UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

American Federation of Teachers, *et al.*,

Plaintiffs,

vs.

SCOTT BESSENT, in his official capacity as Secretary of the Treasury, *et al.*,

Defendants.

Case No. 8:25-cv-00430-DLB

Date: February 19, 2025
Time: 10:00 a.m.
Place: Greenbelt Courthouse
Judge: Hon. Deborah Boardman

REPLY MEMORANDUM IN SUPPORT OF PLAINTIFFS' MOTION FOR TEMPORARY RESTRAINING ORDER

TABLE OF CONTENTS

Page

TABLE OF AUTHORITIES

Page(s)

FEDERAL CASES

FEDERAL STATUTES

FEDERAL REGULATIONS

LEGISLATIVE MATERIALS

OTHER AUTHORITIES

INTRODUCTION

Defendants do not dispute that they granted DOGE representatives access to sensitive data systems protected by the Privacy Act. Nor do they dispute these individuals have actually accessed the personal information of Plaintiffs and millions of other Americans. Instead, Defendants' Opposition principally argues that these sweeping disclosures are lawful under the Privacy Act and the Administrative Procedure Act because the DOGE representatives in question are embedded in their agencies as employees, special government employees, or liaisons, and so can help themselves to these systems and the personal data contained within. That is not the law. And for good reason. Defendants' warped reading of the Privacy Act, under which agencies could rubber stamp any request for personal data by DOGE representatives, would gut the Act's core protections. On its face, the Privacy Act allows agency employees to access information in protected systems of records under only narrow circumstances. Defendants have failed to provide this Court with any lawful explanation to justify granting DOGE affiliates access of this extraordinary depth and breadth. Swift relief is therefore necessary to protect Plaintiffs, who indisputably have standing under binding Fourth Circuit precedent, from this ongoing violation of their fundamental right to privacy.

ARGUMENT

I. Plaintiffs Have Standing

At the outset, Defendants' argument that Plaintiffs lack standing fails. Defendants contend that Plaintiffs have not established a concrete injury sufficient to confer Article III

standing. But Plaintiffs comfortably satisfy that requirement in two distinct ways: violation of their fundamental right to privacy and exposure to the non-speculative risk of identity theft.[1]

A. Defendants Have Violated and Will Continue to Violate Plaintiffs' Privacy

A plaintiff's harm is "concrete" when there is a "close historical or common-law analogue for their asserted injury." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021). Under Fourth Circuit precedent, the unauthorized disclosure of personal information qualifies as such a concrete harm because it is similar to traditionally cognizable privacy harms. In *Garey v. James S. Farrin, P.C.*, 35 F. 4th 917 (4th Cir. 2022), the Fourth Circuit found that plaintiffs had standing to sue after personal injury lawyers obtained accident reports containing their names and addresses, reasoning they had suffered an "invasion of privacy." *See id.* at 919–20, 922. Such "injuries to personal privacy," the court explained, have long been "redressable through private litigation." *Id.*; *see also TransUnion*, 594 U.S. at 425 (noting the traditional harm of "disclosure of private information").

Plaintiffs here have suffered a concrete injury. "[B]oth the common law and the literal understanding of privacy encompass" a person's right to "control" his or her private information. *U.S. Dep't of Just. v. Reps. Comm. for Freedom of Press*, 489 U.S. 749, 763 (1989). That includes the right to fix the limits of the dissemination of that information. *See id.* at 763 & n.15. Here, Plaintiffs entrusted their data to Defendants based on the understanding that it would be accessed only by legally authorized parties and only for legally authorized purposes. *See, e.g.*,

[1] This discussion establishes that Individual Plaintiffs and members of Plaintiff Organizations have standing to sue in their own right. Consequently, Plaintiff Organizations have associational standing to sue, because: 1) as shown, at least one member has standing to sue in their own right; 2) this suit seeks to protect interests germane to Plaintiff Organizations' purpose, *see* Tammelleo Decl. ¶¶ 4–5; Bryant Decl. ¶¶ 4–9; Shackleford Decl. ¶¶ 4–5, ECF No. 14-11; Biggs Decl. ¶¶ 3–7, ECF No. 14-12; and 3) this suit does not require participation of individual members. *See Hunt v. Wash. State Apple Advertising Comm'n*, 432 U.S. 333, 343 (1977). Defendants have not disputed that Plaintiff Organizations satisfy the second and third factors for associational standing.

