IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND

AMERICAN FEDERTION OF STATE, COUNTY AND MUNICIPAL EMPLOYEES, AFL-CIO, *et al.*

Plaintiffs,

v.

SOCIAL SECURITY ADMINISTRATION, *et al.*

Defendants.

Civil Action No. ELH-25-0596

MEMORANDUM OPINION

Table of Contents*

* Because the Memorandum Opinion has not yet been docketed, the Court cites to the numbers that appear on the pages of the Memorandum Opinion, rather than the electronic pagination.

I. Introduction

This case is one of dozens of lawsuits filed since the inauguration of President Donald J. Trump on January 20, 2025, challenging a wide swath of executive orders as well as the implementation of them. In particular, this case concerns the decision of the Social Security Administration ("SSA" or the "Agency") to provide ten anonymous individuals affiliated with the Department of Government Efficiency ("DOGE") with unfettered access to the SSA records of millions of Americans.

"[W]e've just never seen anything like it," proclaimed plaintiffs' counsel at a motion hearing held on March 14, 2025. ECF 45 (Tr., March 14, 2025), at 64.[1] Defense counsel acknowledged at the hearing that SSA has, indeed, provided DOGE affiliates with access to a "massive amount" of records. *Id.* at 17. But, counsel claimed that such access is needed so that DOGE personnel can search for "improper or fraudulent payments" made by SSA. *Id.* at 22.

Ironically, the identity of these DOGE affiliates has been concealed because defendants are concerned that the disclosure of even their names would expose them to harassment and thus invade their privacy. The defense does not appear to share a privacy concern for the millions of Americans whose SSA records were made available to the DOGE affiliates, without their consent, and which contain sensitive, confidential, and personally identifiable information ("PII"). As used here, "'Personally identifiable information' means information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." Office of Mgmt. & Budget, Exec. Office of the President,

[1] With the exception of the Table of Contents, the Court cites to the electronic pagination. However, the electronic pagination does not always correspond to the page number imprinted on a particular submission.

OMB Circular A-130, *Managing Information as a Strategic Resource* (2016), https://perma.cc/L3CV-M6RF.

In particular, the information in SSA's records includes Social Security numbers, personal medical and mental health records, driver's license information, bank account data, tax information, earnings history, birth and marriage records, home and work addresses, school records, immigration and/or naturalization records, health care providers' contact information, family court records, and employment and employer records.

II. Summary

Plaintiffs, two national labor and membership associations and one grassroots advocacy organization, filed suit against the Social Security Administration and three other defendants on February 21, 2025, challenging the legality of SSA's decision to provide unlimited access to an enormous quantity of sensitive, personal, protected, and confidential information pertaining to millions of Americans. ECF 1.[2] On March 7, 2025, plaintiffs filed a "First Amended Complaint For Declaratory and Injunctive Relief," ECF 17 ("Amended Complaint"), which substantially

[2] Several cases have been filed throughout the country asserting similar allegations with respect to disclosures of confidential information by other federal agencies. *See*, *e.g.*, *American Federation of Teachers, at al., v. Bessent, et al.*, 25-DLB-0430, 2025 WL 582063 (D. Md. Feb. 24, 2025) (granting TRO against U.S. Department of Education, and Denise L. Carter, Acting Secretary of Education, as well as against the Office of Personnel Management and its Acting Director, Charles Ezell); *Electronic Privacy Information Center, et al., v. U.S. Office of Personal Management, et al.*, 25-RDA-255, 2025 WL 580596 (E.D. Va. Feb. 21, 2025) (denying preliminary injunction because plaintiffs failed to show irreparable harm); *New York, et al. v. Trump*, *et al*., 25-JAV-1144, 2025 WL 573771 (S.D.N.Y. Feb. 21, 2025) (granting preliminary injunction against U.S. Department of the Treasury and Scott Bessent, the Secretary of the Treasury); *New Mexico, et al., v. Musk, et al*., 25-TSC-429, 2025 WL 520583 (D.D.C. Feb. 18, 2025) (denying TRO because plaintiffs did not show irreparable harm); *Univ. of California Student Ass'n v. Carter*, 25-RDM-354, __ F. Supp. 3d __, 2025 WL 542586 (D.D.C. Feb. 17, 2025) (denying TRO because plaintiffs did not show irreparable harm); *Am. Fed'n of Lab. & Cong. of Indus. Organizations, et al. v. Dep't of Lab., et al.*, 25-JDB-0339, 2025 WL 542825, at *5 (D.D.C. Feb. 14, 2025) (denying TRO because plaintiffs did not show that they were highly likely to succeed on the merits).

revised the lawsuit and added three defendants. As discussed, *infra*, on the same date, plaintiffs also filed a motion for a temporary restraining order. ECF 21.

