



For defendants:

Jeffrey Oestericher  
David E. Farber  
United States Attorney’s Office, Southern District of New York  
86 Chambers Street, 3rd Floor  
New York, NY 10007

**Table of Contents**

Background..... 3

Discussion..... 10

    I. Article III Standing..... 12

        A. Injury in Fact ..... 13

        B. Causation and Redressability ..... 25

    II. Privacy Act Claims ..... 27

        A. Violations ..... 28

            1. Illegal Disclosure ..... 28

            2. Lack of Appropriate Safeguards ..... 41

        B. Injunctive Relief ..... 42

    III. APA Claims ..... 43

        A. Final Agency Action ..... 45

        B. Inadequacy of Alternative Remedies ..... 50

    IV. Ultra Vires Claim..... 53

Conclusion..... 56

DENISE COTE, District Judge:

On February 11, 2025, current and former federal government employees and their unions sued the U.S. Office of Personnel Management (“OPM”) and other defendants for breaches of privacy. The plaintiffs allege that data contained in OPM databases was improperly disclosed to individuals associated with the United States DOGE Service (“USDS”). The defendants have moved to

dismiss the complaint. For the following reasons, that motion is granted in part.

### **Background**

The following allegations, which appear in the complaint and documents integral to it, are accepted as true for purposes of this motion. All reasonable inferences are drawn in the plaintiffs' favor. See Clark v. Hanley, 89 F.4th 78, 90-91 (2d Cir. 2023).

On January 20, 2025, the day of his inauguration, President Trump signed Executive Order 14,158 (the "DOGE Executive Order"). The DOGE Executive Order established the "Department of Government Efficiency" to implement the President's "DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity." It renamed the United States Digital Service as the United States DOGE Service and moved it from the Office of Management and Budget ("OMB") to the Executive Office of the President. It also established within USDS the U.S. DOGE Service Temporary Organization ("Temporary Organization"), which it stated shall "terminate" on July 4, 2026.

The DOGE Executive Order instructed each executive agency to establish a "DOGE Team" in consultation with USDS. Each DOGE Team is to consist of at least four employees, who may include

Special Government Employees hired or assigned within thirty days of the DOGE Executive Order. Each DOGE Team should “typically include one DOGE Team Lead, one engineer, one human resources specialist, and one attorney.”

The DOGE Executive Order also instructed the USDS Administrator to commence “a Software Modernization Initiative,” and instructed Agency Heads to ensure, “to the maximum extent consistent with law,” that USDS has “full and prompt access to all unclassified agency records, software systems, and IT systems.” USDS was instructed to “adhere to rigorous data protection standards.” The DOGE Executive Order stated that it “shall be implemented consistent with applicable law” and should not “be construed to impair or otherwise affect . . . the authority granted by law to an executive department or agency.”

The plaintiffs are individuals currently or formerly employed by the federal government and unions representing federal government employees. The three named individual plaintiffs are a current federal employee working for the Brooklyn Veterans Affairs Medical Center and two former federal employees. The two union plaintiffs are American Federation of Government Employees, AFL-CIO (“AFGE”) and Association of Administrative Law Judges, International Federation of

Professional and Technical Engineers Judicial Council 1, AFL-CIO ("AALJ").

The plaintiffs have sued two sets of defendants. They are the "OPM Defendants," which consist of OPM and its Acting Director Charles Ezell; and the "DOGE Defendants," which consist of USDS, its Acting Director, the Temporary Organization, and Elon Musk.

The complaint alleges that, on January 20, 2025, the OPM Defendants gave at least six DOGE agents immediate access to all personnel systems at OPM. OPM maintains personal and employment information of tens of millions of current and former federal employees, contractors, and job applicants. Those records include identifying information such as names, birthdates, social security numbers, demographic information, education and employment histories, personal health records, financial information, and information concerning family members and other third parties.

A week later, the OPM Defendants gave more DOGE agents access to OPM systems. The complaint asserts that this disclosure of information to the DOGE Defendants was deliberate and willful. The names of systems disclosed to the DOGE Defendants include Enterprise Human Resources Integration ("EHRI"), Electronic Official Personnel Folder, USAJOBS, USA

Staffing, USA Performance, and Health Insurance. The complaint also alleges that DOGE agents were given "administrative" access to the OPM computer systems, which provided them with the ability to modify software and data, including the ability to alter documentation of their own activity.

The complaint also describes irregularities in the process by which the DOGE agents were given access to OPM's systems. At the time they were given access they had not been properly vetted, had not received customary security clearances, and had not received OPM's security training. The complaint alleges that at least one of the DOGE agents had previously been fired from private employment in connection with an investigation of the disclosure of his employer's secrets. Moreover, in violation of the Privacy Act, the DOGE Defendants were given access to OPM data without obtaining the consent of affected individuals and with no lawful need for access to the records disclosed to them.

The complaint describes harms that the plaintiffs fear they may suffer from the disclosure of OPM records to the DOGE agents. These include an increased vulnerability of their personal data to cyberattacks, hacking, and identity theft. Disclosure of their identifying information could be detrimental to their health, safety, and financial security. The complaint

also points to the possibility of retaliatory firing by the Trump administration. The complaint explains that an OPM data breach disclosed in 2015 affected over 22 million people and led to identity theft and fraud.

The complaint, filed on February 11, 2025, brings five claims for relief. Two are brought under the Privacy Act of 1974, 5 U.S.C. § 552a ("Privacy Act"); two are brought under the Administrative Procedure Act, 5 U.S.C. § 701 et seq. ("APA"); and the final claim is an ultra vires claim. The plaintiffs seek declaratory and injunctive relief; they do not seek damages. The plaintiffs ask for a declaration that the OPM Defendants' decision to implement a system by which the DOGE Defendants have access to OPM's records and the plaintiffs' personal information contained in those records is unlawful. They seek to enjoin the defendants from continuing to permit such access or using any illegally obtained information, and they seek the impoundment and destruction of any copies of personal information that has been unlawfully disclosed.

The plaintiffs brought a motion for a temporary restraining order ("TRO") on February 14. They sought a TRO that would prohibit, among other things, the disclosure of protected OPM records to DOGE agents. On February 19, the defendants filed an opposition to the motion for a TRO, which was accompanied by a

declaration from Greg Hogan, OPM's Chief Information Officer. In their opposition, the defendants requested that the motion for a TRO be converted into a motion for a preliminary injunction. Instead of filing a reply, the plaintiffs joined that request on February 23 and indicated that they would seek expedited discovery.

Meanwhile, orders had been issued against the federal government in other DOGE-related litigation, including in an action proceeding in the District of Maryland against OPM, the Department of the Treasury ("Treasury"), and the Department of Education ("DOE") for violations of the Privacy Act and the APA.<sup>1</sup> There, on February 24, the court issued a TRO enjoining OPM from disclosing personally identifiable information ("PII") "to any OPM employee working principally on the DOGE agenda who has been granted access to OPM records for the principal purpose of implementing the DOGE agenda," with the exception of Hogan. Am. Fed'n of Teachers v. Bessent ("Maryland OPM Action"), No. 25cv430, 2025 WL 582063, at \*15 (D. Md. Feb. 24, 2025). On February 26, OPM was ordered to produce an administrative record. Id., ECF No. 46. On March 24, the TRO was converted to

---

<sup>1</sup> In another action brought against OPM and Treasury in the Eastern District of Virginia under the Privacy Act and the APA, a TRO was denied on February 21. Elec. Priv. Info. Ctr. v. OPM ("Virginia OPM Action"), No. 25cv255, 2025 WL 580596 (E.D. Va. Feb. 21, 2025).



a preliminary injunction enjoining OPM from disclosing PII “to any DOGE affiliates, defined as individuals whose principal role is to implement the DOGE agenda as described in Executive Order 14,158 and who were granted access to agency systems of records for the principal purpose of implementing that agenda,” with Hogan, Acting Director Ezell, and Chief of Staff Amanda Scales being exempted. Id., 2025 WL 910054 (order); see also id., 2025 WL 895326 (opinion).<sup>2</sup>

The plaintiffs in the instant action filed a motion for expedited discovery on February 27, which became fully submitted on March 6. An Order of March 7 instructed the defendants to provide the administrative record and other relevant materials to be produced in the Maryland OPM Action to the plaintiffs in this action, and otherwise denied the motion for expedited discovery without prejudice to its renewal.