Cain Decl. ¶ 9, ECF No. 14-3; Fant Decl. ¶ 7, ECF No. 14-4; Goldsmith Decl. ¶ 8, ECF No. 14-5; Grambo Decl. ¶ 7; Martinez Decl. ¶ 9, ECF No. 14-7; Purdy Decl. ¶ 8, ECF No. 14-8. Defendants violated that trust, and thereby deprived Plaintiffs of their right to control access to their data. That "injur[y] to [their] privacy" satisfies the concreteness requirement. *Garey*, 35 F. 4th at 922.[2]

Further, unless this Court steps in, additional invasions of Plaintiffs' privacy rights are imminent. As discussed in Plaintiffs' Motion, Defendants have already disclosed Plaintiffs' personal information. *See* Mot. at 21–22. Those past violations make it considerably more likely that the same harms will occur in the future. *See Murthy v. Missouri*, 603 U.S. 43, 59 (2024) (citing *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 411 (2013)). And the record amply supports that conclusion. To date, DOGE representatives' efforts to access sensitive data have been "unceasing." Declaration of Xiaonan April Hu ("Hu Decl.") Ex. A. And they have not yet accomplished the goals they set out to achieve. *See id.* Ex. B (discussing Musk's ambitions to "end[]" the Department of Education); *id.* Ex. C (describing the desire for "Treasury to be the chokepoint on payments"); *id.* Ex. D (discussing ongoing mass layoffs, which require access to data from OPM); *id.* Ex. E (similar). Unsurprisingly, Elon Musk has chafed at efforts to restrict DOGE's access, *see id.* Ex. F (Musk calling the judge who blocked DOGE access to Treasury

[2] Contrary to Defendants' view, *see* Opp. at 15–16, Plaintiffs do not argue that the mere violation of a statute confers standing. Indeed, not every violation of the Privacy Act interferes with a person's right to control the agency's disclosure of their personal information. *See* 5 U.S.C. § 552a(d)(1) (providing for an individual's access to their own records); *id.* § 552a(d)(2) (allowing an individual to request amendment of their records). But the Privacy Act violations at issue here squarely implicate that right. And the resultant harms are particularly acute. The disclosure of any one of the Plaintiffs' social security numbers, physical addresses, dates of birth, and financial information would be independently concerning. But the disclosure of the sum total of that information is particularly troubling. *See* 120 Cong. Rec. 36,917 (daily ed. Nov. 21, 1974) (statement of Sen. Percy) (describing the Privacy Act's aim to avoid "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"); *see also U.S. Dep't of Justice*, 489 U.S. at 764 (explaining that the law recognizes a "distinction, in terms of personal privacy, between scattered disclosure of the bits of information contained in a rap sheet and revelation of the rap sheet as a whole"). Accordingly, even if some disclosures would not implicate sufficient privacy interests to confer standing, these do.

systems a "corrupt judge protecting corruption"), suggesting that he expects his representatives to make future use of their access. And at this very moment, "Treasury is working to onboard additional DOGE staff." Opp. at 23. In short, there is every reason to think that Defendants will continue to harm Plaintiffs by disclosing their personal information to DOGE representatives unless this Court steps in.

B. Defendants' Disclosures Create an Intolerable Risk of Identity Theft

A material increase in the risk of identity theft is likewise a concrete harm. *See O'Leary v. TrustedID, Inc.*, 60 F. 4th 240, 243–44 (4th Cir. 2023).

