the requirements.” *Id.* (quoting *Doe v. Chao*, 540 U.S. 614, 618 (2004)). “For example, the Act limits the circumstances under which an agency may disclose records of individuals, mandates that agencies closely account for all disclosures, and requires agencies to make reasonable efforts to ensure the accuracy and completeness of records.” *Id.* (internal citations omitted).

In this case, the plaintiff alleges that the defendant violated the Privacy Act by disclosing her private medical information. Compl. ¶¶ 18-22. The Privacy Act provides that “[n]o agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains” 5 U.S.C. § 552a(b). While the Privacy Act protects against disclosure of information, “[n]ot every nonconsensual disclosure of information contained in Privacy Act-protected records constitutes a violation of the Privacy Act.” *Feldman v. CIA*, 797 F. Supp. 2d 29, 38 (D.D.C. 2011). The Act provides various exceptions for disclosure, such as disclosure to employees who have a need for the record to perform their duties, records that must be disclosed under the Freedom of Information Act, 5 U.S.C. § 552, and various other exceptions that are not applicable to the instant dispute. *See* 5 U.S.C. § 552a(b)(1)-(12). Most importantly here, “the Privacy Act only covers disclosures of information that [were] either directly or indirectly retrieved from a system of records. Thus, the disclosure of information derived solely from independent sources is not prohibited by the statute even though identical information may be contained in a system of records.” *Feldman*, 797 F. Supp. 2d at 38 (citing *Doe v. U.S. Dep’t of Treasury*, 706 F. Supp. 2d 1, 6 (D.D.C. 2009)). Accordingly, “[t]o prevail on a Privacy Act claim for unlawful disclosure, ‘a plaintiff must show that (1) the disclosed information is a ‘record’ contained within a ‘system of records’; (2) the agency improperly disclosed the information; (3) the disclosure was willful or

intentional; and (4) the disclosure adversely affected the plaintiff.” *Id.* (quoting *Doe*, 706 F. Supp. 2d at 6).

B. The Shared J Drive is Not A System of Records

As discussed above, the Privacy Act protects against disclosure of records that are contained within a “system of records,” which the Act defines as

a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual[.]

5 U.S.C. § 552a(a)(5). The D.C. Circuit has stated that “[a] system of records exists only if the information contained within the body of material is both retrievable by personal identifier and actually retrieved by personal identifier.” *Paige v. Drug Enforcement Admin.*, 665 F.3d 1355, 1359 (D.C. Cir. 2012) (quoting *Maydak v. United States*, 630 F.3d 166, 178 (D.C. Cir. 2010)). “[R]etrieval capability is not sufficient to create a system of records.” *Henke v. U.S. Dep’t of Commerce*, 83 F.3d 1453, 1460 (D.C. Cir. 1996). The plaintiff must demonstrate that records are actually retrieved by a personal identifier. *Maydak*, 630 F.3d at 172, 178; *Henke*, 83 F.3d at 1460; (“[A] group of records should generally not be considered a system of records unless there is actual retrieval of records keyed to individuals.”); *Bartel v. Fed. Aviation Admin.*, 725 F.2d 1403, 1408 n.10 (D.C. Cir. 1984) (“To be in a system of records, a record must be under the agency’s control, and, in practice, retrieved by an individual’s name or other personal identifier.”); *Krieger v. U.S. Dep’t of Justice*, 529 F. Supp. 2d 29, 42 (D.D.C. 2008) (“The mere capacity to retrieve information indexed under a person’s name, as opposed to a practice where agency employees in fact retrieve records in this way, is insufficient to establish the existence of a system of records under the Privacy Act.”) (internal quotations omitted)); *see also* Office of Management and Budget Privacy Act Implementation Guidelines and Responsibilities, 40 Fed.

Reg. 28,948, 23,952 (July 9, 1975) (identifying a system of records only if: (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 some personal identifier”).