The plaintiffs are the American Federation of State, County and Municipal Employees, AFL-CIO ("AFSCME"); Alliance for Retired Americans ("ARA" or "Alliance"); and American Federation of Teachers ("AFT"). They have sued the Social Security Administration; Leland Dudek, in his official capacity as "purported Acting Commissioner" of the SSA; Michael Russo, in his official capacity as Chief Information Officer ("CIO") of the Agency; Elon Musk, in his official capacity as "Senior Advisor to the President and de facto head of" the Department of Government Efficiency; the "U.S. DOGE Service"; the U.S. DOGE Service Temporary Organization; and Amy Gleason, in her official capacity as the DOGE Acting Administrator.

I shall refer to the SSA, Dudek, and Russo collectively as the "SSA Defendants." I shall refer to the Department of Government Efficiency as "DOGE" and U.S. DOGE Service as "USDS." USDS; U.S. DOGE Service Temporary Organization; Musk; and Gleason shall be collectively referenced as the "DOGE Defendants." And, for convenience, I shall sometimes refer to all of the defendants collectively as the "government." The anonymous individuals associated with DOGE, to whom SSA has granted access to its records, shall be referred to as the "DOGE Team."

Plaintiffs allege that the SSA "has abandoned its commitment to maintaining the privacy of personal data" provided to the Agency by millions of Americans and has unlawfully "opened its data systems to unauthorized personnel from [DOGE] in violation of applicable laws and with disregard fo[r] the privacy interest of the millions of Americans that SSA serves." ECF 17, ¶ 2. They also maintain that the "White House" has demonstrated "a breathtaking disregard for the legal protections Congress and the Executive Branch implemented to protect data belonging to or

pertaining to individual Americans." *Id.* ¶ 12. And, they assert that it is unprecedented for "a group of unelected, unappointed, and unvetted individuals," described variously as White House employees, employees of agencies, and advisors, to gain access to such sensitive information. *Id.* ¶ 10. Similarly, referring to defendant Musk, they assert: "Never before has an industry mogul with countless conflicts of interest—not to mention an undefined role in the administration—sought and gained access to protected, private data on nearly every person in the country." *Id.* ¶ 11.

According to plaintiffs, defendants have "ransacked" the SSA, "installing DOGE associates without proper vetting or training . . . and demanding access to some of the agency's most sensitive data systems." *Id.* ¶ 83. This data includes, among other things, "Social Security numbers, employment and wage information, medical histories, tax return information, and personal addresses . . . ." *Id.* ¶ 1; *see also id*. ¶ 35. Thus, the suit "seeks to protect Plaintiffs and their members against the ongoing (and ever increasing) harm caused by DOGE and certain SSA executives' unlawful seizure of personal, private, and sensitive data from SSA systems." *Id.* ¶ 13.[3]

The Amended Complaint contains seven counts. Counts I, III, IV, and V allege unlawful and arbitrary and capricious Agency action, in violation of the Administrative Procedure Act ("APA"), 5 U.S.C. § 551 *et seq.*

Count I alleges that the SSA Defendants have unlawfully disclosed and continue to disclose "personal records contained in systems of records under their control," without consent of plaintiffs' members, in violation of the Privacy Act, 5 U.S.C. § 552a, and § 706(2) of the APA. ECF 17, ¶ 101. Count I also alleges that the SSA Defendants "entered inter-agency data sharing

[3] Subject matter jurisdiction is founded on 28 U.S.C. § 1331 because this action arises under federal law. ECF 17, ¶ 14.

agreements without abiding [by] the process prescribed by law, 5 U.S.C. § 552a(o)." *Id.* ¶ 102. According to plaintiffs, this conduct constitutes final agency action under 5 U.S.C. § 704. *Id.* ¶ 103. And, plaintiffs allege that the SSA Defendants "have thereby engaged in conduct that is contrary to law, in excess of statutory authority, and arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law" under 5 U.S.C. § 706(2). *Id.* ¶ 104.

In Count II, plaintiffs allege that the SSA Defendants have violated the Privacy Act, 5 U.S.C. § 552a(o), by the same actions identified in Count I. *Id.* ¶ 108–09. Accordingly, plaintiffs allege that they are entitled to civil remedies under 5 U.S.C. § 552a(g). *Id.* ¶ 110.

Count III alleges that the SSA Defendants "unlawfully permitted DOGE Defendants to access and inspect tax return information protected by the Internal Revenue Code, 26 U.S.C. §§ 6103, 7213A, and the Social Security Act, 42 U.S.C. § 1306." *Id.* ¶ 114. According to plaintiffs, this conduct constitutes final agency action under 5 U.S.C. § 704. Therefore, under 5 U.S.C. § 706(2), plaintiffs allege that defendants have "engaged in conduct that is contrary to law, in excess of statutory authority, and arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law . . . ." *Id.* ¶¶ 115, 116.

Count IV alleges that the SSA Defendants "have administered systems containing vast quantities of sensitive personal information without complying with statutorily required security protections" under the Federal Information Security Modernization Act ("FISMA"), 44 U.S.C. §§ 3554(a)(1)–(2), and thus they assert a violation of the APA, 5 U.S.C. § 706(2). *Id.* ¶ 118. Plaintiffs assert that this conduct constitutes a final agency action under 5 U.S.C. § 704 and is arbitrary and capricious under 5 U.S.C. § 706(2).