Plaintiffs have established that DOGE representatives' continued access to Defendants' systems materially increases the likelihood of identity theft. Every time Defendants disclose more data to DOGE or permit DOGE to retain that data, Defendants compound the risk to Plaintiffs. Each passing day and each additional disclosure creates another opportunity for DOGE to intentionally disclose the information to the public or outside the government (as it has already reportedly done with classified information about an intelligence agency, *see* Hu Decl. Ex. H) or have that information taken by bad actors who infiltrate DOGE's systems.

As to the latter, DOGE's security is clearly not up to par. Its website has already been hacked. *See* Hu Decl. Ex. G. At OPM, it used a commercial server that did not comply with legal requirements designed to ensure that its use "would not create any security vulnerabilities." *See id.* Ex. I. And DOGE's representatives are using non-governmental devices to access government servers, increasing their vulnerability. *See id.* Ex. J. In addition to undermining Defendants' argument that they took adequate security measures prior to disclosure, these examples of DOGE's inability or unwillingness to employ even basic security measures all but

guarantee that fraudsters around the world now view the data in DOGE's possession as a soft target. The risk that this data will be misappropriated and misused is a clear and concrete injury.

II. Plaintiffs Are Likely to Prevail on the Merits

A. Plaintiffs Are Entitled to Injunctive Relief Under the APA

Fourth Circuit precedent makes clear that the APA authorizes injunctive relief for violations of the Privacy Act like those at issue here. In *Doe v. Chao*, the court recognized that injunctive relief for government violations of the Privacy Act is "appropriate and authorized by the APA." 435 F.3d 492, 505 n.17 (4th Cir. 2006). Defendants' arguments to the contrary ignore that authority, and instead rely largely on out-of-circuit cases that are easily distinguished.

1. Defendants' Decisions to Disclose Constitute Final Agency Actions

An agency action is final when it: (i) constitutes the "'consummation' of the agency's decisionmaking process"; and (ii) 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) (emphasis added); *see Doe v. Tenenbaum*, 127 F. Supp. 3d 426, 461 (D. Md. 2012) ("[I]t bears emphasis that the *Bennett* court stated the second prong of the finality test in the disjunctive."). Both prongs are satisfied here.

Defendants' decision to provide DOGE representatives with access to sensitive systems of records marks the "consummation" of Defendants' decisionmaking process because the grant of access is not "tentative or interlocutory." *Bennett*, 520 U.S. at 178. Defendants concluded that "providing [DOGE representatives] with system access [is] *necessary*" to fulfil executive-branch policy goals, *see* Opp. at 16–17 (emphasis added), and adopted new technical measures to make such access "broader in scope than what has occurred in the past." Gioeli Decl. ¶ 13, ECF No. 27-3. Defendants assert that the grant of access was not a "consummate[d]" agency decision

"in any formal sense." Opp. at 17 (citing *Soundboard Ass'n v. Fed. Trade Comm'n*, 888 F.3d 1261, 1267 (D.C. Cir. 2018)). But Defendants' own authorities explain that the "key" question is "whether [the] action is properly attributable to the agency itself," which Defendants do not (and cannot) dispute is the case here. *See Soundboard Ass'n*, 888 F.3d 1261, 1267 (recognizing exception to finality where action is "informal, or only the ruling of a subordinate official").

Defendants' decision also determined the parties' rights by (1) granting DOGE representatives a broad new right of access without Plaintiffs' consent; and (2) abrogating Plaintiffs' right to receive notice when DOGE representatives accessed Plaintiffs' records. Defendants concluded "[t]he Privacy Act . . . allows disclosure of information protected under that statute" without Plaintiffs' written consent because "the members of each agency's DOGE Team are employees of their respective agencies," and their respective "SORNs . . . cover the DOGE Team's ambit." *Id.* at 21, 25. Those conclusions were wrong, but they were also plainly legal determinations affecting the parties' respective rights. *See Tenenbaum*, 127 F. Supp. 3d at 461;[3] *Venetian Casino Resort LLC v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008) (holding agency decision to "permit[] employees to disclose confidential information without notice is surely a 'consummation of the agency's decisionmaking process' and 'one by which the submitter's rights and the agency's obligations have been determined'" (quoting *Bennett*, 520 U.S. at 177–78)).