---

<sup>2</sup> Actions brought under the Privacy Act and the APA, but that do not name OPM as a defendant, have granted preliminary relief limiting access to records by individuals affiliated with DOGE: New York v. Trump, No. 25cv1144, 2025 WL 573771 (S.D.N.Y. Feb. 21, 2025) (Treasury); Am. Fed’n of State, Cnty., & Mun. Emps. v. SSA (“Maryland SSA Action”), No. 25cv596, 2025 WL 868953 (D. Md. Mar. 20, 2025) (Social Security Administration (“SSA”)). The following such actions have denied preliminary relief: Am. Fed’n of Lab. v. Dep’t of Lab., No. 25cv339, 2025 WL 542825 (D.D.C. Feb. 14, 2025) (Department of Labor, Department of Health and Human Services, and Consumer Financial Protection Bureau); Univ. of Cal. Student Ass’n v. Carter, No. 25cv354, 2025 WL 542586 (D.D.C. Feb. 17, 2025) (DOE); All. for Ret. Ams. v. Bessent, No. 25cv313, 2025 WL 740401 (D.D.C. Mar. 7, 2025) (Treasury).

On a schedule to which the parties had agreed, and which was adopted by the Court, the defendants moved to dismiss the complaint on March 14. That motion became fully submitted on March 31.

### **Discussion**

The defendants have moved to dismiss the complaint pursuant to Rules 12(b)(1) and 12(b)(6), Fed. R. Civ. P. In support of their Rule 12(b)(1) motion to dismiss, they argue that there is no subject matter jurisdiction because the plaintiffs lack Article III standing to bring their claims. At the pleading stage, "general factual allegations of injury resulting from the defendant's conduct may suffice" to establish Article III standing, "for on a motion to dismiss we presume that general allegations embrace those specific facts that are necessary to support the claim." Cerame v. Slack, 123 F.4th 72, 81-82 (2d Cir. 2024) (citation omitted).

The defendants argue as well that each of the claims in the complaint must be dismissed pursuant to Rule 12(b)(6) for failure to state a claim. A complaint is required to provide "a short and plain statement of the claim showing that the pleader is entitled to relief," Fed. R. Civ. P. 8(a)(2), and "the statement need only give the defendant fair notice of what the claim is and the grounds upon which it rests." McCray v. Lee,

963 F.3d 110, 116 (2d Cir. 2020) (citation omitted). To survive a Rule 12(b)(6) motion to dismiss, a complaint must “state a claim to relief that is plausible on its face.” Doe v. Franklin Square Union Free Sch. Dist., 100 F.4th 86, 94 (2d Cir. 2024) (quoting Ashcroft v. Iqbal, 556 U.S. 662, 678 (2009)). “A claim has facial plausibility when the plaintiff pleads factual content that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged.” Vengalattore v. Cornell Univ., 36 F.4th 87, 102 (2d Cir. 2022) (quoting Iqbal, 556 U.S. at 678). In determining if a claim is plausible, a court must “accept as true all allegations in the complaint and draw all reasonable inferences in favor of the non-moving party,” although “threadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice.” Doe, 100 F.4th at 94 (citation omitted). A court may also consider “documents appended to the complaint or incorporated in the complaint by reference” and “matters of which judicial notice may be taken.” Clark, 89 F.4th at 93 (citation omitted).

“Because standing is jurisdictional under Article III, it is a threshold issue that must be addressed before merits questions such as [] plausibility.” Moreira v. Societe Generale, S.A., 125 F.4th 371, 384 (2d Cir. 2025) (citation

omitted). Following a discussion of the plaintiffs' standing to bring their claims, the arguments for dismissal of the Privacy Act, APA, and ultra vires claims will each be addressed.

#### I. Article III Standing

The defendants argue that the complaint does not allege facts sufficient to confer standing. A plaintiff must establish standing to bring each claim in the complaint. TransUnion LLC v. Ramirez, 594 U.S. 413, 431 (2021).

Article III of the U.S. Constitution requires a plaintiff to have "a personal stake in the case -- in other words, standing." Id. at 423 (citation omitted). A plaintiff must show "(1) an injury in fact, defined as an invasion of a legally protected interest that is concrete, particularized, and actual or imminent; (2) a sufficient causal connection between the injury and the conduct complained of; and (3) a likelihood that the injury will be redressed by a favorable decision." Citizens United to Protect Our Neighborhoods v. Village of Chestnut Ridge, 98 F.4th 386, 391 (2d Cir. 2024) (citing Lujan v. Defs. of Wildlife, 504 U.S. 555, 560-61 (1992)).

Although a union may assert its standing to bring claims either in its own right or as a representative of its members, here the plaintiff unions seek only to assert their members' injuries. See id. at 395. Consequently, under the doctrine of

associational standing, the plaintiff unions must demonstrate that their members would have standing to sue in their own right. Id.

The allegations in the complaint suffice to establish the plaintiffs' standing to bring each of their claims. The defendants do not contend that the plaintiffs' ability to establish standing differs from claim to claim.

A. Injury in Fact

An injury in fact, which is the first element in the standing inquiry, must be concrete, such that it is "real and not abstract." FDA v. All. for Hippocratic Med., 602 U.S. 367, 381 (2024). It must also be particularized, meaning that it must affect the plaintiff "in a personal and individual way and not be a generalized grievance." Id. (citation omitted). Moreover, the injury "must be actual or imminent, not speculative -- meaning that the injury must have already occurred or be likely to occur soon." Id. "Although imminence is concededly a somewhat elastic concept, it cannot be stretched beyond its purpose, which is to ensure that the alleged injury is not too speculative for Article III purposes -- that the injury is certainly impending." Clapper v. Amnesty Int'l USA, 568 U.S. 398, 409 (2013) (citation omitted).

An injury in fact may be tangible or intangible. TransUnion, 594 U.S. at 425. As examples, it may be physical, monetary, an injury to property, or an injury to rights. FDA, 602 U.S. at 381. To assess whether a harm is a concrete injury in fact for purposes of Article III standing, “courts should assess whether the alleged injury to the plaintiff has a ‘close relationship’ to a harm ‘traditionally’ recognized as providing a basis for a lawsuit in American courts.” TransUnion, 594 U.S. at 424 (quoting Spokeo, Inc. v. Robins, 578 U.S. 330, 341 (2016)). While the asserted injury must have “a close historical or common-law analogue,” the analogue need not be an “exact duplicate in American history and tradition,” id., and a plaintiff need not “plead every element of a common-law analog to satisfy the concreteness requirement.” Salazar v. Nat’l Basketball Ass’n, 118 F.4th 533, 542 n.6 (2d Cir. 2024).

Concrete, intangible harms “include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion.” TransUnion, 594 U.S. at 425. Traditional, concrete intangible injuries include as well “harms specified by the Constitution.” Id. In addition, when identifying concrete, intangible harms, “Congress’s views may be instructive.” Id. (citation omitted). “Courts must afford due respect to Congress’s decision to impose a statutory prohibition

or obligation on a defendant, and to grant a plaintiff a cause of action to sue over the defendant's violation of that statutory prohibition or obligation." Id. Even where a statute grants a person a statutory right to sue, however, courts must independently assess whether the plaintiff has shown a concrete injury because of a defendant's violation of law. Id. at 426.

The plaintiffs rely on three theories of intangible injury to support their pleading of Article III standing. They are the tort of intrusion upon seclusion, the tort of disclosure of private information, and the right to privacy as reflected in the Fourth Amendment. The complaint adequately alleges that the individual plaintiffs and members of the plaintiff unions have experienced a concrete injury in fact that is analogous to the tort of intrusion on seclusion. It is unnecessary, as a result, to examine the other two sources of rights upon which they rely.

