UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL-CIO, *et al.*, Plaintiffs, v. U.S. OFFICE OF PERSONNEL MANAGEMENT, *et al.*, Defendants.	Case No. 1:25-cv-01237-DLC

PLAINTIFFS' OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

Page(s)

TABLE OF AUTHORITIES

Page(s)

Cases

Statutes

Other Authorities

INTRODUCTION

Congress passed the Privacy Act following Watergate and the Counterintelligence Program (COINTELPRO) scandal "to restore trust in government and to address what at the time was seen as an existential threat to American democracy."[1] Congress recognized that the federal government's increasing use of databases full of personal records "greatly magnified the harm to individual privacy," and sought to tightly regulate their use by agencies. PL 93–579, 88 Stat 1896 (1974).

The Complaint here plausibly and specifically alleges that in violation of the Privacy Act, the Office of Personnel Management ("OPM") is disclosing databases full of sensitive personal data to the so-called Department of Government Efficiency ("DOGE") and its agents who have no right or authority to access them. Both agencies have also failed to protect the security of those records. Defendants' motion to dismiss should fail.

Plaintiffs have Article III standing.[2] Defendant OPM's actual and ongoing disclosure of Plaintiffs' records to other government officials, and the agencies' lack of security protections, closely mirror violations of historic privacy torts—both intrusion upon seclusion and disclosure of private facts—as well as privacy invasions under the Constitution. Independently, the security failings and disclosure create an imminent risk of future harms: including both government misuse of the records for retaliation among other improper uses, and an even larger data breach at an agency that is already a hacking target. All these harms are traceable to the agencies' Privacy Act violations and can be immediately remedied by an injunction.

Plaintiffs allege that OPM is unlawfully disclosing Plaintiffs' sensitive records to DOGE

[1] U.S. DOJ Overview of the Privacy Act of 1974 (2020 Edition) at 1, https://www.justice.gov/Overview_2020/dl?inline.

[2] References to "Plaintiffs" include union Plaintiffs' members.

agents, not merely granting access that was never used. 5 U.S.C. § 552a(b). Plaintiffs allege that some DOGE agents who obtained these records are not employees of OPM, and none need a massive number of sensitive records to perform their legitimate IT modernization duties. Additionally, Plaintiffs allege that both OPM and DOGE are failing to secure the records. § 552a(e)(10).

In addition to the Complaint's numerous allegations of disclosure that are based on credible news reporting, President Trump's January 20, 2025, Executive Order ("E.O.") itself helps show that OPM disclosed records to DOGE, an agency outside of OPM. The E.O. also helps demonstrate that there is no need for DOGE agents working on "modernizing Federal technology and software" to obtain the sensitive personal records of more than 20 million people. The E.O. contemplates only actions "consistent with the law" and in accordance with "rigorous data protection standards"—not actions that violate the Privacy Act. Defendants failed to follow this command.

Plaintiffs seek injunctive and declaratory relief only, not monetary damages. The Privacy Act itself allows for injunctive relief given the statute's text, structure, and purpose.

But if the Privacy Act does not provide the relief Plaintiffs seek, the Administrative Procedures Act ("APA") allows such relief, as does the court's authority to restrain *ultra vires* conduct. OPM's disclosure and both agencies' security failures in violation of the Privacy Act are unlawful and have deprived Plaintiffs of their privacy rights, constituting reviewable final agency action under the APA.

Under the same fact pattern, a federal court in Maryland entered a preliminary injunction against OPM. *American Federation of Teachers v. Bessent (AFT)*, Civ. No. DLB-25-0430, ECF No. 68 (March 24, 2025). As here, the court found: Plaintiffs have standing by analogy to common law (*id.* at 26); OPM disclosed records to DOGE agents who did not need them in violation of the

Privacy Act (*id.* at 54-55); and that constitutes final agency action. (*id.* at 33, 40).

FACTS

On January 20, 2025, President Trump signed the E.O. establishing DOGE for the purpose of "modernizing federal technology and software." Complaint ("Compl."), ECF No. 1, ¶¶ 3-6, 24-27; Exec. Order No. 14,158, 90 C.F.R. 8441 (2025). The E.O. creates three sets of DOGE actors: (1) it renames the existing "U.S. Digital Service" to the "U.S. DOGE Service" (USDS); (2) within USDS, it creates "the U.S. DOGE Service Temporary Organization" for 18 months; and (3) it directs other agencies to establish internal "DOGE Teams" to implement "the President's DOGE Agenda." § 3(a)-(c).

The Complaint and this Opposition to dismissal refer to all three as "DOGE" or "DOGE agents."[3] The E.O. makes clear that some of the individuals are not officers or employees of OPM. Individuals working for USDS and the Temporary Organization are employees of USDS. § 3(a)-(b). Individuals who make up "DOGE Teams" established within OPM and other agencies are primarily "Special Government Employees" who can be "hired or assigned" from other agencies, including USDS. § 3(c). While OPM's leader must establish a DOGE Team and select its members, it must do so "in consultation with USDS" and team members must "coordinate their work" with USDS. *Id.* The news articles cited in the Complaint use various terms—rather than E.O. definitions—to describe DOGE individuals who obtained OPM records.[4] Compl. ¶¶ 29-30.

[3] Specifically, "DOGE" includes all four DOGE Defendants, their employees and contractors, their detailees to OPM, dual DOGE-OPM employees, and employees who work principally on the DOGE agenda. *See* Compl. ¶¶ 3-6, 24-27 (describing DOGE).

[4] *Washington Post*, "Musk's DOGE agents access sensitive personnel data, alarming security officials" (Feb. 6, 2025), www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/ ("Musk's DOGE agents"; "Agents of billionaire Elon Musk's Department of Government Efficiency"; "members of Musk's pseudo-governmental

The E.O. itself instructs agencies to disclose records, or grant "full and prompt access to" records, to USDS. § 4(b). But disclosure of records to USDS must be "consistent with law" and must be done with "rigorous data protection standards"—meaning agencies must follow the Privacy Act. *Id.*

Starting on January 20, 2025, OPM gave DOGE agents broad access to "all" personnel systems at OPM, including the Enterprise Human Resources Integration; Electronic Official Personnel Folder; USAJOBS; USA Staffing; USA Performance; and Health Insurance. Compl. ¶¶ 29-30. These systems house extremely sensitive records on Plaintiffs, who are former and current federal employees. ¶¶ 2, 15-21, 28. The records contain social security numbers, employment information, financial information, union activity, health information, and much more. ¶ 2.

Plaintiffs specifically and plausibly allege that OPM actually disclosed those records to DOGE agents, not merely that DOGE agents were granted access. *See* Compl. ¶¶1, 8, 9, 10, 11, 15, 18, 19, 20, 29, 30, 31, 36, 37, 40, 41, 42, 46, 48, 49, 62. The Complaint also incorporates news reports from the *Washington Post* and *Musk Watch* that describe these disclosures and subsequent use. ¶¶ 29-30. This includes DOGE agents searching through individual workers' position descriptions in OPM systems and using OPM records to create a mass email list of workers. *Id.* DOGE agents have also set up a server to control the personnel databases. *Id.*

Plaintiffs also allege security failings at OPM and DOGE (¶ 42) including: OPM gave

---

DOGE"; "members of Musk's DOGE team"; "the DOGE team"; "DOGE agents"; "DOGE team member"; "members of the DOGE team"; "DOGE representatives").