The defendant argues that the shared J drive is not a system of records because information is not actually retrieved from the drive by personal identifier. Although it is possible to retrieve information from the drive by searching for specific terms, the defendant asserts that, for documents on the J drive, “it is not the purpose or the practice of the agency to retrieve documents by a personal identifier,” and “the mere capability of retrieving a document by a name is not enough to create a system of records.” Def.’s Second Mot. Summ. J., ECF No. 33, at 9. Based upon the undisputed evidence in the record, the Court agrees.

The defendant attests that the shared J drive consists of “over 13,346 folders and sub-folders” and that the drive does not have “indexing or retrieval capability using identifying particulars built into the shared drive to allow personnel to retrieve [sic] files or documents by name or personal identifier.” Decl. Felicia Davis Batte, ECF No. 6-2, ¶ 5. The defendant acknowledges that it is possible to retrieve documents by using individual search terms, but states that “the [Army Reserve] does not retrieve records using an individual’s personal identifier and that is not the way the shared drive is set up.” *Id.*

The plaintiff does not rebut the defendant’s assertion that the shared J drive is not set up for employees to retrieve records by use of personal identifiers. She argues instead that “[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.” Pl.’s Opp’n Def.’s Second Mot. Summ. J., ECF No. 36, at 12. The plaintiff, however, supplies no evidence, let alone asserts, that

the agency does, in practice, retrieve information on the J drive using individuals' names or personal identifiers. To the contrary, the plaintiff states that "anyone *can* use a personal identifier and find files by such a search, *if so desired*." *Id.* at 11 (emphasis added). The mere capability of retrieving information by personal identifier is simply not sufficient to establish that a system of records exists. *See Henke*, 83 F.3d at 1460.

Indeed, the plaintiff herself acknowledges that "incidental or *ad hoc* retrieval by personal identifier does not convert a group of records into a system of records." Pl.'s Opp'n Second Mot. Summ. J., ECF No. 36, at 9. Nonetheless, she contends that "where an agency compiles information about individuals for investigatory purposes, 'Privacy Act concerns are at their zenith, and if there is evidence of even a few retrievals of information keyed to [personal identifiers], it may well be the case that the agency is maintaining a system of records.'" *Id.* (quoting *Henke*, 83 F.3d at 1461). In support of this proposition, the plaintiff argues that this case is "very similar" to *Bartel v. Federal Aviation Administration*, 725 F.2d 1403 (D.C. Cir. 1984). In *Bartel*, the plaintiff alleged a violation of the Privacy Act after his former supervisor disclosed the findings of an investigation report concerning the plaintiff's conduct. The D.C. Circuit held that although the plaintiff's supervisor may not have "retrieved" the disclosed information from the investigatory file, and may have spoken instead from personal knowledge about the contents of the investigation, the Privacy Act's coverage is not "restricted to information directly retrieved from a tangible recording." *Id.* at 1409.

Bartel is inapplicable to this case for two reasons. First, the facts and circumstances are different. Unlike *Bartel*, there is no evidence that the Perkins Memo or other documents relating to the plaintiff were compiled as part of a formal "investigation." The investigation referenced in *Bartel* concerned the plaintiff's own potentially unlawful disclosure of information, which was

then referred to the United States Attorney for potential criminal prosecution. That situation is a far cry from the instant case where the plaintiff's supervisors met with the plaintiff for a counseling session and recorded personal notes of that session. *See generally Armstrong v. Geithner*, 608 F.3d, 854, 859 (D.C. Cir. 2010) (stating that the court "narrowly tethered the exception [in *Bartel*], however, to the facts of that case").

Second, and more importantly, the plaintiff appears to contend that under *Bartel*, the plaintiff need not demonstrate that the Perkins Memo was contained within a system of records. This is incorrect. At issue in *Bartel* was the scope of the disclosure requirement under the Privacy Act and that is a different issue from whether the documents in this case were contained within a system of records. Indeed, *Bartel* provided minimal discussion of whether the investigatory file at issue was placed in a system of records. To the extent that *Bartel*'s discussion of disclosure is applicable in this case, as the defendant notes, the plaintiff "has no evidence of any disclosure of specific information by any Army employee, regardless of whether that information was independent of or derived from agency records." Def.'s Reply, ECF No. 39, at 16.