2. The Privacy Act Does Not Provide an Adequate Alternative Remedy

Defendants' contention that "the APA does not provide a cause of action" because "there is 'another adequate remedy'" under the Privacy Act aims to upend Fourth Circuit law. *See* Opp.

[3] Defendants' contention that granting access to DOGE representatives "creates no immediate legal effects for the *plaintiffs*," Opp. at 17 (emphasis added), is incorrect but also is irrelevant where, as here, granting access creates legal effects for *Defendants*. *See Tenenbaum*, 127 F. Supp. 3d at 461 (D. Md. 2012).

at 18–20. Defendants' only reference to Fourth Circuit precedent is to cite *Chao* for the proposition that "[i]njunctive relief for [unauthorized disclosure claims] is not available . . . [under] the Privacy Act." 435 F.3d at 19. But as *Chao* makes clear, the fact that injunctive relief is unavailable under the Privacy Act is *exactly why* the APA provides relief here. *See id.* at 505 n.17 (recognizing where "[injunctive] relief is not authorized by the Privacy Act, standing alone," such relief for a violation of the Privacy Act "will instead be appropriate and authorized by the APA"). Ignoring this Circuit's precedent, Defendants ask the Court to rely instead on inapposite out-of-circuit authority. *See* Opp. at 18–20.[4]

B. Defendants' Decisions to Disclose Violated the Privacy Act

The Opposition's attacks a straw man by mischaracterizing the "heart" of Plaintiffs' Privacy Act argument as being about DOGE representatives' status as federal employees. Opp. at 21. In truth, Plaintiffs' motion makes clear that the DOGE representatives—*regardless* of their status as agency employees—lack the requisite "need to know" to obtain access to Plaintiffs' records *and* that no promulgated "routine use" applies to their actions.[5] Mot. at 16-20.

[4] Defendants overread those out-of-circuit cases, which address APA claims that were *duplicative* of Privacy Act claims and do not hold that the APA bars injunctive relief for a Privacy Act violation. *See, e.g., Westcott v. McHugh*, 39 F. Supp. 3d 21, 33 (D.D.C. 2014) (rejecting plaintiff's APA claim for amendment of records because it was "simply a restatement of his Privacy Act claims"); *Poss v. Kern*, No. 23-CV-2199 (DLF), 2024 WL 4286088, at *6 (D.D.C. Sept. 25, 2024) (rejecting APA claim seeking release and amendment of records as duplicative of relief available under the Privacy Act).

[5] Plaintiffs *have* argued that to the extent that disclosures are being made outside of the Defendant agencies, such disclosures cannot fall within the "need to know" exception. Defendants appear to concede this point. *See* Opp. at 21. Defendants also appear to recognize that at least some of the DOGE affiliates are not in fact employed by the agency to which they have been dispatched, *see* Ramada Supp. Decl. ¶¶ 4–5, ECF No. 27-6, and so spill significant ink arguing that these individuals should nonetheless be considered Defendants' employees under the Privacy Act. Under the D.C. Circuit's decision in *Judicial Watch, Inc. v. Dep't of Energy*, 412 F.3d 125, 131 (D.C. Cir. 2005), however, it is doubtful that all of these "dispatched" DOGE affiliates do in fact qualify as employees. But for the reasons discussed in this section, Defendants' attempts to defend their disclosure decisions fail either way.

1. Defendants' Disclosures Do Not Fall Under the "Need-to-Know" Exception

Plaintiffs' motion explained that Defendants' disclosures could not fall under the Privacy Act's "need-to-know" exception because such a conclusion would undermine the purpose of the Privacy Act itself and run afoul of other Congressional constraints on agency authority. Mot. at 17-18. The Opposition's response boils down to the remarkable assertion that the DOGE representatives at the Defendant agencies "need to know '*all* unclassified agency records, software systems, and IT systems' to perform their duties" because the President's Executive Order said so. Opp. at 24.