The Supreme Court has explained that harms analogous to those underlying the tort of intrusion upon seclusion may be concrete for purposes of Article III standing. Id. at 425; see also Gadelhak v. AT&T Servs., Inc., 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.) ("The common law has long recognized actions at law against defendants who invaded the private solitude of another by committing the tort of intrusion upon seclusion." (citation omitted)).

Intrusion upon seclusion is defined as follows:

One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.

Restatement (Second) of Torts § 625B (Am. L. Inst. 1977); see Melito v. Experian Marketing Sols., Inc., 923 F.3d 85, 93 (2d Cir. 2019) (citing § 652B in support of Article III standing analysis). The comments to this section of the Restatement explain that liability depends not “upon any publicity given to the person whose interest is invaded or to his affairs,” but rather on “[t]he intrusion itself.” Id. § 652B cmt. a, b. The tort covers intrusion upon private records but not “the examination of a public record concerning the plaintiff, or of documents that the plaintiff is required to keep and make available for public inspection.” Id. § 652B cmt. c. The interference with the plaintiff’s seclusion must be “substantial.” Id. § 652B cmt. d.

Citing these comments to the Restatement, the Second Circuit has emphasized that intrusion upon seclusion

is a tort that occurs through the act of interception itself. The intrusion itself makes the defendant subject to liability, even though there is no publication or other use of any kind of the information outlined. Nothing more is required after the interception is made for liability to attach based on this tort.



Caro v. Weintraub, 618 F.3d 94, 101 (2d Cir. 2010) (citation omitted). In Caro, the Second Circuit held that liability could arise from a defendant setting up a recording device, pressing "record," and doing nothing more -- that is, the "simple act of the recording itself" -- without listening, publishing, sharing, copying, or any other act that might harm the plaintiff, sufficed to establish intrusion upon seclusion. Id.

The complaint alleges concrete harms analogous to intrusion upon seclusion. The records at issue contain information about the deeply private affairs of the plaintiffs. The records include, for example, social security numbers, health history, financial disclosures, and information about family members. The complaint pleads that for some plaintiffs, disclosure of the simple fact that they are included in the records could compromise their highly sensitive government roles. The individual plaintiffs had every reason to expect that their OPM records would be carefully guarded and kept private and secure. That is in fact what the Privacy Act requires. The plaintiffs allege, however, that these records were disclosed to DOGE agents in a rushed and insecure manner that departed substantially from OPM's normal practices. The complaint alleges that the DOGE agents were not vetted, were not required to obtain security clearances, and were not trained about OPM

security protocols and duties before the records were disclosed to them. DOGE agents were even granted "administrative" access, enabling them to alter OPM records and obscure their own access to those records. As alleged, this intrusion upon the individual plaintiffs' private affairs and confidential information was a substantial invasion of their privacy and would be highly offensive to a reasonable person.

The defendants acknowledge that the plaintiffs can establish their standing through an injury analogous to those actionable under the common law tort of intrusion upon seclusion, and appear as well to acknowledge that the plaintiffs have a right to expect that OPM would keep their personal information private and secure. The defendants argue, however, that the complaint fails to describe an invasion of privacy sufficient to plead standing.

First, the defendants contend that the complaint pleads only that the DOGE agents were granted access to OPM's data systems and does not plead that the DOGE agents in fact used that access to examine OPM records. According to the defendants, the concrete injury required for standing will exist only if the DOGE agents examined or used the records to which OPM gave them access. This argument falls short for two reasons: first, the plaintiffs have adequately alleged that

their records were reviewed and used, and second, the law does not require that to have happened for the plaintiffs to have standing.

To begin with, the complaint plausibly pleads that the DOGE agents demanded immediate access to OPM records, were given that access, including "administrative" control, and entered six OPM systems. It asserts as well, on information and belief, that the DOGE agents continue "to possess and use" the plaintiffs' confidential information. One of the articles incorporated into the complaint reports that the OPM agents reviewed "position description level data" in OPM's EHRI system. The article adds that:

Outside actors have already gained access to some of the massive email lists that OPM created as part of Musk's effort to convince federal employees to resign. A new server being used to control these databases has been placed in a conference room that Musk's team is using as their command center . . . .

It explains that OPM civil servants have been blocked from accessing EHRI and other OPM systems, and that the DOGE team was given "read and write permissions" and "had moved sofa beds into the agency's headquarters to continue their work around the clock." Clearly, the complaint alleges more than a passive grant of access; it plausibly pleads that the DOGE agents actually exploited their access to review, possess, and use OPM records.

The defendants do not identify any cases that support their cramped view of the law.<sup>3</sup> Several courts have rejected it and found standing to exist when an unauthorized third party was granted access to a plaintiff's legally protected data, due to the resulting harm's resemblance to intrusion upon seclusion. E.g., Persinger v. Southwest Credit. Syst., L.P., 20 F.4th 1184, 1192 (7th Cir. 2021) (an "unauthorized inquiry" into credit information sufficient to confer standing); Nayab v. Cap. One Bank (USA), N.A., 942 F.3d 480, 491-92 (9th Cir. 2019) (same); Perry v. Cable News Network, 854 F.3d 1336, 1340-41 (11th Cir. 2017) (same).<sup>4</sup> The Second Circuit has held that "exposure of [the plaintiff's] personally identifiable information to unauthorized third parties," without further use or disclosure,

---

<sup>3</sup> The one opinion that the defendants cite concluded the alleged harm was not analogous to intrusion upon seclusion because the unauthorized access at issue did not concern the plaintiff's truly personal or intimate information and thus was not "substantial." Mills v. Saks.com LLC, No. 23cv10683, 2025 WL 34828, at \*5 (S.D.N.Y. Jan. 6, 2025). The complaint in this case has no such deficiency.

<sup>4</sup> Other decisions, concluding that alleged harms were not analogous to common law intrusion upon seclusion, are distinguishable. In Jones v. Bloomingdales.com, LLC, 124 F.4th 535 (8th Cir. 2024), the Eighth Circuit rejected a similar theory, but only because the plaintiff failed to allege that the defendant was actually exposed to any of her private data when she visited its website. Id. at 539. In Merck v. Walmart, Inc., 114 F.4th 762 (6th Cir. 2024), the Sixth Circuit rejected the analogy to intrusion on seclusion because the plaintiff had consented to the exposure of his data. Id. at 784.

is analogous to harm cognizable under the common law right to privacy. Salazar, 118 F.4th at 541-42; see also Bohnak v. Marsh & McLennan Cos., Inc., 79 F.4th 276, 285-86 (2d Cir. 2023).

Other Circuits have reached the same conclusion. Eichenberger v. ESPN, Inc., 876 F.3d 979, 983-84 (9th Cir. 2017); In re Nickelodeon Consumer Priv. Litig., 827 F.3d 262, 273-74 (3d Cir. 2016).

Moreover, at least four federal courts have found that the plaintiffs before them had made a sufficient showing of concrete injury, as analogous to common law privacy torts, when agencies granted DOGE agents access to repositories of plaintiffs' personal information. Maryland OPM Action, 2025 WL 895326, at \*10-13 (OPM, Treasury, and DOE); Maryland SSA Action, 2025 WL 868953, at \*35-44 (SSA); All. for Ret. Ams., 2025 WL 740401, at \*15-16 (Treasury); New York v. Trump, 2025 WL 573771, at \*11-21 (Treasury). In the Maryland OPM Action, the court explained that the plaintiffs had alleged an ongoing invasion of privacy, analogous to the common law tort of intrusion upon seclusion, based upon OPM having granted the DOGE agents unauthorized access to its members' personal information. 2025 WL 582063, at \*6. It noted that the common law required neither use nor publicity of the plaintiffs' personal information but rather

recognized harm from mere disclosure to an unauthorized recipient. Id.<sup>5</sup>

The defendants also argue that the complaint fails to plead that the plaintiffs are at risk of future harm, specifically that there is a likelihood that their information will be released to third parties. They contend that the identified risks of hacking and retaliation are speculative. As the Court has explained, however, “a person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial.” TransUnion, 594 U.S. at 435 (citing Clapper, 568 U.S. at 414 n.5). The requirement of imminent injury “does not uniformly require plaintiffs to demonstrate that it is literally certain that the harms they identify will come about. Rather, an allegation of future injury is sufficient where the injury is certainly impending, or there is a substantial risk that the harm will occur.” Saba Cap. Cef Opportunities 1, Ltd. v. Nuveen Floating Rate Income Fund, 88 F.4th 103, 111 (2d Cir. 2023) (citation omitted).