Finally, the plaintiff argues at length that the Perkins Memo is a "record" under the Privacy Act. This discussion misses the point. The question is not whether the Perkins Memo and other documents relating to the plaintiff were records,⁵ but whether such records were placed in a system of records.

Although it may appear counterintuitive, the Privacy Act does not protect against

⁵ In a footnote in its reply brief, the defendant states that it "assumes for the purposes of this Reply that the memoranda at issue are 'Privacy Act records,'" but contends that "[i]t is reasonable to believe that the memorandum for record in the present case is not even a record because it falls within the category of 'personal notes.'" Def.'s Reply, ECF No. 39, at 15 n.10. (citing *Bowyer v. Dep't of Air Force*, 804 F.2d 428, 431 (7th Cir. 1986)). The Court need not resolve this issue because, regardless, the Perkins Memo and other documents related to the plaintiff were not placed in a system of records.

disclosure of all records containing personal and private information. In this case, the defendant's placement of documents relating to the plaintiff's mental and physical health on a network drive accessible to other employees was unfortunate and unacceptable. As the D.C. Circuit admonished in *Paige*, "although not an abuse of a system of records," the agency's conduct "is far from a model of agency treatment of private data." *Paige*, 665 F.3d at 1362. Nonetheless, Congress limited the scope of the protections of the Privacy Act to only those files that are "under the control of" the agencies. 5 U.S.C. § 552a(a)(5) ("the term 'system of records' means a group of any records under the control of any agency . . ."); PRIVACY ACT GUIDELINES, at 13-14 (1975), *reprinted in* LEGIS. HISTORY OF THE PRIVACY ACT OF 1974: SOURCE BOOK ON PRIVACY 156, 1027-28 (1976) ("SOURCE BOOK"). This limitation "was intended to accomplish two separate purposes: (1) to determine possession and establish accountability; and (2) to separate agency records from records which are maintained personally by employees of agency but which are not agency records." SOURCE BOOK, at 1027. Congress thus intended for agencies to protect against disclosure of information, but restricted liability only for those records maintained and indexed in a "system of records."

When an agency incorporates records into a "system of records," other Privacy Act prescriptions apply as well. For example, the agency must "publish in the Federal Register" detailed information concerning the nature and scope of the system. *See* 5 U.S.C. § 552a(e)(4). Second, the agency must "upon request by an individual to gain access to his record or to any information pertaining to him which is contained in the system, permit him . . . to review the record and have a copy made of all or any portion thereof in a form comprehensible to him." 5 U.S.C. § 552a(d)(1). Third, the agency is obliged not to disclose records without the consent of the individual to whom the record pertains. 5 U.S.C. § 552a(b). Clearly, these

obligations do not apply to every document created by an agency employee but only to those records considered sufficiently important to the agency's operations or mission to become part of the agency's system of records. Thus, courts that have been confronted with disclosures of documents stored or maintained by agency employees in their desk drawers, in their file cabinets or on their personal computers have regularly concluded that, even if the documents were agency records, they fall outside the "system of records" requirement and, therefore, outside the protections of the Privacy Act. *See, e.g., Boyd v. Secretary of the Navy*, 709 F.2d 684, 686-87 (11th Cir. 1983) (because memorandum "was kept within a random-type file and could only be retrieved by searching through the file," it was not in a "system of records"); *Gowan v. U.S. Dep't of the Air Force*, 148 F.3d 1182, 1191 (10th Cir. 1998) (materials contained in a general disciplinary file labeled "Ethics" do not constitute a system of records because the files are not keyed to the plaintiff); *Hudson v. Reno*, 130 F.3d 1193, 1206 (6th Cir. 1997) ("notes about Plaintiff's misconduct which were kept in a locked drawer and labeled the 'First Assistant's' files" are not in a system of records because they were not retrievable under plaintiff's name), *abrogated on other grounds by Pollard v. E.I. du Pont de Nemours & Co.*, 532 U.S. 843, 848 (2001); *Rivera v. Potter*, 400 F. Supp. 2d 404, 409-10 (D.P.R. 2005) (printouts of email messages, which contained communications of supervisors regarding an investigation of the plaintiff, that were found in USPS facility bathroom where plaintiff worked were not part of any "system of records" and therefore no violation of the Privacy Act occurred). Otherwise, agencies would be forced, for example, to search all the myriad places where an employee could store records to comply with the access requirements of the Privacy Act. As one Circuit court observed, "it is inconceivable that Congress intended to impose such an obligation. The Act clearly envisions that an agency can satisfy its obligation simply and inexpensively by searching