This argument proves far too much. If the President could appoint representatives across multiple agencies and simply dictate that those representatives "need to know" all personal information held by each agency, that would render the Privacy Act—whose animating purpose was to prevent exactly this sort of disclosure—toothless. *See* 120 Cong. Rec. 36,917 (daily ed. Nov. 21, 1974) (statement of Sen. Percy) (describing the Privacy Act's aim to avoid "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"). Thankfully, this Court need not grapple with the Opposition's attempt to subvert the Privacy Act's core protections to the whims of the Executive, because—contrary to Defendants' argument—that is not in fact what Executive Order 14,158 says. Instead, the Order requires agency heads to make information available to DOGE only "to the maximum extent *consistent with law*." Exec. Order No. 14158, 90 Fed. Reg. 8441, 8442 (Jan. 20, 2025) (emphasis added).

In contrast to its (irrelevant) fearmongering about the erosion of the President's Article II authority, the Opposition musters only a single sentence in defense of DOGE representatives' specific need to know the information contained in Defendants' systems—it contends they "need

to know" the personally identifiable information of millions of Americans in order to "modernize" payment systems, implement "workplace reform," and "audit" Education's programs. *See* Opp. at 24. That single sentence is too slender a reed to support the weight of Defendants' decision to grant DOGE representatives unfettered access to Defendants' systems.

Courts permit disclosure pursuant to the need-to-know exception only where an "official examined the record in connection with the performance of duties assigned to him and . . . *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) (emphasis added). Defendants' declarations make clear that the disclosures at issue here are *unprecedented*. *See* Gioeli Decl. ¶ 13, ECF No. 27-3 ("[P]roviding a single individual with access to multiple systems and data records accessed here was broader in scope than what has occurred in the past."). Yet Defendants fail to explain in anything other than the most generic, high-level terms the nature of these DOGE affiliates' duties that purportedly require such unprecedented disclosures, much less *why* those duties require such disclosures. Defendants do not explain, for example, why an undisclosed number of DOGE representatives at OPM "need to know" each of the millions of pieces of sensitive information held in OPM systems in order to "implement workplace reform." Opp. 24. Without *any* explanation from the government, "it is difficult to see how knowledge with such specificity was necessary." *Walker v. Gambrell*, 647 F. Supp. 2d 529, 538 n.4 (D. Md. 2009). In addition, for the reasons set forth in Plaintiffs' Motion, there is ample reason to question whether access to Defendants' system was truly in service of a legitimate or lawful employee duty at all. *See* Mot. at 18.

2. Defendants Have Failed to Identify any Applicable "Routine Use"

As an initial matter, the Opposition fails to respond to Plaintiffs' argument that Defendants' purported uses of the accessed data are incompatible with the purposes for which

the relevant data was collected. *See* Mot. at 19-20. Accordingly, Defendants have forfeited any argument that their proffered routine uses are, in fact, compatible with the purpose for which the agencies collected the data. Defendants are required to make such a showing in order to invoke the "routine use" exception. *See* 5 U.S.C. § 552a(a)(7). This forfeiture alone is fatal to Defendants' routine use defense.

The Opposition passingly identifies a handful of "routine uses" that supposedly justify Defendants' sweeping disclosures, but none of the published uses identified by the Opposition in fact comports with lawful uses actually undertaken by the agencies, let alone with the purpose for which the relevant data was collected. For example, Defendants suggest that OPM's decision to disclose was made for the "routine use" of "help[ing] eliminate waste, fraud, and abuse in Governmental programs," Opp. at 25 (citing 77 Fed. Reg. 73694, 73697 (Dec. 11, 2012), but that argument has no support in Defendants' own evidence and misinterprets OPM's promulgated routine uses.