Count V alleges: "SSA Defendants have disclosed an unfathomable amount of sensitive, personally identifying information about the American public without acknowledging that SSA

was changing its policies, identifying the source of its authority to do so, or providing any analysis whatsoever of why its decision is not arbitrary and capricious, and without considering the consequences, including the reliance interests of Plaintiffs and their members," in violation of 5 U.S.C. § 706(2). *Id.* ¶ 122.

In Count VI, plaintiffs allege *ultra vires* actions by the DOGE Defendants. They assert that, "[i]n directing and controlling the use and administration of Defendant SSA's systems, the DOGE Defendants have breached secure government systems and caused the unlawful disclosure of the personal data of tens of millions of people." *Id.* ¶ 126. And, according to plaintiffs, this constitutes "*ultra vires* actions that injure Plaintiffs by exposing their sensitive, private, and personally identifiable information and increasing the risk of further disclosure of their information." *Id.* ¶ 129.

Count VII asserts that the naming of Leland Dudek as the Acting Commissioner of SSA constitutes a violation of the Appointments Clause of the Constitution, U.S. CONST. art. II, § 2, cl. 2. Specifically, plaintiffs assert that as "Acting Commissioner, Defendant Dudek is exercising significant authority and discretion. He therefore was purporting to act as an officer for purposes of the Appointments Clause." *Id.* ¶ 132. But, they observe that "Defendant Dudek was neither nominated by the President nor confirmed by the Senate. Nor has Congress enacted a law authorizing him to perform the functions and duties of the Commissioner without Senate confirmation." *Id.* ¶ 133. Therefore, plaintiffs posit that Dudek is acting in violation of 42 U.S.C. § 902, *id.* ¶ 134, and his "grant of initial and continued access to SSA systems is thus unlawful and must be invalidated." *Id.* ¶ 135.

At approximately 10:20 p.m. on Friday, March 7, 2025—two weeks after suit was initially filed—plaintiffs filed a "Motion For Temporary Restraining Order, Preliminary Injunction, and/or

5 U.S.C. § 705 stay." ECF 21. The motion is supported by a memorandum (ECF 21-1, collectively the "Motion") and numerous exhibits. *See* ECF 22. Plaintiffs seek a temporary restraining order ("TRO") that, among other things, does the following, ECF 21 at 1–2: (1) enjoins the DOGE Defendants from accessing, using, or disclosing tax "return information, personally identifiable information, or non-anonymized information" housed by the SSA; (2) directs the DOGE Defendants to "disgorge or delete all unlawfully obtained, disclosed, or accessed data"; (3) prohibits the DOGE Defendants from "installing any software on SSA devices" or "accessing, or disclosing any SSA computer or software code"; and (4) enjoins all defendants' "access, inspection, disclosure, or use of any SSA information system," or "data obtained therefrom," for any purpose other than those permitted by the Privacy Act and other applicable laws.

On Monday, March 10, 2025, the Court held a telephone scheduling conference with counsel, on the record. ECF 25. Pursuant to the Scheduling Order that followed (ECF 30), defendants filed an opposition to the Motion on March 12, 2025. ECF 36 ("Opposition"). The Opposition is supported by two exhibits. Plaintiffs replied on March 13, 2025. ECF 39 ("Reply). With the Reply, they submitted additional exhibits. Neither side has challenged the Court's consideration of any of the exhibits.[4]

The Court held a Motion hearing on March 14, 2025, at which argument was presented. ECF 43. I briefly summarize each side's arguments, focusing on the points of contention that are pertinent to resolution of the Motion.

Plaintiffs contend that they have standing to pursue their claims. ECF 39 at 6. They point to "three concrete, particularized, and actual or imminent injuries" suffered by their members: "(1)

[4] In the Motion, the parties never address the Appointments Clause claim in Count VII. Therefore, I shall not do so here.

an invasion of privacy akin to intrusion upon seclusion, (2) exposure to an increased and non-speculative risk of identity theft, and (3) an increased likelihood of disruption in benefit payments." *Id.* at 7. These harms, plaintiffs say, are far more than a "'bare statutory violation'" of the Privacy Act. *Id.* at 8 (citation omitted). And, plaintiffs argue that participation of their individual members is not necessary to establish standing because they seek injunctive relief. *Id.* at 12.