While the mere risk of future harm may not qualify by itself “as

---

<sup>5</sup> In an opinion on the plaintiffs’ application for a TRO in the Virginia OPM Action, the court considered but did not rule on whether the plaintiffs had standing to challenge OPM and Treasury granting DOGE agents access to the plaintiffs’ private data. 2025 WL 580596, at \*6.

a concrete harm" when seeking damages, that does not hold true for a suit seeking injunctive relief. TransUnion, 594 U.S. at 435-36.

The complaint has plausibly pleaded an ongoing harm as well as an imminent and substantial risk of future harm. As an initial matter, the complaint's allegation of ongoing unauthorized access by the DOGE agents to the plaintiffs' data is sufficient to meet the injury in fact requirement. In other words, the plaintiffs allege that the harm is more than imminent -- it is already here. The plaintiffs need not allege a sufficient likelihood of future disclosure because, as discussed above, further disclosure is not necessary for the harm that Article III requires.

Even so, the complaint also pleads that a risk of future harm exists and that the risk is substantial. It describes OPM giving sweeping and uncontrolled access to DOGE agents who were not properly vetted or trained. That access included the ability to install and modify software and to alter internal documentation of access to the data. It identifies one of the DOGE agents as a 19-year-old who is known online as "Big Balls" and had been fired by a cybersecurity firm following an internal investigation into the leaking of proprietary information that coincided with his tenure. It explains as well that OPM is a

target of cyberattacks, and that in 2015 OPM publicly disclosed that it had been subject to a data breach affecting over 20 million people. Because of the extraordinary access given to DOGE agents, U.S. security experts have already raised concerns that “Russia, China, Iran and other adversaries could seek to exploit the chaos by launching new cyber intrusions.”

These allegations amply plead the existence of risk necessary to support a finding of standing. They plead that the plaintiffs’ highly sensitive and confidential data has already been disclosed to individuals without proper vetting or training, and that that access has made the OPM data more vulnerable to hacking, identify theft, and other activities that are substantially harmful to the plaintiffs. See Bohnak, 79 F.4th at 286-87 (data breach alone, without misuse of data, sufficient for standing for plaintiff seeking damages); New York v. Trump, 2025 WL 573771, at \*11-12 (discussing the risk of future harm arising from DOGE agents’ alleged unauthorized access to Treasury data).

To support their motion, the defendants minimize the unusual course of events described in the complaint. They state that OPM simply gave access to its records to a “limited number of new federal employees.” That is not a fair characterization of the complaint, which is entitled at this stage of proceedings



to be “construed in favor of the plaintiffs.” Liberian Cmty. Ass’n v. Lamont, 970 F.3d 174, 184 (2d Cir. 2020).

B. Causation and Redressability

The final elements of an injury in fact, causation and redressability, “are often flip sides of the same coin.” FDA, 602 U.S. at 380 (citation omitted). “If a defendant’s action causes an injury, enjoining the action or awarding damages for the action will typically redress that injury.” Id.

The complaint plausibly alleges that the defendants caused the plaintiffs’ injuries. The OPM Defendants, who are responsible for the safekeeping of the plaintiffs’ records, disclosed them to DOGE agents without requiring those agents to be appropriately vetted or trained, and without limiting their access in the ways required by the Privacy Act. This harm is redressable through an injunction, which may prohibit improper disclosure from continuing and, to the extent that any information from OPM records has been copied, order that the information be impounded and destroyed.

The defendants argue the chain of causation is too attenuated. They claim that the plaintiffs do not allege, and will be unable to demonstrate, that the disclosure to DOGE agents will cause them any harm from extra-governmental actors because they do not adequately plead that unauthorized access to

OPM records is likely to occur "notwithstanding OPM's existing internal security controls and mitigation efforts." There are several difficulties with this argument, and it is not necessary to discuss all of them. For one, it ignores the primary theory of harm discussed above -- that the disclosure to the DOGE agents itself establishes cognizable injury. That disclosure is plainly traceable to the OPM Defendants, and they do not suggest otherwise.

What is more, it is a core contention of the complaint that OPM did not adhere to its "existing internal security controls." The plaintiffs allege that the OPM Defendants disclosed OPM's records to DOGE agents who did not receive the security clearances and vetting that OPM normally requires of new employees; the OPM Defendants did not submit those agents to OPM's normal security training; the OPM Defendants gave unlimited access to OPM records to those agents; and the OPM Defendants disclosed OPM records to the agents in violation of the restrictions imposed by the Privacy Act. Whether the plaintiffs will prevail on their complaint's causes of action, or the defendants will succeed in showing that OPM's existing internal security controls were followed, must await future proceedings. At present, the plaintiffs have plausibly pleaded

an injury in fact caused by the defendants' illegal behavior, which may be redressed through a declaration and injunction.

## II. Privacy Act Claims

The complaint pleads two claims under the Privacy Act. Congress passed the Privacy Act in 1974. It found that the "privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by Federal agencies," and that the "increasing use of computers" has "greatly magnified the harm to individual privacy that can occur." Privacy Act of 1974, Pub. L. No. 93-579, §§ 2(a)(1)-(2), 88 Stat. 1896. As reflected in the Senate Report, the purpose of the Privacy Act is to

promote governmental respect for the privacy of citizens by requiring all departments and agencies of the executive branch and their employees to observe certain constitutional rules in the computerization, collection, management, use, and disclosure of personal information about individuals.

S. Rep. No. 93-1183, at 1 (1974). "The key operating concept of the Privacy Act is that individual rights must be recognized and balanced in agency uses of information." Doe v. DiGenova, 779 F.2d 74, 84 (D.C. Cir. 1985) (citation omitted); see also Maryland SSA Action, 2025 WL 868953, at \*23-24 (describing legislative history of the Privacy Act).

The plaintiffs have plausibly alleged violations of two provisions of the Privacy Act: 5 U.S.C. § 552a(b), which

prohibits certain disclosures of records, and 5 U.S.C. § 552a(e)(10), which imposes a duty to establish appropriate safeguards to ensure the security and confidentiality of records. Declaratory and injunctive relief to address these violations of the Privacy Act is not available under the Privacy Act, but, as will be described below, it is available under the APA.

A. Violations

1. Illegal Disclosure

The plaintiffs allege that the OPM Defendants have violated the Privacy Act, and are continuing to do so, by disclosing OPM's records to the DOGE Defendants. Correctly anticipating the defense the defendants are relying on here, the complaint pleads as well that the DOGE Defendants did not have a need for the records in the performance of any lawful duty they may have at OPM or elsewhere in the federal government.

The Privacy Act provides that:

No agency shall disclose any record which is contained in a system of records by any means of communication to any person, or to another agency, except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains[.]

5 U.S.C. § 552a(b). That provision is followed by twelve enumerated exceptions listed in § 552a(b)(1)-(12). The first exception, and the one pertinent here, permits disclosure "to

those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.” Id. § 552a(b)(1) (“Exception (b)(1)”). The Senate Report explains the intent of § 552a(b) and § 552a(b)(1):

The section envisions that if an employee dealing with official information about a person is requested to surrender that person’s record to someone who clearly has no need for it, he should decline or seek to define the purpose of the requested disclosure. One of the results of this section may be to promote a sense of ethical obligation on the part of Federal officials and employees to ascertain when improper disclosure of information within the agency may be sought or promoted for personal, political or commercial motives unrelated to the agency’s administrative mission.