Musk Watch, "Musk associates given unfettered access to private data of government employees" (Feb. 3, 2025), https://www.muskwatch.com/p/musk-associates-given-unfettered ("Musk's associates installed at the Office of Personnel Management"; "Musk team running OPM"; "Musk associates"; "government outsiders"; "Musk underlings embedded at OPM"; "Musk's team"; "Musk's aides"; "Musk" himself).

DOGE agents "administrative" access to all personnel systems at OPM on the day the new agency was established, which allows them to alter internal documentation of their own activity (¶ 9); neither OPM nor DOGE properly conducted security vetting before allowing officials to access OPM's systems, resulting in the hiring of a person who was previously fired from a cybersecurity firm in relation to an internal investigation into leaking proprietary information (¶¶ 8, 33); neither OPM nor DOGE provided officials with proper training before officials gained access to OPM's systems (¶ 58); and DOGE Defendants do not maintain public security policies. ¶ 58.

Plaintiffs allege that OPM's disclosure to DOGE and both agencies' security failings have caused harm in the form of: privacy invasion from OPM actually disclosing records to DOGE (¶¶ 2, 8-9, 28-31); imminent risk that DOGE will misuse these records, including to fire supposedly "disloyal" employees (¶¶ 39-40); and imminent risk, caused by Defendants' recklessness, of records theft. ¶¶ 8-9, 32, 41-42.

ARGUMENT

I. PLAINTIFFS HAVE ARTICLE III STANDING

For standing, "a plaintiff must show (i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021). "Where, as here, the defendants move to dismiss a complaint based on a 'facial' challenge to the plaintiffs' standing (meaning that defendants do not offer any evidence of their own), the court must 'determine whether, accepting as true all material factual allegations of the complaint, and drawing all reasonable inferences in favor the plaintiffs, the complaint alleges facts that affirmatively and plausibly suggest that the plaintiffs have standing to sue.'" *Farrakhan*

v. ADL, 23cv9110 (DLC), 2024 WL 1484449, *3 (S.D.N.Y. 2024) (Cote, J.).[5]

Here, the Complaint contains detailed and plausible allegations of standing. Plaintiffs below separately address their actual and imminent injuries in fact, each of which alone supports standing. Plaintiffs next address causation and redressability.

Three named individual Plaintiffs assert their own injuries. Compl. ¶¶ 18-20. Two union Plaintiffs have associational standing to assert their members' injuries. ¶¶ 15-17. *See Building Trades Council v. Downtown Dev., Inc.*, 448 F.3d 138, 144 (2d Cir. 2006) (finding associational standing where, as here, an association's members have standing, their interests are germane to the association's purpose, and member participation is not needed); *Nat'l Assn. of Letter Carriers v. USPS*, 604 F. Supp. 2d 665, 670 (S.D.N.Y. 2009) (finding a union had associational standing to assert a Privacy Act claim for its members). *Cf.* Memorandum of Law in Support of Defendants' Motion to Dismiss, ECF No. 62 ("MTD") at 5.

A. Actual Records Disclosure Injures Plaintiffs.

Defendant OPM is disclosing records to DOGE agents. Compl. ¶¶ 2, 8-9, 28-31. Some are employed by OPM and some are employed by DOGE. *Supra* at 3. *Cf.* MTD 1 (erroneously suggesting that Plaintiffs allege disclosure only to "non-governmental DOGE actors"). They accessed and used OPM records. *Supra* at 4. *Cf.* MTD 7 (erroneously suggesting that Plaintiffs allege only that OPM "granted … access" to DOGE). Both agencies failed to secure the records. *Supra* at 4-5.

This is "concrete" injury[6] under *TransUnion*, 594 U.S. at 423. This is because it has "a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit." *Id.* at

[5] On a "facial" Rule 12(b)(1) challenge as here, "the plaintiff has no evidentiary burden." *Carter v. HealthPort*, 822 F.3d 47, 56 (2d Cir. 2016). *Cf.* MTD 4.

[6] It also is "actual," so need not be "imminent." *TransUnion*, 594 U.S. at 423.

424. An "intangible" injury can be "concrete" if it has an "analogue" in common law privacy—namely, "intrusion upon seclusion" or "disclosure of private information"—or to "harms specified by the Constitution." *Id.* at 424-25. Here, Plaintiffs' injuries are closely analogous to all three.

The analogy need be "close" but not "exact." *Id.* at 424. A plaintiff need not "adequately plead every element of an analog." *Salazar v. NBA*, 118 F.4th 533, 543 n.6 (2d Cir. 2024). It is "irrelevant" whether a plaintiff "would prevail" at common law. *Persinger v. Sw. Credit Sys., L.P.*, 20 F.4th 1184, 1192 (7th Cir. 2021). *See also In re USAA Data Sec. Ltgn.*, 621 F. Supp. 3d 454, 466 (S.D.N.Y. 2022) (analog was "close" though "debatable"); *Rand v. Travelers Co.*, 637 F. Supp. 3d 55, 66 (S.D.N.Y. 2022) (same).

In assessing concreteness, courts afford "due respect" to Congress. *TransUnion*, 594 U.S. at 425. Here, the Privacy Act gives "forceful recognition" to the "confidentiality of sensitive information" in "personnel files." *NASA v. Nelson*, 562 U.S. 134, 156 (2011).

1. Plaintiffs' injuries are analogous to intrusion on seclusion.

Intrusion on seclusion addresses "invasion into matters that a person would deem deeply private, personal, and confidential." *Mills v. Saks.com*, 23 Civ. 10638 (ER), 2025 WL 34828, *4 (S.D.N.Y. 2025). It covers "one who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another…if the intrusion would be highly offensive to a reasonable person." *Id.* (quoting Restatement of Torts § 652B). It does not require "any publicity." Restatement § 625B, cmt. a.

Here, the analogy is close. Plaintiffs' personal records contain their race, disability, medical conditions, union activity, and more. Compl. ¶ 2. Individually and taken together, the records are "deeply private, personal, and confidential." OPM's actual disclosure to DOGE agents is an "intrusion" that reasonable people would find "highly offensive."