Further, plaintiffs argue that the Court has authority to resolve their APA claims because plaintiffs "clearly challenge" a final agency action, identified as SSA's decision to open its "'data systems to unauthorized personnel'" from DOGE, "'in violation of applicable laws and with disregard for the privacy interests' of millions of Americans." *Id.* at 13 (citation omitted). According to plaintiffs, this constitutes an "agency action" because, *inter alia*, it is "'discrete' and 'circumscribed'", and "a far cry from the types of 'workaday' dealings at issue in the cases Defendants cite." *Id.* at 14 (citation omitted). And, plaintiffs posit that this agency action is "final" because the "'practical effect' of Defendants' decision to grant DOGE personnel access to SSA systems . . . is that unauthorized personnel can view, copy, and analyze extensive PII about Plaintiffs' members." *Id.* at 15. In turn, "[t]hat decision . . . 'determined' DOGE's rights to those data systems and 'determined' Plaintiffs' rights with respect to the privacy of its PII—both of which independently render the decision final agency action." *Id.*

Turning to the TRO elements, plaintiffs argue that they are likely to succeed on the merits of their claims, because defendants' actions "flout" the Privacy Act, the Social Security Act, the Tax Reform Act of 1976 (*i.e.*, the Internal Revenue Code), and SSA's own rules and regulations. ECF 21-1 at 24; *see also id.* at 22–26. In short, they argue that SSA granted DOGE affiliates "nearly unlimited access to systems of records containing sensitive personally identifiable information," without requesting or receiving the consent of plaintiffs' members. *Id.* at 23. And,

according to plaintiffs, the exception in the Privacy Act that permits disclosure of information to an agency's employees who "need" access to it does not apply here. ECF 39 at 18. As plaintiffs put it, *id.*: "Defendants' broad invocations of 'modernization' and 'detecting fraud, waste, and abuse' are simply insufficient to justify the unprecedented level of access provided here."

According to plaintiffs, their members are "irreparably harmed by DOGE's ongoing, illegal access to their sensitive information." ECF 21-1 at 29 (boldface omitted). They highlight that SSA databases contain "among the most sensitive personal data the government has," such as extensive medical information, and some of this information "concerning 'health conditions like HIV or STDs can result in stigma, social isolation, job loss, housing loss, and other harms.'" *Id.* at 29, 30 (citation omitted). In their view, this type of privacy violation "cannot be rectified by money damages down the road." *Id.* at 30. Plaintiffs also argue that their members are irreparably harmed "by the now-increased risk that their information is more easily accessible by bad actors." *Id.* at 31 (boldface omitted). The information that SSA maintains, plaintiffs say, has "'anything a scammer would want to know, to do just about anything a scammer would want to do.'" *Id.* (citation omitted). Finally, plaintiffs argue that the balance of the equities and public interest weigh in favor of issuing a TRO because "'there is a substantial public interest in having governmental agencies abide by the federal laws'" and the "government cannot suffer harm from [a TRO] that merely ends an unlawful action . . . ." *Id.* at 33 (citation omitted).

Defendants maintain that plaintiffs lack standing to pursue their claims. They argue, *inter alia*, that plaintiffs' members have not suffered a concrete injury in fact. ECF 36 at 11. In defendants' view, disclosure of information to government employees cannot qualify as an injury in fact, *id.* at 13, and the alleged increased risk of identity theft and disruption of Social Security payments are too speculative so as to be concrete for purposes of Article III of the Constitution.

Defendants also argue that participation of plaintiffs' individual members is necessary for Counts I and II, which implicate the Privacy Act, and therefore plaintiffs lack standing as to those claims. *Id.* at 14–15.

As to SSA, defendants contend that plaintiffs have failed to identify a final agency action, and therefore plaintiffs' claims are precluded under the APA. *Id.* at 16. In particular, defendants argue that "day-to-day" agency operations are not "agency action" within the meaning of the APA. *Id.* at 17, 19. And, in defendants' view, even if there was an "agency action" here, it is not a "final" one. *Id.* at 19. That is so, according to defendants, because plaintiffs' "identified actions are both tentative and interlocutory in nature"; "no new finalized policy has been implemented"; no existing policy has been "definitively changed"; and "the data access decision alleged has no 'direct and appreciable legal consequences'" for plaintiffs. *Id.* at 19, 20, 21. Further, defendants argued at the hearing that DOGE is not a government agency.

In addition, defendants contend that plaintiffs are not likely to succeed on the merits of their claims. *Id.* at 22. According to defendants, the Privacy Act "does not permit organizations to sue for injunctive relief over a decision to provide access to particular government employees." *Id.* at 23. Even if it did, defendants argue that there is no Privacy Act violation because the members of the DOGE Team working at SSA are employees of SSA, and they are in need of the data that was made accessible to them to perform their duties. *Id.* at 23–24. For similar reasons, defendants contend that there is no violation of the other statutes or regulations at issue. *See id.* at 26–28.

Moreover, defendants contend that plaintiffs cannot show irreparable harm. *Id.* at 31. They largely rehash the same arguments they raised with respect to standing, *i.e.*, that plaintiffs' alleged injuries are not concrete or are too speculative. *Id.* But, they also assert that there is no irreparable

harm because plaintiffs can pursue the recovery of monetary damages under the Privacy Act. *Id.* at 32. Finally, defendants argue that a TRO would "harm" the public interest because it would limit "the President's ability to effectuate the policy choices the American people elected him to pursue", including "identifying fraud, waste, and abuse throughout the federal government." *Id.* at 33.