OPM's SORN does authorize a "routine use" related to eliminating waste, fraud, and abuse, but it is expressly limited to disclosures *made to other agencies "for use in computer matching." Id.* (emphasis added). Defendants' OPM declaration tellingly does not state that Defendants' disclosures were made for this specific purpose. *See* Hogan Decl. ¶¶ 12–13, ECF No. 27-8. Doubtless, that is because OPM is prohibited by law from engaging in "computer matching" with DOGE. The Privacy Act specifically bars disclosure for use in computer matching "except pursuant to a written agreement between the source agency and the recipient agency." 5 U.S.C. § 552a(o)(1). OPM and DOGE *could not possibly* have an effective computer matching agreement, as the Act requires a 30-day waiting period before any computer matching agreement takes effect, *id.* § 552a(o)(2)(B), and DOGE has existed for less than a month, Krause

Decl. ¶ 2, ECF No. 27-1. In any event, the Hogan Declaration suggests that "all individuals with access to sensitive OPM records . . . are employees of OPM." Hogan Decl. ¶ 12. To the extent that is correct, a routine use of disclosing data to other agencies for automated computer matching purposes cannot possibly justify disclosure to employees of OPM itself.

At Treasury, the Opposition points to a published routine use "for the purpose of identifying, preventing, or recouping improper payments to an applicant for, or recipient of, federal funds," Opp. at 25, but Defendants' declarations make clear that they are improperly reading this "routine use" exception to encompass actions that Congress has forbidden. Congress has tightly circumscribed Treasury's role in processing duly authorized payments, limiting it to ensuring that payments are "in proper form," "certified and approved" by another agency, and "computed correctly." 31 U.S.C. § 3325(a)(2). Treasury is not empowered to flag payments for purported compliance with Executive Orders or for any other substantive reason; such responsibility rests with the "certifying offic[er]" at the agency making the payment. 31 U.S.C. § 3528(a); *see State v. Bowsher*, 734 F. Supp. 525, 530 (D.D.C. 1990) ("The disbursing officials [at Treasury] do not review the vouchers to determine the legality or propriety of the underlying claims."). Yet the "Treasury DOGE Team" has apparently made use of the disclosed systems to "identify payments that may have been improper under the President's Executive Orders," specifically transactions related to "foreign development assistance." Krause Decl. ¶ 17. Defendants may not seek to insulate such *ultra vires* actions from Privacy Act scrutiny as "routine uses." *See FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 125 (2000) (An agency "may not exercise its authority in a manner that is inconsistent with the administrative structure that Congress enacted into law." (internal quotation and citation omitted)).

With respect to the Department of Education ("Education"), the Opposition fails to identify a published routine use that even arguably authorizes Defendants' disclosure of one of the systems of record at issue: NSLDS. It points to a SORN that allows for disclosure to "support governmental researchers and policy analysts," Opp. at 25 (citing 84 Fed. Reg. 47265, 47269 (Sept. 9, 2019)), but that published "routine use" is specific to the administration of "programs" operated under Title IV of the Higher Education Act of 1965. *See* 84 Fed. Reg. at 47269 ("The Department may disclose records to the specified users for the following *program purposes* . . . . (f) To support governmental researchers and policy analysts . . . ." (emphasis added)); *id.* at 47267 (explaining that the NSLDS system is maintained for various purposes relating to "title IV HEA programs"). There is no indication in the record that the disclosed data has been used to support "researchers or policy analysts" involved in the administration of Title IV programs.[6]

The Opposition also points to published routine uses related to supporting investigations into "fraud, waste, and abuse" to justify their disclosures of three other Education systems of records—CODS, FAS, and FMS—but these justifications differ markedly from those advanced in public and even those referenced in Defendants' declarations *in this case*. As explained in Plaintiffs' Motion, Elon Musk—the head of DOGE—has publicly stated a goal of ending the Education altogether. Mot. at 19; *see* Hu Decl. Ex. B. And Defendants' declarations make clear that Education's use of the disclosed systems is not limited to investigating fraud, waste, and abuse, but also involves "identify[ing] contracts and grants that are . . . *inconsistent with*

[6] The Ramada Declaration includes a one-sentence reference to DOGE representatives at Education "help[ing] senior Department leadership obtain access to accurate data and data analytics to inform their policy decisions at the Department." Ramada Decl. ¶ 4. But there is no indication that these vague "data analytics" efforts have anything to do with the Title IV programs that are the subject of the relevant SORN, or that the "senior" leadership referenced are government researchers or policy analysts.

leadership's policy priorities." Ramada Supp. Decl. ¶ 8, ECF No. 27-6 (emphasis added). Defendants cannot justify their disclosure of data for use in achieving their broader "policy priorities"—including ending the Department of Education—under the guise of a "routine use."