Thus, three courts have already found concrete injury from records disclosure to DOGE by

analogy to this tort. In *AFT*, Civ. No. DLB-25-0430, 2025 WL 582063, *15 (D. Md. Feb. 24, 2025), the court granted a temporary restraining order enjoining OPM from disclosing records to OPM employees working on the DOGE agenda. Finding standing, it reasoned the "sensitive" records at issue "create a comprehensive picture of the plaintiffs' familial, professional, or financial affairs." *Id.* at 6. In *Alliance for Retired Americans v. Bessent*, Civ. No. 25-0313 (CKK), 2025 WL 740401, *17 (D.D.C. March 7, 2025), the court found standing, emphasizing "the sensitivity of the information." In *AFSCME v. Social Security Administration*, Civ. No. ELH-25-0596, 2025 WL 868953, *43-44 (D. Md. March 20, 2025), the court found standing, given the "unrestricted access to PII" provided to DOGE "without specified need, and/or without adequate training, detail agreements, and/or background investigations." *See also EPIC v. OPM*, Civ. No. 1:25-cv-255 (RDA/WBP), 2025 WL 580596, *6 (E.D. Va. Feb. 21, 2025) (standing "based on the common law tort of intrusion upon seclusion may be sustainable").[7]

Likewise, courts find concrete injury by analogizing this tort to data privacy injuries like the one here. For example:

- It is analogous to using a tracking pixel to disclose video viewing to a third party, violating the Video Privacy Protection Act (VPPA). *Pileggi v. Wash. Newspaper Co.*, Civ. No. 23-345 (BAH), 2024 WL 324121, *5 (D.D.C. 2024); *Feldman v. Star Tribune Co.*, 659 F. Supp. 3d 1006, 1014-15 (D. Minn. 2023); *James v. Disney Co.*, 701 F. Supp. 3d 942, 951 (N.D. Cal. 2023).
- It is analogous to acquisition of a "propensity-to-pay score," violating the Fair Credit Reporting Act. *Persinger*, 20 F.4th at 1192.

[7] In *Doe v. OPM*, Civ. No. 25-234 (RDM)2025 WL 513268, *5-6 (D.D.C. Feb. 17, 2025), the plaintiff did not "identify any common-law analogues," and challenged a much narrower disclosure than here (just name, work email, and possibly workplace). *Cf.* MTD 10.

- The umbrella "invasion of privacy" tort is analogous to collecting biometrics, *Bryant v. Compass Group*, 958 F.3d 617, 623, 626 (7th Cir. 2020), and retaining them, *Fox v. Dakkota LLC*, 980 F.3d 1146, 1154-55 (7th Cir. 2020), violating the Illinois Biometric Information Privacy Act (BIPA). *See also Seale v. Peacock*, 32 F.4th 1011, 1020-21 (10th Cir. 2022) (holding this umbrella tort analogous to unauthorized access under the Stored Communications Act).

Defendants erroneously attempt to graft a novel element onto the analogy to intrusion on seclusion: that a person "examined" or "reviewed" the data. MTD 7-8. The cases above don't require this, and Defendants cite none that do. In *Feldman*, the court ruled that the intrusion need not be "accompanied by review" of the data, rejecting the defendant's objection that it had not been "seen by *anybody*." 659 F. Supp. 3d at 1015 (emphasis in original). As to the "examples" of intrusions in a Comment to the Restatement (MTD 7), examples are not requirements, and it is highly intrusive to "open" a sealed envelope without reading the letter. Regardless, the news reports cited in the Complaint describe subsequent review by DOGE, not just access. Compl. ¶ 29-30.

2. Plaintiffs' injuries are analogous to disclosure of private fact.

Disclosure of private fact is a "well-established common-law analog" that prohibits "publicity to a matter concerning the private life of another," if it would be "highly offensive to a reasonable person" and "not of legitimate concern to the public." *Salazar*, 118 F.4th at 541 (quoting Restatement of Torts § 652D). Here, the records are "private," and Defendant OPM disclosed them to DOGE agents who have no "legitimate concern" with them.

Thus, in *State of New York v. Trump*, 25-CV-01144 (JAV), 2025 WL 573771, *27 (S.D.N.Y. Feb. 21, 2025), the court preliminarily enjoined the Treasury Department from disclosing records to DOGE. It ruled the "past harm in the unauthorized disclosure" of financial

information was "concrete," after identifying "disclosure of private fact" as a "well-established common-law analog." *Id.* at 11.

Likewise, the Second Circuit has twice analogized this tort to privacy injury like the one here. In *Salazar*, the court analogized it to the VPPA injury of disclosure to just one entity. 118 F.4th at 541-43; *accord Martin v. Meredith Corp.*, 657 F. Supp. 3d 277, 283 (S.D.N.Y. 2023) (Cote, J.); *Carter v. Scripps Networks, LLC*, 670 F. Supp. 3d 90, 95-96 (S.D.N.Y. 2023). In *Bohnak v. Marsh Co.*, the court analogized it to negligent cybersecurity that caused a breach, even though the stolen data had not been misused. 79 F.4th 276, 279, 285-86 (2d Cir. 2023); *accord Rand*, 637 F. Supp. 3d at 66 (S.D.N.Y.); *Wynne v. Audi*, No. 21-cv-08518-DMR, 2022 WL 2916341, *4-5 (N.D. Cal. July 25, 2022). Further, the Seventh Circuit analogized common law to disclosure of biometrics to just one vendor, because the BIPA violation deprived the plaintiff of "control" over their data. *Cothran v. White Castle*, 20 F.4th 1156, 1161 (7th Cir. 2023). *See also DOJ v. RCFP*, 489 U.S. 749, 763 (1989) ("privacy encompasses the individual's control of information concerning [their] person").

Defendants' argument that there is no harm because there has not been public disclosure of Plaintiffs' records lack merit. MTD 8-9. The records need not be "publicly" disclosed: disclosure to one entity is enough, like to a pixel owner (*Salazar*, 118 F.4th at 541-43), a thief (*Bohnak*, 79 F.4th at 285-86), or a vendor (*Cothran*, 20 F.4th at 1161). Nor is disclosure "outside of the government" required: disclosure to DOGE agents is enough, *Trump*, 2025 WL 573771 * 27.

3. Plaintiffs' injuries are analogous to unconstitutional search.

TransUnion authorizes analogy from challenged injury to "harms specified by the Constitution." 594 U.S. at 425. Accordingly, by congressional design, the Privacy Act parallels the Fourth Amendment in restricting unjustified collection, disclosure, and use of personal data by

the government. Congress found "the right to privacy is a personal and fundamental right *protected by the Constitution*," and so it was "necessary … to regulate the collection, maintenance, use, and dissemination" of personal data. PL 93-579, 88 Stat. 1896 (1974) (emphasis added). Thus, in *Patel v. Facebook, Inc.*, the court found "concrete" injury when a company processed biometrics in violation of BIPA, given the "close historical relationship" between such injury and "constitutionally protected zones of privacy." 932 F.3d 1264, 1472-73 (9th Cir. 2019). That court emphasized "recent Fourth Amendment jurisprudence" recognizing that "advances in technology can increase the potential for unreasonable intrusions into personal privacy." *Id.*

Here, there is a close analogy between the Privacy Act and the Fourth Amendment: both limit how government processes the data of its own employees. *See, e.g., City of Ontario v. Quon*, 560 U.S. 746, 756 (2010) ("The Fourth Amendment applies … when the government acts in its capacity as employer.").

Another close analogy is that the Privacy Act and the Fourth Amendment both limit new disclosures and uses of old data. Specifically, the Fourth Amendment guarantees that the government must have a new justification—and ordinarily a warrant—for a new disclosure or use of data. *See, e.g., U.S. v. Hasbajrami*, 945 F.3d 641, 670 (2d Cir. 2019) (search by FBI of communications data collected by NSA is "a separate Fourth Amendment event that, in itself, must be reasonable"); *U.S. v. Runyan*, 275 F.3d 449, 464 (5th Cir. 2001) (search enabled by earlier "private search" is limited to its "scope," and further search requires warrant); *U.S. v. Sedaghaty*, 728 F.3d 885, 913 (9th Cir. 2013) (search enabled by warrant is limited to its "scope," and further search requires "obtaining a new warrant").