For the reasons that follow, I shall grant the Motion. A TRO shall issue.

III. Background

A. The Parties

1. Plaintiffs

AFSCME is a "national labor organization and unincorporated membership organization" headquartered in Washington, D.C. ECF 17, ¶ 16. According to the Amended Complaint, "AFSCME is the largest trade union of public employees in the United States, with around 1.4 million members organized into approximately 3,400 local unions, 58 councils, and other affiliates in 46 states, the District of Columbia, and Puerto Rico." *Id.* Of AFSCME's members, "approximately 200,000 are retired public service workers who continue to remain members of AFSCME, participate in its governance, and advocate for fairness, equality, and income security for retired Americans." *Id.*

Alliance is a "grassroots advocacy organization with 4.4 million members headquartered in Washington, D.C." *Id.* ¶ 17. The ARA was founded by the AFL-CIO Executive Council in 2001 and has 40 state alliances, as well as members in every state. *Id.* The Alliance's retiree members include "former teachers, industrial workers, state and federal government workers, construction workers, and community leaders united in the belief that every American deserves a secure and dignified retirement after a lifetime of hard work." *Id.*

AFT is a "national labor organization headquartered in Washington, D.C." *Id.* ¶ 18. It represents "over 1.8 million members who are employed as pre-K through 12th-grade teachers, early childhood educators, paraprofessionals, and other school-related personnel; higher education faculty and professional staff; federal, state, and local government employees; and nurses and other healthcare professionals." *Id.* According to the Amended Complaint, "[a]pproximately 490,000 of AFT's members are retired, and most benefit from programs administered by SSA." *Id.* Plaintiffs assert, *id.*: "Economic and retirement security is at the core of AFT's mission."

As I discuss in more detail, *infra*, each plaintiff has many members for whom SSA holds personal, sensitive information, such as Social Security Numbers ("SSN"), bank account numbers, medical and mental health information, tax information, and home addresses. *See*, *e.g.*, ECF 22-1 (Declaration of Ann Widger, Director of Retirees at AFSCME), ¶¶ 10–13; ECF 22-6 (Declaration of Richard J. Fiesta, Executive Director of Alliance), ¶ 9; ECF 22-8 (Declaration of Bernadette Aguirre, Director of the Retiree Division of AFT), ¶ 8. And, members of each organization are concerned that DOGE's access to this information violates their privacy interests, increases their risk of identity theft, and increases the risk that the benefits to which they are entitled will be delayed or cut off. *See* ECF 22-1, ¶¶ 16, 17, 27, 30, 32; ECF 22-6, ¶¶ 7, 12, 13; ECF 22-8, ¶¶ 12, 13, 15.

2. Defendants

The Social Security Administration is an "independent federal agency," ECF 17, ¶ 19, founded in 1935, during the Great Depression. *Id.* ¶ 28. It was intended to "'give some measure of protection to the average citizen,' particularly those facing 'poverty-ridden old age.'" *Id.* (quoting SOC. SEC. ADMIN., *Presidential Statement on Signing the Social Security Act* (August 14, 1935), https://perma.cc/7RDU-EDWD).

SSA is "the nation's principal benefit-paying agency," ECF 17, ¶ 28, and "manages and administers" several of "the largest federal benefit programs," including the Old-Age, Survivors, and Disability Insurance program ("OASDI") and the Supplemental Security Income program ("SSI"). *Id.* ¶¶ 19, 30. "Collectively, SSA pays over $1.5 trillion to seventy million people—more than one in five Americans—each year." *Id.* ¶ 32 (citing SOC. SEC. ADMIN., *Fact Sheet*, https://perma.cc/595S-B36F). SSA "has roughly 57,000" employees. ECF 39-1 (Supplemental Declaration of Tiffany Flick) ("Flick II Decl."), ¶ 7.

Most of Social Security's beneficiaries are retired. ECF 17, ¶ 31. But, "others receive benefits because they have a qualifying disability; are the spouse (or former spouse) or child of someone who receives or is eligible for Social Security; or are the spouse (or former spouse), child, or dependent parent of a deceased worker.[]" *Id.* (citing SOC. SEC. ADMIN., *Understanding the Benefits* (2025) 2, https://perma.cc/V2MH-VANX). The Agency "pays more benefits to children than any other federal program.[]" ECF 17, ¶ 31 (citing SOC. SEC. ADMIN., *Understanding the Benefits* (2025) 2, https://perma.cc/V2MH-VANX). The benefits SSA provides "lift 22 million people, including over 16 million adults aged sixty-five and over, out of poverty.[]" ECF 17, ¶ 32 (citing Kathleen Romig, *Social Security Lifts More People Above the Poverty Line Than Any Other Program*, CTR. ON BUDGET & POL'Y PRIORITIES (Jan. 21, 2025), https://perma.cc/6U8X-7U9A).