S. Rep. No. 93-1183, at 51-52 (1974); see also Pilon v. U.S. Dep’t of Just., 73 F.3d 1111, 1120-22 (D.C. Cir. 1996) (legislative history and purpose of the Privacy Act).

To plead the violation of § 552a(b) at issue here, a plaintiff must adequately allege that:

- (1) an agency covered by the Privacy Act maintains a system of records;
- (2) the agency disclosed to another person or agency a record contained in that system that pertains to the plaintiff;
- (3) the plaintiff did not submit a written request for the record’s disclosure to the agency or give prior written consent to the disclosure; and
- (4) no exception under the Privacy Act applied, including § 552a(b)(1).

See Chichakli v. Tillerson, 882 F.3d 229, 233 (D.C. Cir. 2018) (requiring a plaintiff seeking damages to plead the disclosure did not fall under the “routine use” exception, § 552a(b)(3)); Quinn v. Stone, 978 F.2d 126, 131 (3d Cir. 1992) (listing elements for claim for damages under the Privacy Act).<sup>6</sup>

The Privacy Act and agency regulations contain definitions for critical terms. There is no dispute that OPM is one of the agencies to which the Privacy Act applies. See 5 U.S.C. § 552a(a)(1) (defining agency). A “record” is defined as

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

Id. § 552a(a)(4). A “system of records” is defined 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[.]

Id. § 552a(a)(5). The term “maintain” is defined to include “maintain, collect, use, or disseminate.” Id. § 552a(a)(3).

---

<sup>6</sup> Since the plaintiffs are not seeking damages, they need not plead either “adverse effect” or “intentional or willful” disclosure, which derive from the Privacy Act’s civil remedies provision. See Quinn, 978 F.2d at 131 n.6, 135; 5 U.S.C. § 552a(g)(1)(D), (g)(4).

"Individual" is defined as "a citizen of the United States or an alien lawfully admitted for permanent residence." Id. § 552a(a)(2).

OPM's own regulations, enacted in 1988, govern the "maintenance, protection, disclosure and amendment of records" within the systems of records protected by the Privacy Act. 5 C.F.R. § 297.101. OPM's regulations define "disclosure" as "providing personal review of a record, or a copy thereof, to someone other than the data subject or the data subject's authorized representative, parent, or legal guardian." Id. § 297.102.

OPM's regulations also address, among other things, the conditions for the disclosure of records, how to make requests for records, and exempt records. They require OPM to "maintain a record of disclosures" from a "system of records" except when "the disclosure is made to those officers and employees of the Office or agency who have a need for the record in the performance of their duties" or pursuant to FOIA. Id. § 297.403(a).

The complaint plausibly alleges a violation of § 552a(b). It asserts that OPM maintains a system of records, as defined by the Privacy Act, and that it disclosed those records without the written consent of the individuals to whom those records

pertained. It pleads as well that Exception (b)(1) did not permit the disclosures, both because they were made to DOGE agents who were not officers or employees of OPM and because, even if the DOGE agents were employees of OPM, they did not have a need for those records in the performance of any lawful duty. Other federal courts have found a likelihood that plaintiffs will succeed in their claims that government defendants violated § 552a(b) by disclosing confidential records to DOGE agents. Maryland OPM Action, 2025 WL 895326, at \*19-28 (OPM, Treasury, and DOE); Maryland SSA Action, 2025 WL 868953, at \*60-64 (SSA).

The defendants do not dispute that the plaintiffs have pleaded several elements of a § 552a(b) claim. They do not dispute that the Privacy Act's restrictions apply to OPM, or that the complaint adequately pleads that the OPM Defendants gave DOGE agents access to OPM records without the written consent of the individuals to whom those records pertain. They have several arguments, however, to support dismissal of this claim.

i. Disclosure

The defendants contend that the complaint does not adequately allege that the records were "disclosed" to the DOGE agents. They argue that a disclosure for purposes of the Privacy Act requires not just transmission to another person but



also review of the records by that individual. This argument fails.

First of all, the complaint amply pleads that the DOGE agents viewed, possessed, and used the OPM records. Indeed, the goal of the endeavor described in the complaint, including the documents it incorporates, was to equip the DOGE agents to use OPM records on an expedited basis even though doing so circumvented OPM's ordinary security practices.

In any event, the defendants misconstrue the term "disclose." To show a violation of the Privacy Act, a plaintiff need not prove that the individual to whom the records were disclosed actually reviewed, much less used, those records. As noted above, OPM's regulations define disclosure as "providing personal review of a record, or a copy thereof, to someone other than the data subject or the data subject's authorized representative, parent, or legal guardian." 5 C.F.R. § 297.102. Under this definition, "providing" access to another person for their review of a record is a disclosure. This is consistent with how other agencies have defined disclosure for purposes of their own compliance with the Privacy Act. For example, OMB states that "disclosure may be either the transfer of a record or the granting of access to a record," 40 Fed. Reg. 28948, 28953 (July 9, 1975), while the SSA defines "disclosure" as

“making a record about an individual available to or releasing it to another party.” 20 C.F.R. § 401.25. While these regulatory definitions are not binding, they are informative in light of these agencies’ “body of experience and informed judgment” related to maintaining large systems of records that are subject to the Privacy Act. Loper Bright Enters. v. Raimondo, 603 U.S. 369, 402 (2024) (citation omitted).

These regulatory definitions are also consistent with congressional intent and the plain meaning of the word “disclose.” See Pilon, 73 F.3d at 1119-24. In interpreting terms in the Privacy Act, including the term “disclose,” the D.C. Circuit took “particular care not to undermine the Act’s fundamental goals.” Id. at 1118. It concluded that, under the Privacy Act, “disclose” includes “virtually all instances [of] an agency’s unauthorized transmission of a protected record.” Id. at 1124.

The defendants’ reliance on Wrocklage v. Dep’t of Homeland Sec., 769 F.3d 1363 (Fed. Cir. 2014), to advance a different definition of the term “disclose” fails. Wrocklage overruled a finding of the Merit Systems Protection Board that a Customs and Border Protection Officer violated the Privacy Act when he emailed a document to a person who never viewed it. Id. at 1368. Wrocklage did not construe a regulatory definition of

"disclose," much less OPM's definition of that term. United States v. John Doe, Inc. I, 481 U.S. 102 (1987), on which the defendants rely in their reply, in fact undercuts their argument. It construed the term "disclose" in Fed. R. Crim. P. 6(e), holding that the rule prohibits those with information about the workings of a grand jury "from revealing such information to other persons who are not authorized to have access to it." Id. at 108. It recited the common dictionary definitions of "disclose" as including to "open up" and to "expose to view." Id. at 108 n.4 (citation omitted).

ii. Employment Status

In relying on Exception (b)(1), the defendants also contend that the complaint does not plausibly plead that the DOGE agents were not OPM employees at the time they demanded and received access to OPM records.<sup>7</sup> The determination of one's employment status within a federal agency is not always straightforward.

Title 5 of the United States Code, which contains the Privacy Act, defines the term "employee." 5 U.S.C. § 2105(a).

---

<sup>7</sup> While this Opinion addresses the adequacy of the pleadings, the defendants have not offered much reassurance that, as a matter of historical fact, DOGE agents were OPM employees at the time they were given access to OPM's records. The Hogan declaration submitted on February 19, 2025 does not explain whether the DOGE agents had been "onboarded" by OPM when they were first given access to OPM records. It also admits that at least one of the DOGE engineers was the paid employee of an agency other than OPM, without identifying the agency.