Unconstitutional search is closely analogous to Plaintiffs' injury. OPM unlawfully disclosed personal records to government officials who don't need them. Compl. ¶¶ 8-9, 29-31.

Cf. In re OPM Breach Ltgn., 928 F.3d 42, 54-55 (D.C. Cir. 2019) (breach victims sufficiently pled "concrete" injury to "constitutional right to informational privacy").

B. Imminent Records Misuse and Theft Injures Plaintiffs.

Plaintiffs also are injured by future risks caused by OPM's current disclosures to DOGE agents and security failures. First, DOGE agents may misuse these records. Compl. ¶¶ 39-40. Second, thieves or foreign adversaries may steal them. ¶¶ 8-9, 32, 41-42. These harms are "concrete" and "imminent." *TransUnion*, 594 U.S. at 423.

1. The risks of misuse and theft are concrete.

If a plaintiff alleges "concrete" injury from "material risk" that "information would be disseminated in the future to third parties," they "may pursue forward-looking, injunctive relief to prevent the harm from occurring," if they show the separate standing requirement of "imminent" risk. *TransUnion*, 594 U.S. at 435. So the risks of misuse and theft are concrete if they are imminent.

These risks also are concrete by analogy to the three traditional harms above. *See Trump*, 2025 WL 573771, *12 ("risk of future harm" through disclosure to DOGE and "potential hacking" was "concrete," noting the analogy to "disclosure of private fact").

2. The risks of misuse and theft are imminent.

Injury is "imminent" if it "is certainly impending, or there is a substantial risk that harm will occur." *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 158 (2014) (cleaned up). Here, the injury is both.

In *Trump*, the court found "imminent" injury based on "the risk of exposure of [the plaintiffs'] confidential information to officials of USDS/DOGE and to the public through potential hacking." 2025 WL 573771, *12. The court reasoned that the disclosures were "rushed and ad hoc," "broad and unprecedented," and "undertaken under political pressure"; that the

government conceded this "created heightened security risks"; and that it was "unclear whether training was provided." *Id.* The court cited opinions that "routinely" found injunctive relief standing "where inadequate cybersecurity measures" put "confidential information at risk." *Id.* (citing *Baton v. Ledger*, 740 F. Supp. 3d 847, 882 (N.D. Cal. 2024); *USAA*, 621 F. Supp. 3d at 473; *In re Cap. One Breach Ltgn.*, 488 F. Supp. 3d 374, 414-15 (E.D. Va. 2020).

As in *Trump*, Plaintiffs' Complaint here alleges imminent injury because OPM provided DOGE agents "sweeping authority to install and modify software" and "alter internal documentation of their own activities" under pressure (Compl. ¶ ¶ 9, 29); DOGE agents exercised this authority to "disrupt[]"systems (¶ 32), and implement "new and untested protocols [and] technologies" absent "security safeguards" (¶ 42); and new staff lacked vetting (¶¶ 8-9, 33). When criminals and foreign nations inevitably "exploit the chaos" (¶ 32), Plaintiffs will be exposed: to identity theft (¶ 42) and to "retaliation from people who oppose their agency's work" (¶¶ 40-41). Plaintiffs also allege risk that DOGE agents will misuse this data, for example, to fire people who are transgender or "disloyal," or to "shutter entire departments." ¶ 40.

Likewise, the Second Circuit held that data breach victims faced "imminent" injury, though their data had not been misused. *Bohnak*, 79 F.4th at 288; *accord Rand*, 637 F. Supp. 3d at 67. It reasoned that the plaintiff's data "was exposed as a result of a targeted attempt by a third party to access the data set," which included sensitive data like "name and SSN." 79 F.4th at 289. The court specifically held that "known misuse of information" is not needed to show "imminent" injury. *Id.* Plaintiffs here likewise suffer intentional exposure of their highly sensitive data.

Defendants' contrary arguments fail. MTD 9-12. Injury here is not speculative: as in *Trump* and *Bohnak*, it is imminent. Indeed, Defendant OPM's earlier neglect caused one of the worst data breaches in history. Compl. ¶ 32.

Given the extraordinary factual context, the Court should "not confer [the] presumption" of regularity to OPM's and DOGE's actions, especially "when the government says one thing while expressly doing another." *Nat'l Council of Nonprofits v. Off. of Mgmt. and Budget*, 25-cv-239-LLA, ECF No. 51 (D.D.C. Feb. 25, 2025) (declining to apply the presumption of good faith on voluntary cessation); *id.* ¶ 6-8. In any event, courts "decline to consider the presumption of regularity at the motion to dismiss stage…since presumptions are evidentiary standards that are inappropriate for evaluation at the pleadings stage." *Dorce v. City of New York*, 608 F. Supp. 3d 118, 142 n.9 (S.D.N.Y. 2022).[8] While Defendants allege disclosure to only "a limited number" of people, MTD 10, that is outside the pleadings and needs discovery.

C. Plaintiffs' Injuries are Caused by Defendants and Redressable by Injunction.

Plaintiffs specifically and plausibly allege that OPM disclosed records and DOGE agents accessed them. Also, there is imminent risk of misuse and theft, given Defendants' reckless creation of new cybersecurity vulnerabilities. *Supra* at 4-5. Thus, Plaintiffs' injuries plainly are "caused by" Defendants and can be "redressed by" an injunction that prohibits ongoing unlawful disclosure and requires DOGE agents to delete copies of information unlawfully obtained. *TransUnion*, 594 U.S. at 423.

Defendants suggest the only disclosure at issue is to an "OPM DOGE team" and not to "non-OPM DOGE." MTD 11. But Plaintiffs dispute this. *Supra* at 3, 6. Regardless, disclosure within OPM still violates the Privacy Act because it is not necessary, *see infra* section II(A)(3), and it creates imminent risk of retaliation, theft and misuse. Finally, Defendants argue that risk

[8] The "facial" Rule 12(b)(1) posture here is unlike the factual posture in *USPS v. Gregory*, 534 U.S. 1, 10 (2001) (appeal from "ALJ's factual findings"), and *Schneiter v. U.S.*, 159 Fed. Cl. 356, 374-76 (2022) (denying motion based on sworn statement). *Cf.* MTD 10-11.

from "intra-governmental access" is low, MTD 11, but that just rehashes their failed arguments against injury-in-fact.

II. PLAINTIFFS ADEQUATELY ALLEGE PRIVACY ACT VIOLATIONS

Plaintiffs allege Defendants have violated two provisions of the Privacy Act: unlawful records disclosure, 5 U.S.C. § 552a(b), and cybersecurity failures, *id.* § (e)(10). A "complaint will survive a motion to dismiss under Rule 12(b)(6) if it alleges facts that, taken as true, establish plausible grounds to sustain a plaintiff's claim for relief." *Cornelio v. Connecticut*, 32 F.4th 160, 168 (2d Cir. 2022). Courts "construe the complaint liberally, accept all factual allegations in the complaint as true, and draw[] all reasonable inferences in the plaintiff's favor." *Costin v. Glens Falls Hosp.*, 103 F.4th 946, 952 (2d Cir. 2024).