In addition to dispersing funds to eligible beneficiaries, SSA issues Social Security Numbers to "U.S. citizens, permanent residents, and other eligible noncitizens." ECF 17, ¶ 29. To date, more than "450 million" SSNs have been issued. *Id.* SSA also "helps administer" federal programs, such as "Medicare, Medicaid, SNAP, eVerify, and the Help America Vote Act." *Id.* ¶ 33.

"To facilitate its work on behalf of the American public, SSA collects and houses some of the most sensitive, personally identifiable information (including personal health information) of

millions of seniors, working-age adults, and children." *Id.* ¶ 34. By way of example, Form SS-5, "which applicants must submit to SSA to receive a" SSN, "requires applicants to provide their name (including prior names or other names used), place and date of birth, citizenship, ethnicity, race, sex, phone number, and mailing address, as well as their parents' names and [SSNs]."

The Agency also collects a wide range of other personal information, including "driver's license and identification card information, bank and credit card information, birth and marriage certificates, pension information, home and work addresses, school records, immigration and/or naturalization records, health care providers' contact information, family court records, employment and employer records, psychological or psychiatric health records, hospitalization records, addiction treatment records, and tests for, or records about, HIV and AIDS." *Id.* ¶ 35.

Moreover, SSA collects tax and earnings information. *Id.* ¶ 36. In particular, employers submit to SSA a W-3 form each year that shows "total earnings, Social Security wages, Medicare wages, and withholdings for all employees for the previous year." *Id.*

Plaintiffs do not elaborate about required financial contributions paid to Social Security. But, the Court takes notice that retirement benefits are funded by the nation's workforce, through mandatory payment of payroll taxes by both employers and employees. At certain ages, individuals become eligible for retirement benefits, calculated based on work history and earnings. This means that SSA collects the work and earnings history of nearly all working Americans for the entirety of their working lives. *See*, *e.g.*, ECF 22-3 (Declaration of John Doe), ¶ 5 (stating that SSA has 65 years of his employment records); *see also* Social Security Administration, *Understanding the Benefits* (2025), https://www.ssa.gov/pubs/EN-05-10024.pdf.

The Agency is subject to a "panoply of laws" that govern and protect SSA's data systems and the disclosure of information held by SSA. ECF 17, ¶ 39. These include the Privacy Act, the

Social Security Act, the Tax Reform Act of 1976, the Taxpayer Browsing Protection Act, and FISMA. *Id.*

Leland Dudek is the "purported" Acting Commissioner of the SSA. *Id.* ¶ 20. He was selected by President Trump on or about February 16, 2025, after the resignation of Michelle King, then the Acting SSA Commissioner. ECF 1, ¶ 88.[5] Dudek approved the data access to the DOGE Team that is at issue here. *See* ECF 36-1 (Declaration of Russo), ¶ 6.

Michael Russo is the Chief Information Officer of the SSA. ECF 17, ¶ 21. He has served in this role since February 3, 2025. ECF 36-1 (Russo Declaration), ¶ 1. In this role, he is responsible for implementation and management of information technology, and he is "responsible for oversight of grants of permissions [sic] to access SSA systems." *Id.* ¶ 2.

Elon Musk is a "Senior Advisor to the President and the de facto Head of DOGE." ECF 17, ¶ 23. U.S. DOGE Service, previously the U.S. Digital Service,[6] was established by Executive Order 14,158 and renamed as the United States DOGE Service. *Id.* ¶ 24. USDS is part of the Executive Office of the President ("EOP"). *Id.* U.S. DOGE Service Temporary Organization is a "temporary organization also created by Executive Order 14,158 and headed by the U.S. DOGE Service Administrator." *Id.* ¶ 25.

[5] Dudek had previously been a GS-15 employee and a manager in SSA's Office of Program Integrity working on anti-fraud measures. ECF 1, ¶ 89. The SSA placed Dudek on administrative leave after "leadership received reports that Dudek had shared information with nonagency personnel as early as December 2024 and had reportedly pressured career staff to 'help DOGE representatives.'" *Id.* ¶ 90. Dudek reportedly wrote in a now-deleted LinkedIn post, "I confess. I moved contractor money around to add data science resources to my anti-fraud team to examine Direct Deposit Fraud . . . . I confess. I bullied agency executives, shared executive contact information, and circumvented the chain of command to connect DOGE with the people who get stuff done." *Id.*

[6] The United States Digital Service was a technology unit established in 2014 with Congressional appropriations, and housed within the Executive Office of the President.

Amy Gleason is the Acting Administrator of USDS and the U.S. DOGE Service Temporary Organization. *Id.* ¶ 26. She was named to the position on February 25, 2025. *See Citizens for Resp. & Ethics in Washington v. U.S. Doge Serv.* ("*CREW*"), No. 25-CV-511 (CRC), 2025 WL 752367, at *2 (D.D.C. Mar. 10, 2025).