C. Defendants' Decisions to Disclose Were Arbitrary and Capricious

The declarations submitted in support of the Opposition—along with recent public events—only serve to confirm Defendants' disclosures were made capriciously. Defendants' purported security mitigations have already failed, suggesting that Defendants did not, in fact, appreciate the true extent of the security risks associated with these disclosures. For instance, the Opposition touts the fact that Education "required all DOGE Team members to complete information security training." Opp. at 26. But Defendants' declarations make clear that they have not been able to effectively implement that most basic protection. As of February 16, more than three weeks after DOGE began working in Education, one of its representatives had still not completed either ethics or information security training. Ramada Supp. Decl. ¶ 9. As noted *supra*, DOGE's website, where it reportedly has posted classified information, has already been hacked. Hu Decl. Ex. G. It is apparent that Defendants made these disclosures hastily and without proper consideration of the security risks involved, including enforcement of basic policies like security training for a group inexperienced in operating sensitive government record systems. *See id.* Ex. L at 16 (former Treasury officials expressing concern that disclosures to "unaccountable or inexperienced actors like DOGE [] pose[] significant operational risks for fraud, theft, or espionage").

III. Defendants' Disclosures Will Cause Irreparable Harm Absent an Injunction

Defendants' argument that Plaintiffs have suffered no harm from their sweeping disclosures is meritless. They do not appear to dispute that a harm to Plaintiffs' privacy is

"quintessential[ly]" irreparable, or that the "disclosure of sensitive financial and personal information 'is a bell that one cannot unring.'" Mot. at 21 (first quoting *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000); and then quoting *Senior Execs. Ass'n v. United States*, 891 F. Supp. 2d 745, 755 (D. Md. 2012)). Instead, their opposition reduces to an argument that Plaintiffs' fears are speculative. Opp. at 27–28.

Defendants ignore the fundamental injury caused by their conduct. Every time they unlawfully disclose Plaintiffs' information, they intrude on Plaintiffs' privacy and infringe on Plaintiffs' interest in controlling who sees and uses their personal information (and for what purpose)—quintessential irreparable harm. *See supra* pp. 2–3; Mot. at 22–23. Absent judicial intervention, those future injuries are virtually certain to occur. Indeed, it is all but guaranteed that, left unchecked, DOGE representatives will continue to exploit their access to Plaintiffs' sensitive personal data and violate Plaintiffs' privacy rights. *See supra* pp. 3–4.

Moreover, for all the reasons already provided above, the other dangers Plaintiffs face are both acute and distinctly likely. There is far more than a mere *possibility*, Opp. at 27, that Plaintiffs will become victims of identity theft or that their data will otherwise be misused. DOGE's lax approach to information security and the highly valuable nature of Plaintiffs' data have left a target on their backs. *See supra* p. 4. It is only a matter of time before individuals who wish to harm or steal from Plaintiffs get their hands on that information. *See* Goldsmith Decl. ¶ 13 ("This unlawful data access puts my life and my family at risk. . . . I feel that the risk of my data being leaked and weaponized against my family has never been higher.").

IV. The Equities and Public Interest Favor Plaintiffs

The equities and public interest favor protecting the status quo over Defendants' policy goals of rapidly transforming federal agencies' operations in unprecedented ways. As discussed

above, Plaintiffs face ongoing and irreparable injury from the unauthorized disclosures of their sensitive information. *See supra* p. 14. Defendants fail to articulate any comparable harm that would counsel against injunctive relief.