A. Plaintiffs State a Claim for Violation of 5 U.S.C. § 552a(b).

Under Section (b) of the Privacy Act, an agency may not "disclose any record" to "any person" or "agency" without consent, unless a statutory exception applies. 5 U.S.C. § 552a(b). Exception (b)(1) from the Act's anti-disclosure rule only authorizes a disclosure made to "officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." § 552a(b)(1). Here, the well-pled allegations in the Complaint make clear that Defendants disclosed Plaintiffs' protected records, without their consent, to DOGE agents who had no need to use them in the course of the legitimate duties, including to non-OPM employees. *Supra* at 3-4.

Among other things, Plaintiffs specifically and plausibly allege that OPM actually disclosed their records to DOGE agents, not merely that DOGE agents were granted access. *See* Compl. ¶¶1, 8, 9, 10, 11, 15, 18, 19, 20, 29, 30, 31, 36, 37, 40, 41, 42, 46, 48, 49, 62. *Cf.* MTD 7. The news reports cited in the Complaint even describe use following access. *Id.* ¶ 29-30. Defendants cannot excuse their unauthorized disclosures by reading the term "viewed" into the

definition of "disclose." MTD n.4. *Cf. Devine v. U.S.*, 202 F.3d 547, 551-52 (2d Cir. 2000) (noting "we shall not read in additional conditions"). While Plaintiffs allege more, simply "making available information" is a disclosure under 552a(b). *Quinn v. Stone*, 978 F.2d 126, 134 (3d Cir. 1992); *see also Pilon v. DOJ*, 73 F.3d 1111, 1119 (D.C. Cir. 1996) (finding disclosure can mean "unauthorized dissemination"). This is the government's own guidance. OMB, Privacy Act Implementation, 40 Fed. Reg. 28948, 28953 (July 9, 1975) ("A disclosure may be...the granting of access to a record."); *Cf.* 20 C.F.R. § 401.25 (defining "disclosure" in the Social Security Act).

The Complaint also makes clear that exception § 552a(b)(1) does not apply here for three independent reasons: (1) OPM disclosed Plaintiffs' records to "employees" of other agencies; (2) recipients are not using these records for a legitimate "duty"; and (3) recipients do not "need" these records to perform any legitimate duty.[9]

1. Some DOGE agents who obtained records are not "of the" OPM.

Exception (b)(1) applies only to intra-agency disclosures. OPM's disclosures to DOGE agents who are not employed by OPM do not qualify, and the Complaint alleges at least some of the DOGE agents were not OPM employees. *Supra* at 3. OPM gave Defendants Musk and DOGE—including several DOGE agents identified by name in the Complaint—"unrestricted, wholesale access to OPM systems and records." Compl. ¶¶ 8, 10 29, 36. Defendants themselves claim that E.O. 14,158 required OPM to give DOGE, a separate agency, "access to all" of OPM's sensitive data systems. MTD 2, 22; *see also* Compl. ¶ 5; E.O. § 4(b).

Contrary to Defendants' arguments, Plaintiffs alleged that the recipients of their data

[9] Regardless, Privacy Act exceptions are best resolved after discovery. *See Fleck v. Dep't of Veterans Affs.*, Civil Action No. 18-1452 (RDM), 2020 WL 42842, *6 (D.D.C. Jan. 3, 2020) (exemptions under 5 U.S.C. § 552a(j)). That is especially true here because the face of the Complaint does not allege Defendants have a legitimate need for the records. Plaintiffs allege the opposite. Compl. ¶¶ 10, 37, 49.

included non-OPM DOGE agents, some of whom have been installed at OPM under irregular and exceptionally opaque circumstances. *See* Compl. ¶¶ 5-6, 8-10, 24-27. The news reports cited in the Complaint are not to the contrary. They use a series of informal terms to describe DOGE, rather than referring to definitions of the EO. *Supra at 3 n.4.*

Even if some DOGE agents are also simultaneously employed by OPM, as Defendants suggest, MTD 20, these "dual employees could be impermissibly sharing the defendant agencies' records with officials outside of the agency." *AFL-CIO v. Dep't of Labor*, No. 1:25-cv-00339 (D.D.C.), ECF No. 71, at 11-12. Whether impermissible inter-agency disclosures occurred thus turns on the specific facts of "how this dual employment operates." *Id*.

At bottom, Defendants' contention that all DOGE agents are OPM employees, MTD 20-22, is a factual question that cannot be resolved on the pleadings, particularly given the unusually convoluted employment relationships of relevant individuals. Discovery is needed.

2. DOGE agents are not using the records for a legitimate "duty."

Exception (b)(1) applies only to record disclosures to agency employees who need them "in the performance of their duties." While DOGE's duties might include IT improvement, they cannot plausibly extend to DOGE-coordinated efforts to fire civil servants deemed "disloyal" to the President or based on their gender identity. Compl. ¶ 40. This is not a legitimate government "duty."

Likewise, DOGE agents have no legitimate "duty" in using OPM data for mass firings. Indeed, another court preliminarily enjoined DOGE from dismantling USAID given the likelihood of Appointments Clause and Separation of Powers violations. *Does 1-26 v. Musk*, Civil Action No. 25-0462-TDC, 2025 WL 840574, *32 (D. Md. Mar. 18, 2025).

3. DOGE agents do not "need" the records.

Regardless of their employment status, DOGE agents do not "need" the sensitive records

of millions of people in OPM's databases to perform their duties. *Cf.* MTD, 22-23. The term "need" means "to have an urgent or essential use" for something, *Need*, Black's Law Dictionary (5th ed. 1979), or a "clear and approved reason for requiring access." *Need-to-Know Basis*, Black's Law Dictionary (12th ed. 2024). DOGE's stated duties are to modernize government IT, and OPM is tasked to help create a plan to address hiring practices. *See* E.O. 14,158 or E.O. 14,170. Records that are being disclosed but that are unnecessary—or not needed—to accomplish DOGE's purposes include employees' race, disability, medical condition, or union activity, as well as all data on former employees or rejected job applicants. Compl. ¶ 2.

Remarkably, Defendants assert that DOGE agents need "*all* unclassified agency records, software systems, and IT systems" because the President said so. MTD 22 (quoting E.O.) (emphasis added). This proves too much. The E.O. on which Defendants rely does not go as far as they suggest (MTD 22-23): it requires agency heads to make information available to DOGE only as "consistent with law." E.O. § 4(b). The Privacy Act is a "law" that imposes a "need" requirement on intra-agency disclosure, so the E.O. does not purport to limit this rule. § 552a(b)(1). In the words of Privacy Act co-sponsor Sen. Percy, the Act is meant to prevent "the day when a bureaucrat in Washington … can use his organization's computer facilities to assemble a complete dossier of all known information about an individual." 120 Cong. Rec. 36,917 (Nov. 21, 1974).