B. Post-Election Period

The presidential election was held on November 5, 2024. Days later, on November 12, 2024, President-elect Trump announced the formation of the "Department of Government Efficiency," with the stated goal "to dismantle Government Bureaucracy, slash excess regulations, cut wasteful expenditures, and restructure Federal Agencies." Colleen Long & Jill Colvin, *Trump says Musk, Ramaswamy will form outside group to advise White House on government efficiency*, AP NEWS (Nov. 12, 2024), https://perma.cc/UW7W-GAQW; *see CREW*, 2025 WL 752367, at *1. Technology moguls Elon Mush and Vivek Ramaswamy were identified as the individuals who were to lead the new department. *Id.*

Musk and Ramaswamy subsequently published an opinion piece in the *Wall Street Journal*, declaring their intent to "advise DOGE at every step to pursue three major kinds of reform: regulatory rescissions, administrative reductions and cost savings." Elon Musk & Vivek Ramaswamy: *The DOGE Plan to Reform Government*, WALL ST. J. (Nov. 20, 2024), https://perma.cc/9TBR-E9ZF. According to Musk and Ramaswamy, DOGE would operate through "embedded appointees" at federal agencies and would identify "thousands" of regulations for repeal by the President. *Id.* In addition, they claimed that DOGE would seek "mass head-count reductions across the federal bureaucracy." *Id.*[7]

[7] Shortly after President Trump's inauguration on January 20, 2025, news reports indicated that Mr. Ramaswamy was no longer involved with DOGE. *See* Thomas Beaumont & Jonathan J. Cooper, *Ramaswamy won't serve on Trump's government efficiency commission as he mulls run*

C. Post-Inauguration Period

1. Executive Order 14,158

Following President Trump's inauguration on January 20, 2025, he wasted no time in creating DOGE. On the day of his inauguration, President Trump issued Executive Order 14,158, Fed. Reg. 8441 (Jan. 20, 2025) ("Order" or "E.O."). It is titled "Establishing and Implementing the President's 'Department of Government Efficiency.'" The 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." *Id.* § 1. The E.O. also renamed the United States Digital Service as the "United States DOGE Service (USDS)" and declared that USDS "shall be established in the Executive Office of the President." *Id.* § (3)(a).[8] In addition, the Order established a "USDS Administrator . . . in the Executive Office of the President" who "shall report to the White House Chief of Staff." *Id.* § 3(b).

In addition, the E.O. creates "a temporary organization known as 'the U.S. DOGE Service Temporary Organization'" that "shall be headed by the USDS Administrator and shall be dedicated to advancing the President's 18-month DOGE agenda." *Id.* The Order states, *id.*: "The U.S. DOGE Service Temporary Organization shall terminate on July 4, 2026."

---

for Ohio governor, AP NEWS (Jan. 20, 2025), https://perma.cc/G8CF-FZFJ. Mr. Ramaswamy has since announced his campaign for governor of Ohio. *See* Ana Faguy & Brandon Drenon, *Vivek Ramaswamy announces run for governor in Ohio*, BBC NEWS (Feb. 25, 2025), https://perma.cc/9E6P-7D74.

[8] The distinctions between DOGE and USDS are not entirely clear. But, for the purpose of this Memorandum Opinion, the terms are largely interchangeable.

Further, the Order provides, *id.* § 3(c): "In consultation with USDS, each Agency Head[9] shall establish within their respective Agencies a DOGE Team of at least four employees, which may include Special Government Employees,[10] hired or assigned within thirty days of the date of this Order. Agency Heads shall select the DOGE Team members in consultation with the USDS Administrator. Each DOGE Team will typically include one DOGE Team Lead, one engineer, one human resources specialist, and one attorney. Agency Heads shall ensure that DOGE Team Leads coordinate their work with USDS and advise their respective Agency Heads on implementing the President's DOGE Agenda."

Section 4 of the Order concerns "Modernizing Federal Technology and Software to Maximize Efficiency and Productivity." *Id.* § 4. It provides, *id.* § 4(a): "The USDS Administrator shall commence a Software Modernization Initiative to improve the quality and efficiency of government-wide software, network infrastructure, and information technology (IT) systems. Among other things, the USDS Administrator shall work with Agency Heads to promote inter-operability between agency networks and systems, ensure data integrity, and facilitate responsible data collection and synchronization."

Relevant here, § 4(b) of the E.O. states: "Agency Heads shall take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to

[9] The Executive Order defines "Agency Head" as "the highest-ranking official of an agency, such as the Secretary, Administrator, Chairman, or Director, unless otherwise specified in this order." Exec. Order. No. 14,158, § 2(b).

[10] A Special Government Employee may be a temporary "officer or employee" who is "retained, designated, appointed, or employed to perform, with or without compensation . . . temporary duties either on a full-time or intermittent basis" for up to 130 days in any 365-day period. 18 U.S.C. § 202(a). They are exempt from some of the ethics rules to which most federal employees are subject. *See* 18 U.S.C. §§ 203, 205, 207–209.

ensure USDS has full and prompt access to all unclassified agency records, software systems, and IT systems. USDS shall adhere to rigorous data protection standards."