Federal employees can be "detailed" from one agency to another pursuant to the Economy Act when the "head of an agency . . . place[s] an order with . . . another agency for goods or services." 31 U.S.C. § 1535(a). Title 31, which contains the Economy Act, defines an "agency" as "a department, agency, or instrumentality of the United States Government." Id. § 101. Courts have resisted further defining the term "agency" given "the myriad organizational arrangements for getting the business of the government done." Burch v. Pioneer Credit Recovery, Inc., 551 F.3d 122, 124 (2d Cir. 2008) (citation omitted). In determining which agency employs a detailed employee, the D.C. Circuit applies a functional approach that includes an evaluation of all the circumstances of the relationship, such as what work they do, where they work, and who supervises them. Jud. Watch, Inc. v. Dep't of Energy, 412 F.3d 125, 131-32 (D.C. Cir. 2005) (citation omitted).

Accordingly, in determining whether Exception (b)(1) applies, it will be relevant at some point in this litigation to determine whether, at the time they were first given access to OPM records, the DOGE agents were OPM employees. To the extent they were detailed from another component of the government at the time they were first given access, it may be necessary to determine whether that entity was a federal agency, and whether

that agency or OPM employed the DOGE agent. As already described, Exception (b)(1) of the Privacy Act only permits OPM to disclose its records to its own employees.

The issue for now is whether the complaint plausibly pleads a claim. The complaint states that "Musk and other DOGE actors were not government employees at the time they demanded and received access to the OPM computer networks." Relying on press reports incorporated into the complaint, it explains that many of the DOGE agents who were given access to OPM records were under the age of 25 and "until recently" were employees of Musk's private companies. As previously described, the complaint alleges as well that the ordinary clearance and training procedures were not followed before the DOGE agents accessed the OPM records. Finally, the complaint explains that USDS and the Temporary Organization, which were directing the work of the DOGE agents, are components of the Executive Office of the President and thus entirely separate entities from OPM. These and related allegations suffice to find that the complaint plausibly pleads that DOGE agents who were given access to OPM records were not OPM employees.

The defendants argue that one of the press reports incorporated into the complaint contradicts the complaint's allegation that the DOGE agents were not OPM employees. To the

contrary, the Washington Post article to which the defendants refer describes the individuals accessing OPM data systems as “Musk’s agents,” “members of Musk’s pseudo-governmental DOGE,” “Musk’s DOGE team,” and “DOGE agents.” The article did not purport to explore the complexities of determining agency employment status. See, e.g., Jud. Watch, Inc., 412 F.3d at 131-32. As one court has already observed, even if DOGE agents were assigned to an agency’s DOGE Team, that is not dispositive of their employment status within the agency. See Am. Fed’n of Lab., 2025 WL 542825, at \*2-4 (observing, inter alia, that USDS may not wish to accept the obligations that would accompany a finding that it is an “agency”).

To the extent that the defendants are contending in their motion that disclosure of OPM records to DOGE agents would have been lawful even if the agents were not OPM employees, that argument fails. As explained, Exception (b)(1), on which the defendants are relying to justify the disclosures at issue here, applies to “those officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.” 5 U.S.C. § 552a(b)(1) (emphasis supplied).

## iii. Need to Review

Finally, the defendants contend that the complaint fails to plead that any DOGE agents who were employees of OPM did not have a need to review the OPM records. As has been noted, disclosure of an OPM record to another OPM employee is permitted when that employee has "a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1); see also 5 C.F.R. § 297.401(a). This argument also fails.

The term "need" is not defined in the Privacy Act. In determining whether an official has a "need" for a record within the meaning of § 552a(b)(1), courts consider "whether the official examined the record in connection with the performance of duties assigned to him and whether he had to do so in order to perform those duties properly." Bigelow v. Dep't of Def., 217 F.3d 875, 877 (D.C. Cir. 2000). This is described as a "need to know" requirement. Maryland SSA Action, 2025 WL 868953, at \*63.

The complaint alleges that no exception to the Privacy Act covers the DOGE Defendants' access to records held by OPM and, in a more specific reference to Exception (b)(1), that the OPM records were disclosed to DOGE agents who did not have "a lawful and legitimate need" for such access. This conclusory assertion adequately pleads a claim. The information that will identify

the appropriate exemption and potentially justify the disclosure is “peculiarly within the possession and control of the defendant.” Arista Recs., LLC v. Doe 3, 604 F.3d 110, 120 (2d Cir. 2010).<sup>8</sup>

The defendants argue that the DOGE agents needed full access to OPM systems because they were working to implement the DOGE Executive Order, that is, to “improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems.” Whether it was necessary, in order to achieve that goal, to give unrestricted access to multiple databases of OPM records to each of the DOGE agents, and whether the DOGE agents used their access for that purpose, is beyond the scope a Rule 12(b)(6) inquiry. At this stage, the inquiry is whether the plaintiffs have met their burden of pleading their claim. They have done so.<sup>9</sup>

---

<sup>8</sup> It is unnecessary to decide whether the exceptions to § 552a(b) should be treated as affirmative defenses that a plaintiff need not plead. Generally, however, “when a statutory prohibition is broad and an exception is quite narrow, it is more probable that the exception constitutes an affirmative defense.” Cunningham v. Cornell Univ., 86 F.4th 961, 975-76 (2d Cir. 2023) (citation omitted).

<sup>9</sup> Two federal courts have found that plaintiffs are likely to succeed on their claims that an agency’s disclosure to DOGE agents did not satisfy the “need to know” requirement. Maryland OPM Action, 2025 WL 895326, at \*19-28 (OPM, Treasury, and DOE); Maryland SSA Action, 2025 WL 868953, at \*64 (SSA).



2. Lack of Appropriate Safeguards

In their second Privacy Act claim, the plaintiffs allege that the defendants violated their duty to safeguard the plaintiffs' records as required by § 552a(e)(10) of the Privacy Act. This provision states:

Each agency that maintains a system of records shall . . . establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

5 U.S.C. § 552a(e)(10) (emphasis supplied); see Chambers v. U.S. Dep't of Interior, 568 F.3d 998, 1007 n.7 (D.C. Cir. 2009).

The complaint adequately alleges that the OPM Defendants failed to establish appropriate safeguards to ensure the security and confidentiality of the OPM records they disclosed to the DOGE Defendants. In particular, it pleads that the OPM Defendants did not establish security vetting and security training for the DOGE Defendants before they were given such access.

The defendants do not make any argument addressed specifically to this claim. Their sole, brief reference to this claim is made in connection with the APA claims. Accordingly, the only remaining issue is whether the plaintiffs may obtain

relief under the Privacy Act for their well-pleaded Privacy Act claims.

B. Injunctive Relief

The Privacy Act provides that an individual may bring suit against an agency that “fails to comply with any [] provision of [the Privacy Act], or any rule promulgated thereunder, in such a way as to have an adverse effect on an individual.” 5 U.S.C. § 552a(g) (1) (D). Monetary remedies are available for any violation of the statute by an agency “which was intentional or willful.” Id. § 552a(g) (1), (g) (4). In contrast, individuals may obtain injunctive relief in only two circumstances: courts may order agencies to amend an individual’s records or to give an individual access to their own records. Id. § 552a(g) (2) (A), (g) (3) (A). Accordingly, the plaintiffs may not obtain declaratory or injunctive relief under the Privacy Act for the violations they have alleged here. Sussman v. U.S. Marshals Serv., 494 F.3d 1106, 1122 & n.10 (D.C. Cir. 2007) (Privacy Act does not provide injunctive relief for § 552a(b) violation).

The plaintiffs argue otherwise. But they rely on older cases that concern a provision of the Privacy Act that is not at issue here, § 552a(e) (7), and cases that have been superseded by more recent decisions by Courts of Appeals. See Sussman, 494

F.3d at 1122; Doe v. Chao, 435 F.3d 492, 504 (4th Cir. 2006) (collecting cases).

The plaintiffs also argue that courts have inherent equitable power to provide “complete relief in light of the statutory purposes” of the Privacy Act. Mitchell v. Robert DeMario Jewelry, Inc., 361 U.S. 288, 292 (1960). As described below, the plaintiffs may seek that relief through the APA.