As other courts have ruled, DOGE agents do not need "unprecedented, unfettered access" to entire agency records systems to "accomplish the goals of modernizing technology, maximizing efficiency and productivity, and detecting fraud, waste, and abuse," and thus the "need" exception to the Privacy Act does not apply. *AFSCME*, 2025 WL 868953, *63-64 (describing DOGE's similar access to SSA systems).

B. Plaintiffs State a Claim for Violation of 5 U.S.C. § 552a(e)(10).

Plaintiffs adequately allege that OPM and DOGE failed to "establish appropriate administrative, technical, and physical safeguards" to "insure the security and confidentiality of records" and "protect against any anticipated threats or hazards." § 552a(e)(10). This security provision is a simple, nondiscretionary mandate[10] that OPM should know from litigation arising from its previous security breach. It requires agencies to "take basic, known, and available steps" to protect personal records. *In re OPM Breach Litig.*, 928 F.3d at 63 (finding eight specific safeguards like training, logging, and oversight that OPM previously neglected). *See also In re VA Data Theft Ltgn.*, Misc. No. 06-0506 (JR), 2007 WL 7621261, *5 (D.D.C. Nov. 16, 2007).

To state a claim under § 552a(e)(10), Plaintiffs must identify a safeguard that the agencies "should have established but did not." *Conyers v. U.S. Dep't of Veterans Affs.*, 16-CV-0013 (JFB) (SIL), 2018 WL 1089736, at *4 (E.D.N.Y. Feb. 26, 2018). Plaintiffs have easily done so here.

Plaintiffs allege the following basic security failings at OPM and DOGE that violate the statute: OPM gave DOGE Defendants "administrative" access to all personnel systems at OPM on the day they were hired or earlier (Compl. ¶¶ 7, 9, 29); neither OPM nor DOGE properly conducted security vetting before allowing officials to access OPM's systems (¶ 8, 33); neither OPM nor DOGE provided officials with proper training before officials gained access to OPM's systems (¶ 58); and DOGE Defendants do not maintain public security policies that prohibit the above actions. ¶ 58.

[10] *NSS, Inc. v. Iola*, 700 F.3d 65 (3d Cir. 2012), cited by Defendants, MTD 16, is irrelevant to this issue, since it was an ERISA case construing the term "appropriate" to expand judicial "discretion" to issue equitable relief. *Id.* at 101. Similarly, *Doe v. OPM*, Civil Action No. 25-234 (RDM), 2025 WL 513268 (D.D.C. Feb. 17, 2025), did not address Section (e)(10) or the Privacy Act at all. Defendants' implication that (e)(10) is so broad that "there is no law to apply," *Chrysler Corp. v. Brown*, 441 U.S. 281, 317 (1979), does not square with multiple court decisions enforcing that provision.

These security failings have harmed Plaintiffs by: allowing Plaintiffs' personal records to be disclosed to government officials with no lawful or legitimate need for such access (¶¶ 2, 10); creating risk that these illegally disclosed records could be used to fire purportedly "disloyal" employees (¶ 40); and making the systems that store Plaintiffs' records more vulnerable to new cyber intrusions, especially in light of OPM's past security problems. ¶ 32, 41, 42.

III. INJUNCTIVE RELIEF IS AN APPROPRIATE REMEDY

The Privacy Act itself allows for injunctive relief to stop Defendants' ongoing harm.[11] If not, the Administrative Procedures Act allows such relief. Defendants' attempt to deny both remedies would render this Court "powerless to prevent an agency from systematically running roughshod over the rights the Act was promulgated to protect." *Doe v. Herman*, Civ. No. 97-0043-B, 1998 WL 34194937, *6 (W.D. Va. Mar. 18, 1998).

A. The Privacy Act Allows Injunctive Relief.

Under the text of the Privacy Act, the Court has jurisdiction to provide the injunctive relief that Plaintiffs seek. Plaintiffs "may bring a civil action against the agency, and the district courts of the United States shall have jurisdiction in the matters," when an agency illegally discloses records or fails to maintain security of them. 5 U.S.C. § 552a(g)(1)(D). While there are additional hurdles to obtain money damages, § 552a(g)(4), that does not foreclose injunctive relief.

Courts have allowed plaintiffs to seek injunctive relief under the Privacy Act itself, even when that relief is separate from correction or access to records. *See Haase v. Sessions*, 893 F.2d 370, 374 n.6 (D.C. Cir. 1990) (expungement of records for violation of § 552a(e)(7)); *Wabun-Inini v. Sessions*, 900 F.2d 1234, 1245 (8th Cir. 1990) (same). *See also Doe v. DiGenova*, 779 F.2d 74,

[11] Plaintiffs are seeking only injunctive and declaratory relief. *See* Compl. at 1, 18 ("Complaint for Declaratory and Injunctive Relief" and "Prayer for Relief"). Plaintiffs are not seeking monetary damages.

79 n.8 (D.C. Cir. 1985) (invalidating regulations allowing for records disclosure to the extent inconsistent with Privacy Act).[12]

Given the Privacy Act's text, structure, and purpose, the Court has the "historic power of equity to provide complete relief in light of the statutory purposes." *Mitchell v. Robert DeMario Jewelry*, 361 U.S. 288, 291-92 (1960). *See also Porter v. Warner Holding Co.*, 328 U.S. 395, 398 (1946) ("Unless otherwise provided by statute, all the inherent equitable powers of the District Court are available for the proper and complete exercise of that jurisdiction."); *Haase*, 893 F.2d at 374 n.6.

Here, Plaintiffs allege their records are being illegally disclosed and recklessly secured. The Privacy Act grants individuals and the Court jurisdiction for "any other" violation under § 552a(g)(1)(D), and it does not prohibit injunctive relief "by a necessary and inescapable inference" under these circumstances. *Porter*, 328 U.S. 395 at 398; *Mitchell*, 361 U.S. at 291. Congress passes laws "cognizant" of the courts' power to grant complete relief. *Mitchell*, 361 U.S. at 292. Rather than prohibiting injunctive relief, the Privacy Act merely specifies when certain forms of limited and uncommon equitable relief are appropriate—correction and access to records under 552a(g)(2)-(3)—and when money damages are appropriate under the heightened standard of 552a(g)(4).

Moreover, a specific purpose of the Privacy Act is to "permit an individual to prevent" unlawful records disclosure. PL 93–579, § 2(A)(5)(B)(2). This purpose can be accomplished only

[12] Defendants cite other out-of-circuit cases that say the opposite. *See Sussman v. U.S. Marshal Serv.*, 494 F.3d 1106, 1122 (D.C. Cir. 2007)*; Parks v. IRS*, 618 F.2d 677, 684 (10th Cir. 1980); *Cell Assocs. v. NIH*, 579 F.2d 1155, 1160 (9th Cir. 1978). But as to when injunctive relief is allowed under the Privacy Act, a "split of authority exists." *Herman*, 1998 WL 34194937, *3. *See also Sussman*, 494 F.3d at 1122 n.10 (noting the inconsistency within the DC Circuit). The Second Circuit has not decided the issue.

by allowing plaintiffs to seek an injunction to prevent the ongoing privacy violations they allege. Plaintiffs should not be forced to continue to suffer ongoing harm and wait patiently until those violations have ceased, at which point they can possibly seek money damages. *Cf. Mitchell*, 361 U.S. at 293 ("We cannot read the Act as presenting those it sought to protect with what is little more than a Hobson's choice.").