its structured files under the individual's name or other identifying symbol.” *Bechhoefer v. United States Dep’t of Justice*, 312 F.3d 563, 567 (2d Cir. 2002).

The Court recognizes that in this case the filenames of the documents pertaining to the plaintiff contained the plaintiff's name, which allowed her to discover the files by searching the shared J drive for “York,” her last name. Def.’s Mot. Summ. J., ECF No. 33, Ex. A, Dep. Lawanda York, 26:13-26:20. The fact that some documents were labeled with her name does not convert the shared J drive into a system of records, particularly where there is no evidence that the agency used the shared drive to retrieve information by personal identifiers and the drive was not created for employees to do so. *See* Decl. Felicia Davis Batte, ECF No. 6-2, ¶ 5 (stating that “[t]he shared drive is not organized in a manner to facilitate retrieving documents or files by an individual's name or personal identifier. . . . Although it is possible to retrieve documents in the manner described by Mrs. York, [the Army Reserve] does not retrieve records using an individual's personal identifier and that is not the way the shared drive is set up.”); *see also Bechhoefer*, 312 F.3d at 566-67 (finding that a letter stored in an agency employee's drawer with the plaintiff's name on the letterhead was not in a “system of records” and therefore the Privacy Act was not violated when the letter was disclosed).

In this case, the plaintiff cannot demonstrate that the shared J drive is a system of records. Consequently, the defendant is entitled to judgment as a matter of law.

C. The Plaintiff Cannot Demonstrate Actual Disclosure

Even assuming that the shared J drive is a system of records, to sustain a claim that the defendant violated the Privacy Act the plaintiff must demonstrate that the agency improperly disclosed the information. The defendant argues that the plaintiff's claim fails because she

cannot show actual disclosure of the Perkins Memo or other documents related to her on the shared J drive. The Court agrees.

Although the Privacy Act requires the plaintiff to demonstrate improper disclosure, “[n]ot every nonconsensual disclosure of information contained in Privacy Act-protected records constitutes a violation of the Privacy Act.” *Feldman*, 797 F. Supp. 2d at 38. An improper disclosure under the Privacy Act “generally must result from an individual’s having ‘actually retrieved’ the information from the system of records in which it is contained.” *Paige*, 665 F.3d at 1359; *see also Armstrong v. Geithner*, 608 F.3d 854, 857 (D.C. Cir. 2010); *Bartel*, 725 F.2d at 1408 (“[Section 552a(b)] prohibits nonconsensual disclosure of any information that has been retrieved from a protected record.”). Thus, “[t]he disclosure of information derived solely from independent sources is not prohibited by the statute even though identical information may be contained in [a] system of records.” *Doe v. U.S. Dep’t of Treasury*, 706 F. Supp. 2d 1, 6 (D.D.C. 2009).