### III. APA Claims

The complaint brings two claims under the APA. First, the plaintiffs assert that the defendants’ actions were contrary to law because they violated the Privacy Act and the Federal Information Security Management Act (“FISMA”). Second, they assert that the OPM Defendants acted in an arbitrary and capricious manner because they failed to engage in reasoned decision-making when altering OPM policies, specifically by failing to consider their legal obligations and possible harms when giving the DOGE Defendants access to OPM’s records for purposes other than those authorized by the Privacy Act. The complaint adequately pleads both APA claims.

The APA enables a reviewing court to “hold unlawful and set aside agency action” that is “arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.” 5 U.S.C. § 706(2) (A). Agency action is arbitrary and capricious

only if the agency has relied on factors which Congress has not intended it to consider, entirely failed to consider an important aspect of the problem, offered an explanation for its decision that runs counter to the evidence before the agency, or is so implausible that it could not be ascribed to a difference in view or the product of agency expertise.

Am. Cruise Lines v. United States, 96 F.4th 283, 286 (2d Cir. 2024) (citation omitted).

As explained above, the complaint adequately alleges a violation of the Privacy Act. Accordingly, it adequately alleges that the defendants' actions were "not in accordance with law" under 5 U.S.C. § 706(2)(A). Given this conclusion, it is unnecessary to also decide whether it adequately alleges a violation of FISMA.

The complaint also adequately alleges that the OPM Defendants violated the APA by acting in an arbitrary and capricious manner. It alleges that OPM's decision to give multiple DOGE agents immediate and unrestricted access to OPM's records was a gross departure from OPM's longstanding practices of carefully vetting individuals who receive access, making sure they obtain customary security clearance, and providing them with the appropriate security training. The complaint alleges that OPM rushed the onboarding process, omitted crucial security practices, and thereby placed the security of OPM records at grave risk. OPM took these actions despite the instruction in

the DOGE Executive Order that it “shall be implemented consistent with applicable law” and that USDS shall “adhere to rigorous data protection standards.”<sup>10</sup>

The defendants argue that the complaint’s APA claims are not reviewable for two reasons. They contend that the plaintiffs fail to identify a final agency action, and that the plaintiffs cannot resort to the APA because they have “other adequate alternative remedies” under the Privacy Act. Neither argument succeeds.

A. Final Agency Action

The APA only provides for judicial review of “final agency action.” 5 U.S.C. § 704. The APA defines “agency action” to include “the whole or a part of an agency rule, order, license, sanction, relief, or the equivalent or denial thereof, or failure to act.” 5 U.S.C. § 551(B). The word “action” is meant to “cover comprehensively every manner in which an agency may exercise its power.” Whitman v. Am. Trucking Ass’ns, 531 U.S. 457, 478 (2001).

---

<sup>10</sup> Some federal courts have recently awarded preliminary relief on APA claims where agencies granted DOGE agents access to repositories of personal information. Maryland OPM Action, 2025 WL 895326, at \*19 (OPM, Treasury, and DOE); Maryland SSA Action, 2025 WL 868953, at \*53 (SSA); New York v. Trump, 2025 WL 573771, at \*19-21 (Treasury).

For an agency action to be “final,” two conditions must be met: “First, the action must mark the consummation of the agency’s decisionmaking process -- it must not be of a merely tentative or interlocutory nature. And second, the action must be one 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) (citation omitted). Courts take a “pragmatic approach” in analyzing finality. U.S. Army Corps of Eng’rs v. Hawkes Co., 578 U.S. 590, 599 (2016). There is no requirement that there be a writing to memorialize a final agency action. See Brotherhood of Locomotive Eng’rs & Trainmen v. Fed. R.R. Admin., 972 F.3d 83, 100 (D.C. Cir. 2020).

The complaint adequately alleges that OPM engaged in a final agency action when it abruptly changed its longstanding practices by giving access to sensitive and legally protected records in violation of those practices, federal statutes, and even the terms of the DOGE Executive Order. According to the complaint, the decision to give such rushed access to DOGE agents was the “consummation” of OPM’s decisionmaking process. It was neither a tentative nor interlocutory decision. No more deliberation needed to occur. And it was a decision from which the legal consequences pleaded in the complaint have flowed. As courts have emphasized, this prong must be assessed in a

“pragmatic” fashion; the focus is on “the concrete consequences an agency action has or does not have.” Ipsen Biopharmaceuticals, Inc. v. Azar, 943 F.3d 953, 956 (D.C. Cir. 2019) (citation omitted). Here, the complaint asserts that sensitive OPM records of tens of millions of Americans were disclosed to unvetted and untrained individuals with no legal right or duty to access those records.

The defendants argue that, for several reasons, there was no final agency action. First, they contend that the decision to grant this access to new employees was nothing more than an “informal” action reflecting OPM’s day-to-day operations, as opposed to a “formal” action, such as adopting a new policy. This argument fails. To begin with, final agency actions are not limited to “formal” actions. “[T]he absence of a formal statement of the agency’s position, as here, is not dispositive.” Her Majesty the Queen in Right of Ontario v. U.S. E.P.A., 912 F.2d 1525, 1531 (D.C. Cir. 1990). More significantly, however, the defendants mischaracterize the pleadings. The complaint plausibly alleges that actions by OPM were not representative of its ordinary day-to-day operations but were, in sharp contrast to its normal procedures, illegal, rushed, and dangerous.

The defendants next argue that OPM's decision to give new employees access to its data systems does not have direct and appreciable legal consequences. But the complaint has adequately pleaded that its decision does have legal consequences, both in violating the Privacy Act and in violating the APA's prohibition against arbitrary and capricious agency action.

Finally, the defendants contend that the decision to give new employees broad access to its records without proper vetting and training is beyond the scope of APA review since, under the Privacy Act, OPM has discretion over which security and training measures it should adopt. As described above and as will be repeated here for ease of reference, the Privacy Act provides that each agency that maintains a system of records "shall"

establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.

5 U.S.C. § 552a(e)(10). This provision is the basis for the plaintiffs' second Privacy Act claim.

The APA does not preclude review of the defendants' actions. The APA establishes a "basic presumption of judicial review for one suffering legal wrong because of agency action."



Dep't of Homeland Sec. v. Regents of the Univ. of Cal., 591 U.S. 1, 16 (2020) (citation omitted). That presumption can be rebutted by a showing that the "agency action is committed to agency discretion by law." Id. (quoting 5 U.S.C. § 701(a)(2)). This exception to judicial review, however, is read "quite narrowly." Weyerhaeuser Co. v. U.S. Fish & Wildlife Serv., 586 U.S. 9, 23 (2018). "A court could never determine that an agency abused its discretion if all matters committed to agency discretion were unreviewable." Id. Therefore, the exception applies only to "those rare circumstances where the relevant statute is drawn so that a court would have no meaningful standard against which to judge the agency's exercise of discretion." Id. (citation omitted).

The argument that OPM has unreviewable discretion over the conduct at issue here misses the mark. The complaint alleges that OPM disclosed its records to the DOGE agents without following the systems it had adopted pursuant to 5 U.S.C. § 552a(e)(10) to safeguard its records. The complaint is not seeking review of whether OPM's customary practices are "appropriate," as the defendants suggest, or review of OPM's discretion to choose among various "appropriate" measures for guaranteeing the security of records; it is challenging the decision by OPM to depart radically from its established

safeguards and to give access to DOGE agents in violation of the law.

B. Inadequacy of Alternative Remedies

The defendants next argue that the complaint's APA claims must be dismissed because the APA only provides for judicial review of agency actions "for which there is no other adequate remedy in a court." 5 U.S.C. § 704. The "adequate remedy" requirement is "narrowly construed . . . to apply only in instances when there are 'special and adequate review procedures' that permit an adequate substitute remedy." Sharkey v. Quarantillo, 541 F.3d 75, 90 n.14 (2d Cir. 2008) (quoting Bowen v. Massachusetts, 487 U.S. 879, 903 (1988)). An alternative remedy is not adequate if it provides only "doubtful and limited relief." Bowen, 487 U.S. at 901. To be adequate, a remedy need not provide "identical" relief to that available under the APA "so long as it offers relief of the same genre." Garcia v. Vilsack, 563 F.3d 519, 522 (D.C. Cir. 2009) (citation omitted).