The Court should not follow the non-controlling decisions cited by Defendants because those decisions ignore the Privacy Act's purpose written into the law and rely too heavily on the purported intent of Congress. *Compare* PL 93–579, § 2(A)(5)(B)(2) (defining "the purpose of this act" as empowering individuals to "prevent" unlawful disclosure), *with Parks*, 618 F.2d at 684 ("Moreover, the legislative history evidences an intent to preclude the availability of injunctive relief in all cases."), *and Cell Assocs.*, 579 F.2d at 1160. Given the Privacy Act's purpose written into the law, this Court should "presume that the statute says what it means." *Devine*, 202 F.3d at 551.

B. If the Privacy Act Does Not Allow Injunctive Relief, the APA Does.

Even if the Court does not locate the power to grant injunctive relief in the text of the Privacy Act itself, the Administrative Procedures Act ("APA") provides such relief.

The Supreme Court has looked favorably on Privacy Act lawsuits for injunctive relief when brought under the APA. *FAA v. Cooper*, 566 U.S. 284, 303 n.12 (2012) (Privacy Act violations can be remedied "possibly by allowing for injunctive relief under" the APA)[13]; *Doe v. Chao*, 540 U.S. 614, 619 n.1 (2004) (Privacy Act does not specify standards for injunctive relief because of "the general provisions for equitable relief within" the APA).

Numerous courts have granted injunctive relief under the APA for violations of the Privacy

[13] Defendants cite *FAA v. Cooper* without addressing its footnote 12. MTD 24.

Act. *Doe v. Chao*, 435 F.3d 492, 505 n.17 (4th Cir. 2006) (granting APA injunctive relief for illegal disclosure of social security number)[14]; *Doe v. Stephens*, 851 F.2d 1457, 1466 (D.C. Cir. 1988) (granting APA declaratory relief for illegal disclosure of psychiatric records); *Herman*, 1998 WL 34194937, *2 (granting stipulated APA injunctive relief for illegal disclosure of social security numbers). This is consistent with decisions from related cases in the past month, where plaintiffs brought only APA claims. *AFT*, 2025 WL 582063, *8 (OPM systems). *Trump*, 2025 WL 573771, *23 (Treasury systems); *AFSCME*, 2025 WL 868953, *53 (Social Security Administration systems).

Defendants cannot have it both ways: either the Privacy Act provides for the injunctive remedy Plaintiffs seek, or the APA provides that remedy because it is not duplicative. All the cases Defendants cite, in fact, support this position. (MTD 18-19); *see Chao*, 435 F.3d at 504 n.17 (allowing injunctive relief through APA but denying Privacy Act remedy); *Westcott v. McHugh*, 39 F. Supp. 3d 21, 33 (D.D.C. 2014) (allowing Privacy Act claim to go forward, but denying APA claim); *Tripp v. Dep't of Def.*, 193 F. Supp. 2d 229, 238 (D.D.C. 2002) (same); *Mittleman v. U.S. Treasury*, 773 F. Supp. 442 (D.D.C. 1991) (denying APA claim because the "relief" that plaintiff sought is available under the Privacy Act).

Defendants are attempting "neat legal maneuvers" to deny plaintiffs any remedy to stop the ongoing harm. *Herman*, 1998 WL 34194937, *6. But the Court has authority to enjoin Defendants from "running roughshod over" Plaintiffs' rights. *Id*.

IV. PLAINTIFFS ADEQUATELY ALLEGE AN APA VIOLATION

Defendants' violations of the Privacy Act constitute final agency actions that are subject to review under the APA. OPM's decision to disclose Plaintiffs' records and OPM's and DOGE's

[14] Defendants likewise cite *Doe v. Chao* without addressing its footnote 17. MTD 25.

reckless security policies constitute the consummation of decisionmaking by the Defendant agencies, and significant legal consequences flow from each of those policies. These decisions are therefore final agency action subject to review under the APA. Specifically, Defendants' adoption of a new policy of information disclosure—or change of an existing one—is indisputably final agency action.

Under the APA, courts can set aside agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706. "Agency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court are subject to judicial review." 5 U.S.C. § 704.[15] An agency action is final if it (1) "mark[s] the consummation of the agency's decisionmaking process" and (2) is an action "by which rights or obligations have been determined, or from which legal consequences will flow." *Bennett v. Spear*, 520 U.S. 154, 177-78 (1997); *see also Biden v. Texas*, 597 U.S. 785, 808 (2022). Notably, courts take a "pragmatic approach" to finality. *U.S. Army Corps of Engineers v. Hawkes Co.*, 578 U.S. 590, 599 (2016).

Defendants changed their agencies' security policies or adopted wholly new policies allowing DOGE agents to obtain Plaintiffs' records held by OPM. These unlawful records disclosures and reckless security policies violated the Privacy Act, *supra* section II, constituting action that is both "arbitrary and capricious" and "not in accordance with law." 5 U.S.C. § 706(2)(A).

The deprivation of Plaintiffs' privacy rights through disclosure and security failures is an

[15] If the Court does not locate the power to grant injunctive relief in the text of the Privacy Act itself, Plaintiffs have no other "adequate remedy." 5 U.S.C. § 704; *supra* section III(B). Moreover, monetary relief for past harm is not an adequate substitute for prospective relief for ongoing harm. *Cf. Bowen v. Massachusetts*, 487 U.S. 879, 905 (1988).

action "by which rights or obligations have been determined," and is thus a final agency action. *Chrysler Corp.*, 441 U.S. at 318–19 (a decision by an agency to "disclose" a plaintiff's records is a "reviewable agency action" that the Court can enjoin); *Venetian Casino Resort, L.L.C. v. EEOC*, 530 F.3d 925, 930–31 (D.C. Cir. 2008) (holding that the EEOC's decision to release without notice confidential documents the employer provided during EEOC investigations was a final agency action subject to judicial review). Defendants here implemented "a policy of permitting … disclos[ure]," *Venetian*, 530 F.3d at 931, by incorrectly determining that OPM does not need Plaintiffs' written authorization to disclose their records to DOGE agents and that DOGE agents have a legitimate need for those records.

OPM's decision to disclose records to DOGE and both agencies' decision to implement inadequate security, which led to that disclosure, was neither tentative nor interlocutory in nature. It was "the consummation of the agency's decisionmaking process." *Bennett*, 520 U.S. at 177–78. There was nothing further for the agency to do to formalize the decisions. No written decision was required to finalize the actions. *Bhd. of Locomotive Eng'rs & Trainmen v. Fed. R.R. Admin.*, 972 F.3d 83, 100 (D.C. Cir. 2020) ("[T]he absence of a written memorialization by the agency does not defeat finality. … Agency action generally need not be committed to writing to be final and judicially reviewable.") (citing *Venetian*, 530 F.3d at 930–31); *Amadei v. Nielsen*, 348 F. Supp. 3d 145, 165 (E.D.N.Y. 2018) (noting "plaintiff can satisfy the finality requirement without offering evidence of a formal or official statement regarding the agency's position").[16] Nor does OPM's authority to revoke or restrict the access render their decisions tentative. OPM decided that DOGE

[16] Indeed, a "contrary rule would allow an agency to shield its decisions from judicial review simply by refusing to put those decisions in writing.'" *R.I.L-R v. Johnson*, 80 F. Supp. 3d 164, 184 (D.D.C. 2015). Moreover, at the motion to dismiss stage, courts must draw inferences that support the existence of an official policy. *Amadei*, 348 F. Supp. 3d at 165.

agents could access their record systems, and DOGE agents did so. These actions marked the consummation of the decision-making process.