Defendants claim that a restraining order "would harm the public interest by limiting the President's ability to effectuate [his] policy choices." Opp. at 28. But Defendants fail to address the fact that the President has repudiated that claim. *See* White House, *President Trump Holds a Press Conference with Prime Minister Shigeru Ishiba of Japan*, YouTube, at 15:42–16:31 (Feb. 7, 2025), https://www.youtube.com/live/jMiAE9XWig?si=S0NkrDwEwLbrvTYM&t=942 (explaining DOGE does not need access to Americans' personal information). Defendants also contend—without citation or elaboration—that a restraining order "would cause cascading harms by preventing federal employees from doing their jobs." Opp. at 28–29. But Defendants fail to explain how providing DOGE representatives with access to Plaintiffs' private information is necessary to achieve any of Defendants' statutory duties. Finally, Defendants contend that a restraining order is "unnecessary here" because "Treasury and Education have paused access to data systems pending the outcome of preliminary injunction proceedings." *Id.* at 29. But that fact only goes to show that enjoining additional Defendants (or briefly extending the pause for the Treasury and Education Defendants, should other courts' injunctions on those Defendants' disclosures lapse) will not cause them any meaningful harm.

CONCLUSION

For the foregoing reasons, the Court should grant Plaintiffs' Motion for Temporary Restraining Order.

DATED: February 18, 2025

By: */s/ Xiaonan April Hu*
(signed by filer with permission)

Xiaonan April Hu (*pro hac vice*)
MUNGER, TOLLES & OLSON LLP
601 Massachusetts Avenue NW
Washington, DC 20001
(202) 220-1123
April.Hu@mto.com

John L. Schwab (*pro hac vice*)
MUNGER, TOLLES & OLSON LLP
350 S Grand Ave 50th Floor
Los Angeles, California 90071
(213) 683-9260
John.Schwab@mto.com

Carson Scott (*pro hac vice*)
Roman Leal (*pro hac vice*)
MUNGER, TOLLES & OLSON LLP
560 Mission Street, Twenty-Seventh Floor
San Francisco, California 94105-2907
(415) 512-4000
Carson.Scott@mto.com
Roman.Leal@mto.com

/s/ Mark Hanna

Mark Hanna (Fed. Bar No. 16031)
David J. Rodwin (Fed. Bar No. 18615)
MURPHY ANDERSON, PLLC
1401 K Street NW, Suite 300
Washington, DC 20005
T: (202) 223-2620 | F: (202) 296-9600
mhanna@murphypllc.com
drodwin@murphypllc.com

Daniel McNeil (*pro hac vice*)
General Counsel
American Federation of Teachers, AFL-CIO
555 New Jersey Ave. NW
Washington, DC 20001
T: (202) 393-6305 | F: (202) 393-6385
dmcneil@aft.org

Benjamin L. Berwick (*pro hac* forthcoming)
PROTECT DEMOCRACY PROJECT
15 Main Street, Suite 312
Watertown, MA 02472
(202) 579-4582
ben.berwick@protectdemocracy.org

Jessica A. Marsden (*pro hac vice*)
PROTECT DEMOCRACY PROJECT
510 Meadowmount Village Circle, No. 328
Chapel Hill, NC 27517
(202) 579-4582
jess.marsden@protectdemocracy.org

Kristy Parker (*pro hac vice*)
Jane Bentrott (*pro hac vice*)
Shalini Goel Agarwal (*pro hac* pending)
PROTECT DEMOCRACY PROJECT
2020 Pennsylvania Ave. NW, Suite 163
Washington, DC 20006
202-843-3092
kristy.parker@protectdemocracy.org
jane.bentrott@protectdemocracy.org
shalini.agarwal@protectdemocracy.org

Laurence M. Schwartztol (*pro hac vice*)
DEMOCRACY AND RULE OF LAW CLINIC
Harvard Law School 1525 Massachusetts Avenue
Cambridge, MA 02138 (617) 998-1877
lschwartztol@law.harvard.edu