The defendant asserts that “there is no evidence that an actual disclosure occurred,” which the plaintiff must demonstrate in order to maintain her Privacy Act claim. Def.’s Second Mot. Summ. J., ECF No. 33, at 3. On this point, the defendant is correct. During her deposition, the plaintiff was asked if there was anyone who would testify that they “actually found documents on the shared driver prior to . . . March 14,” to which plaintiff responded “[t]here’s no proof that it was accessed and there’s no proof that it wasn’t.” Def.’s Second Mot. Summ. J., ECF No. 33, Ex. A, Dep. Lawanda York, 28:11-28:21. Given that the plaintiff bears the burden at trial of proving by a preponderance of the evidence that actual disclosure occurred, and her concession that there is no evidence of such actual disclosure, the plaintiff’s Privacy Act claim must fail.

The plaintiff argues that there is “at least a question of material fact” as to whether other employees viewed the documents containing the plaintiff’s information and that it is “highly likely that other employees saw these files.” Pl.’s Opp’n Def.’s Second Mot. Summ. J., ECF No. 36, at 16. Although she can supply no direct evidence, the plaintiff states that “[i]n some instances, circumstantial evidence alone can support a finding that a disclosure came from a record.” *Id.* at 14. In this case, the plaintiff relies solely on a comment made by Master Sgt. Rodriguez in January 2007, three months prior to her discovering the Perkins Memo on the shared J drive. According to the plaintiff, Master Sgt. Rodriguez informed her that “people know your business” and that “everyone knew what was going on with me and that I should research more on how the information was getting out.” *Id.* at 6-7. The plaintiff believes that her narration of this single conversation can sustain her burden of proving that actual disclosure occurred, but it simply cannot.

As the defendant notes, the plaintiff was told only that others knew her “business,” which is an “amorphous assertion [that] could refer to any number of things.” Def.’s Reply, ECF No. 39, at 18. Moreover, Master Sgt. Rodriguez did not work in the plaintiff’s office and did not have access to the shared J drive. Def.’s Second Mot. Summ. J., ECF No. 33, Ex. A, Dep. Lawanda York, 29:1-29:4; *see also* Def.’s Reply, ECF No. 39, at 11-12. The simple fact that he knew of the plaintiff’s “business” is indeterminate because he could have obtained information through a number of alternate sources. Finally, to the extent that the plaintiff relies on her own recollection of the conversation she had with Master Sgt. Rodriguez in order to prove that disclosure actually occurred, that evidence is most likely inadmissible hearsay. *See Gleklen v. Democratic Congressional Campaign Comm.*, 199 F.3d 1365, 1369 (D.C. Cir. 2000) (stating that “[w]hile a nonmovant is not required to produce evidence in a *form* that would be admissible at

trial [at the summary judgment stage], the evidence still must be capable of being converted into admissible evidence” and holding that the plaintiff’s “evidence about [a] conversation is sheer hearsay” and “therefore counts for nothing”). The record does not include any testimony from Master Sgt. Rodriguez, or any of the plaintiff’s other work colleagues, to substantiate the plaintiff’s claim that others knew about her “business,” or that if they were aware of such “business,” the information was obtained from viewing files relating to the plaintiff on the shared J drive.

The plaintiff relies on *Doe v. U.S. Postal Service*, 317 F.3d 339 (D.C. Cir. 2003), to argue that evidence showing that the plaintiff’s private information was “common knowledge” to coworkers is sufficient to withstand summary judgment. In that case, however, the court denied summary judgment because the record contained deposition testimony from at least four of the plaintiff’s co-workers, who all testified that the plaintiff’s supervisor disclosed information regarding the plaintiff’s HIV status and that this supervisor had access to protected records. Here, the plaintiff can supply no such evidence. The only evidence that the plaintiff can supply is purely circumstantial, inconclusive, and likely inadmissible hearsay. A reasonable juror therefore would not be able to conclude that the plaintiff sustained her burden of demonstrating that actual disclosure of confidential information occurred.

IV. CONCLUSION

For the reasons stated above, the defendant’s motion for summary judgment is GRANTED. An appropriate Order shall accompany this Memorandum Opinion.

DATED: MARCH 27, 2012

/s/ Beryl A. Howell
BERYL A. HOWELL
United States District Judge