V. PLAINTIFFS ADEQUATELY ALLEGE *ULTRA VIRES* ACTION

Finally, Plaintiffs sufficiently allege *ultra vires* actions by DOGE Defendants. An *ultra vires* claim is a non-statutory claim for judicial review of lawless government actions. Consequently, "[c]ourts have long recognized that an aggrieved party can sue in federal court to challenge agency action as *ultra vires*, even when a statute does not specifically delineate that right." *Ctr. for Biological Diversity v. McAleenan*, 404 F. Supp. 3d 218, 235–36 (D.D.C. 2019). "Our system of jurisprudence rests on the assumption that all individuals, whatever their position in government, are subject to federal law…. All the officers of the government from the highest to the lowest, are creatures of the law, and are bound to obey it." *Butz v. Economou*, 438 U.S. 478, 506 (1978). *Ultra vires* review serves to avoid leaving "the individual … to the absolutely uncontrolled and arbitrary action of a public and administrative officer, whose action is unauthorized by any law." *Am. Sch. of Magnetic Healing v. McAnnulty*, 187 U.S. 94, 110 (1902).[17]

A governmental official or entity's action is *ultra vires* where it "plainly" exceeds its lawful authority and is "contrary to a specific prohibition in the statute that is clear and mandatory." *Yale New Haven Hosp. v. Becerra*, 56 F.4th 9, 26–27 (2d Cir. 2022). "When an executive acts *ultra vires*, courts are normally available to reestablish the limits on his authority." *Open Society Justice Initiative v. Trump*, 510 F. Supp. 3d 198, 214 (S.D.N.Y. 2021); *see also Make the Road New York v. Pompeo*, 475 F. Supp. 3d 232, 267 (S.D.N.Y. 2020) (finding that plaintiff not only sufficiently

[17] *Ultra vires* claims were recognized by the Supreme Court in *McAnnulty* before the passage of the APA, and "[n]othing in the subsequent enactment of the APA altered the *McAnnulty* doctrine of review." *Chamber of Com. of U.S. v. Reich*, 74 F.3d 1322, 1327–28 (D.C. Cir. 1996). *See also* 5 U.S.C. § 559 ("This subchapter ... do[es] not limit or repeal additional requirements imposed by statute or otherwise recognized by law.").

alleged, but was likely to prevail on, claim that Presidential proclamation was *ultra vires*). Because Congress has not expressly withdrawn courts' jurisdiction to review the DOGE Defendants' lawless behavior, and because their actions are "plainly beyond the bounds" or "clearly in defiance" of any authority DOGE Defendants possess, Plaintiffs have adequately pleaded their *ultra vires* claim. *See Fed. Express Corp. v. U.S. Dep't of Com.*, 39 F.4th 756, 764 (D.C. Cir. 2022).

In directing and controlling the use and administration of Defendant OPM's systems, DOGE Defendants have breached secure government systems and caused the unlawful disclosure of the personal data of tens of millions of Americans, despite having no lawful authority to access these systems. Compl. ¶¶ 77-79, 81-82; *supra* Part II. Through such conduct, DOGE Defendants have engaged and continue to engage in *ultra vires* actions that violate federal law, exceed their authority, and injure Plaintiffs and their members by exposing their private information and increasing the risk of further disclosure of their information. *Id.*

Defendants contend that Plaintiffs' *ultra vires* claim "is coextensive with [Defendants'] alleged violations of the Privacy Act." MTD at 24. But if the Court does not locate the power to grant injunctive relief in the Privacy Act, or Plaintiffs' alternative claims are otherwise unavailable, the Court has authority to restrain DOGE's *ultra vires* actions to induce illegal disclosures of records and failure to secure those records. *See Nat'l Ass'n of Letter Carriers*, 604 F. Supp. 2d at 673 (entertaining claim for injunction for *ultra vires* conduct for Privacy Act violations). The actions of the DOGE Defendants are *ultra vires* because DOGE agents had no authority to access and collect OPM data, and the Executive Orders do not create such authority.[18] *See supra*, section

[18] An executive order cannot grant statutory or constitutional authority. "Fundamentally, administrative agencies are creatures of statute, and accordingly possess only the authority that

II(A). Even if some DOGE agents were made employees of OPM, the DOGE Defendants never had a need for the information to perform their lawful duties. *Id.*

CONCLUSION

For the foregoing reasons, Plaintiffs respectfully request that the Court deny Defendants' motion to dismiss. If, however, the Court grants the motion, Plaintiffs respectfully request leave to amend.

Dated: March 24, 2025

Respectfully submitted,

/s/ F. Mario Trujillo

F. Mario Trujillo (admitted pro hac vice)
Victoria Noble
ELECTRONIC FRONTIER FOUNDATION
815 Eddy Street
San Francisco, CA 94109
(415) 436-9333

Rhett O. Millsaps II
Mark A. Lemley (admitted pro hac vice)
Mark P. McKenna (admitted pro hac vice)
Christopher J. Sprigman
LEX LUMINA LLP
745 Fifth Avenue, Suite 500
New York, NY 10151
(646) 898-2055

Norman L. Eisen (admitted pro hac vice)
STATE DEMOCRACY DEFENDERS FUND
600 Pennsylvania Avenue SE #15180
Washington, DC 20003

Subodh Chandra (admitted pro hac vice)
THE CHANDRA LAW FIRM LLC
The Chandra Law Building

Congress has provided." *PFLAG, Inc. v. Trump*, Civil No. 25-337-BAH, 2025 WL 685124, *16 (D. Md. Mar. 4, 2025). "'[A]n agency literally has no power to act ... unless and until Congress confers power upon it.'" *New York v. Trump*, C.A. No. 25-cv-39-JJM-PAS, 2025 WL 357368, *2 (D.R.I. Jan. 31, 2025) (*quoting La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986)). "Any action that an agency takes outside the bounds of its statutory authority is ultra vires." *City of Providence v. Barr*, 954 F.3d 23, 31 (1st Cir. 2020)).

1265 W. 6th Street, Suite 400
Cleveland, OH 44113

Counsel for Plaintiffs

CERTIFICATE OF COMPLIANCE

I certify that, excluding the caption, table of contents, table of authorities, signature block, and this certification, the foregoing Plaintiffs' Opposition to Defendants' Motion to Dismiss contains 8,732 words, calculated using Microsoft Word for Mac, which complies with Rule 7.1(c) of the Local Rules of the United States District Court for the Southern District of New York.

Dated: March 24, 2025 */s/ F. Mario Trujillo*