The defendants' argument that the APA is unavailable to the plaintiffs because the Privacy Act provides an "adequate" remedy fails. For reasons already explained, the Privacy Act does not provide injunctive or declaratory relief for the claims at issue here. And while monetary relief is available under the Privacy

Act, the plaintiffs do not seek it in this action and, in any event, it would not stop the illegal disclosures alleged here or undo any of their effects, and therefore would provide only “doubtful and limited relief.” Bowen, 487 U.S. at 901.<sup>11</sup> As a result, the plaintiffs have no adequate recourse under the Privacy Act and may pursue their request for injunctive relief under the APA. See Maryland OPM Action, 2025 WL 582063, at \*8 (OPM, Treasury, and DOE).

The defendants’ Kafkaesque argument to the contrary would deprive the plaintiffs of any recourse under the law. They contend that the plaintiffs have no right to any injunctive relief -- neither under the Privacy Act nor under the APA. In the defendants’ view, the Privacy Act has carefully circumscribed injunctive remedies (which have been described above), those remedies are not available here, and the plaintiffs cannot circumvent the Privacy Act’s comprehensive remedial scheme by obtaining injunctive remedies through the APA. This argument promptly falls apart under examination.

First, as discussed, courts begin with a presumption that agency action is reviewable under the APA. Regents of the Univ. of Cal., 591 U.S. at 16. That presumption is overcome only when

---

<sup>11</sup> While the claims assert that the plaintiffs have sustained and will continue to sustain actual damages, the complaint seeks only declaratory and injunctive relief.

it is "fairly discernible" that Congress intended otherwise. Am. C.L. Union v. Clapper, 785 F.3d 787, 803-04 (2d Cir. 2015) (citation omitted). Indeed, "if the express provision of judicial review in one section of a long and complicated statute were alone enough to overcome the APA's presumption of reviewability for all final agency action, it would not be much of a presumption at all." Id. at 804 (citing Sackett v. E.P.A., 566 U.S. 120, 129 (2012)). Here, the Privacy Act explicitly provides for injunctive relief in two circumstances, while being silent regarding other circumstances. See 5 U.S.C. § 552a(g)(2)(A), (g)(3)(A). That is not "fairly discernible" evidence that Congress intended to preclude judicial review of APA claims alleging violations of the Privacy Act's substantive provisions or arbitrary and capricious actions by OPM that strike at the privacy concerns that drove the enactment of the Privacy Act. Clapper, 785 F.3d at 803-05.

Second, and more notably, the defendants have not identified any comparable cases in which injunctive relief which was ruled to be unavailable under the Privacy Act was also not available under the APA. Instead, the Supreme Court has suggested that injunctive relief is available under the APA in such circumstances. See, e.g., Cooper, 566 U.S. at 303 n.12; Doe v. Chao, 540 U.S. 614, 619 n.1 (2004); see also Doe v.

Stephens, 851 F.2d 1457, 1466 (D.C. Cir. 1988); Doe v. Chao, 435 F.3d at 504-05; Radack v. U.S. Dep't of Just., 402 F. Supp. 2d 99, 104 (D.D.C. 2005); Maryland SSA Action, 2025 WL 868953, at \*53 (SSA); Maryland OPM Action, 2025 WL 582063, at \*8 (OPM, Treasury, and DOE).

The cases on which the defendants rely are easily distinguished. In those cases, courts denied relief under the APA where the plaintiffs sought amendment of agency records or access to their own records, which are types of injunctive relief that can be obtained under the Privacy Act. See 5 U.S.C. § 552a(g) (2) (A), (g) (3) (A); Poss v. Kern, No. 23cv2199, 2024 WL 4286088, at \*6 (D.D.C. Sept. 25, 2024); Westcott v. McHugh, 39 F. Supp. 3d 21, 33 (D.D.C. 2014) (seeking amendment of United States Army reprimand record).

#### IV. Ultra Vires Claim

Finally, the defendants move to dismiss the complaint's ultra vires claim. This fifth and final cause of action is pleaded against the DOGE Defendants alone and asserts that no law permitted them to access and administer OPM systems.

The ultra vires right of action is a "nonstatutory" form of judicial review that derives from the inherent equitable powers of courts. Fed. Express Corp. v. U.S. Dep't of Com., 39 F.4th 756, 765 (D.C. Cir. 2022). This doctrine is available when

agency action is a clear departure from a statutory mandate or blatantly lawless. Id. at 764. Ultra vires claims are based on the premise that “if an agency action is unauthorized by the statute under which the agency assumes to act, the agency has violated the law and the courts generally have jurisdiction to grant relief.” Id. at 763 (citation omitted). Ultra vires claims are only available in the “extremely limited” circumstance where three requirements are met:

(i) the statutory preclusion of review is implied rather than express; (ii) there is no alternative procedure for review of the statutory claim; and (iii) the agency plainly acts in excess of its delegated powers and 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) (quoting DCH Reg’l Med. Ctr. v. Azar, 925 F.3d 503, 509 (D.C. Cir. 2019)).

The first of these requirements limits the availability of ultra vires review to situations where, on one hand, “Congress has not authorized statutory judicial review,” but, on the other hand, Congress “has not barred judicial comparison of agency action with plain statutory commands.” Fed. Express Corp., 39 F.4th at 765 (citation omitted). To satisfy the second requirement, plaintiffs must show that they have been “wholly deprived of a meaningful and adequate means of vindicating their alleged statutory rights.” Nat’l Air Traffic Controllers Ass’n

AFL-CIO v. Fed. Serv. Impasses Panel, 437 F.3d 1256, 1264-65 (D.C. Cir. 2006) (quoting Bd. of Governors of Fed. Rsrv. Sys. v. MCorp Fin., Inc., 502 U.S. 32, 43 (1991)). Thus, the Supreme Court has suggested that ultra vires review is cabined to situations where it is needed to avoid "a sacrifice or obliteration of a right which Congress has given." MCorp Fin., Inc., 502 U.S. at 43 (citation omitted). To satisfy the third requirement, plaintiffs must show that "the agency has plainly and openly crossed a congressionally drawn line in the sand." Fed. Express Corp., 39 F.4th at 765. Given these stringent requirements, ultra vires claims have been described as "essentially a Hail Mary pass." Changji Esquel Textile Co. v. Raimondo, 40 F.4th 716, 722 (D.C. Cir. 2022) (citation omitted).

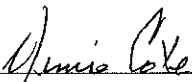
The defendants argue that the ultra vires claim should be dismissed because it is "coextensive" with the complaint's Privacy Act claims and the plaintiffs have failed to plead that Exception (b)(1) of the Privacy Act did not permit the OPM Defendants to disclose OPM records to the DOGE Defendants. This argument fails. The complaint alleges a massive disclosure of the OPM records of tens of millions of Americans to unvetted and untrained individuals who had no legal right to access those records, in wholesale disregard of the Privacy Act. It pleads that this intrusion was directed and controlled by the DOGE

Defendants, including individuals in USDS or associated with USDS. The DOGE Defendants have no statutory authority with respect to OPM records, such that these alleged actions were "blatantly lawless." Fed. Express Corp., 39 F.4th at 764 (citation omitted). The complaint adequately pleads that the DOGE Defendants "plainly and openly crossed a congressionally drawn line in the sand." Id. at 765.

**Conclusion**

The defendants' March 14, 2025 motion to dismiss under Rule 12(b)(6) is granted as to the complaint's First and Second Claims, except insofar as they are a predicate to the complaint's other claims. The defendants' motion to dismiss under Rule 12(b)(1) is denied. The defendants' motion to dismiss claims Three, Four, and Five under Rule 12(b)(6) is denied.

Dated: New York, New York  
April 3, 2025

  
\_\_\_\_\_  
DENISE COTE  
United States District Judge