2. Executive Order 14,210

On February 11, 2025, President Trump signed an executive order titled "Implementing the President's 'Department of Government Efficiency' Workforce Optimization Initiative." Executive Order 14,210, 90 Fed. Reg. 9669 (Feb. 14, 2025). It states, in part, *id.* § 1: "To restore accountability to the American public, this order commences a critical transformation of the Federal bureaucracy. By eliminating waste, bloat, and insularity, my Administration will empower American families, workers, taxpayers, and our system of Government itself."

Section Three of the order is titled "Reforming the Federal Workplace to Maximize Efficiency and Productivity." Section 3(a) provides: "Pursuant to the Presidential Memorandum of January 20, 2025 (Hiring Freeze), the Director of the Office of Management and Budget shall submit a plan to reduce the size of the Federal Government's workforce through efficiency improvements and attrition (Plan)." Subject to certain exceptions, the Plan requires "that each agency hire no more than one employee for every four employees that [sic] depart, consistent with the Plan and any applicable exemptions and details provided for in the Plan."

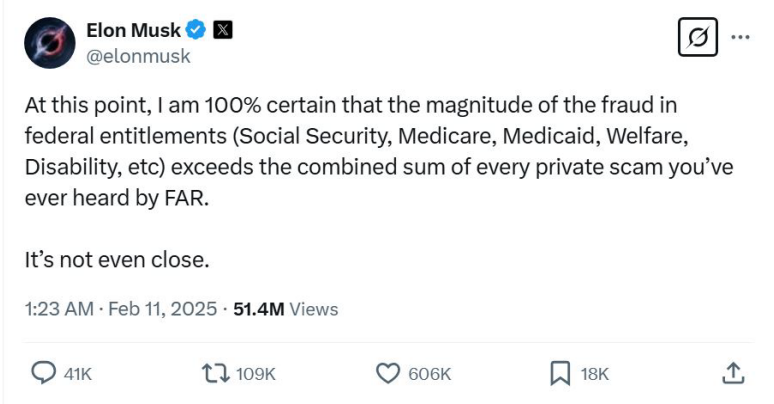
Section 3(b) requires "[e]ach Agency Head" to develop "a data-driven plan, in consultation with its DOGE Team Lead, to ensure new career appointment hires are in highest-need areas." In connection with this directive, the order states: (i) "This hiring plan shall include that new career appointment hiring decisions shall be made in consultation with the agency's DOGE Team Lead, consistent with applicable law"; (ii) "The agency shall not fill any vacancies for career appointments that the DOGE Team Lead assesses should not be filled, unless the Agency Head

determines the positions should be filled"; and (iii) "Each DOGE Team Lead shall provide the [USDS] Administrator with a monthly hiring report for the agency." *Id.* § 3(b)(i)–(iii).

Section 3(c) of the order concerns "Reductions in Force", but does "not apply to functions related to public safety, immigration enforcement, or law enforcement." It states, in part: "Agency Heads shall promptly undertake preparations to initiate large-scale reductions in force (RIFs), consistent with applicable law, and to separate from Federal service temporary employees and reemployed annuitants working in areas that will likely be subject to the RIFs."

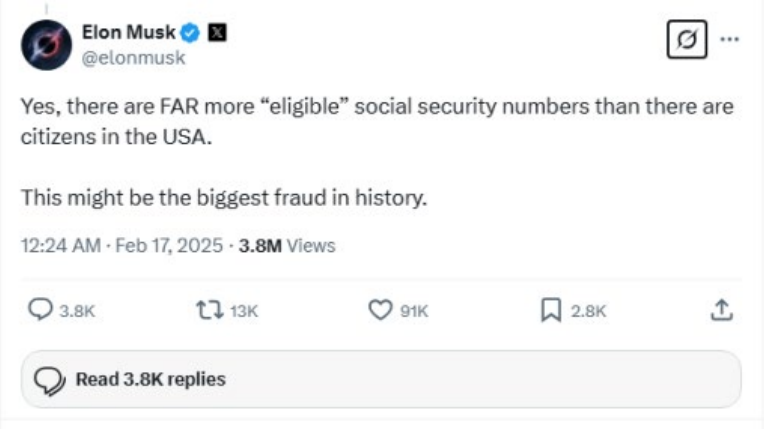
3. SSA in the Crosshairs

According to the Amended Complaint, "President Trump, Elon Musk, and other administration officials have had their sights set on Social Security for the past year . . . ." ECF 17, ¶ 60. For example, President Trump and Mr. Musk have "repeatedly suggested that there is widespread fraud within Social Security, as well as other entitlements." *Id.* ¶ 65. On February 11, 2025, Musk posted on "X", formerly known as Twitter, as follows:



See id. ¶ 66.[11] And, on February 17, 2025, Musk posted on X, *see id.* ¶ 67:

[11] Plaintiffs provided the permalink for all "X" posts.



Further, the Amended Complaint states, *id.* ¶ 68: "On February 17, 2025, White House Press Secretary Karoline Leavitt stated on Fox News that President Trump 'has directed Elon Musk and the DOGE team to identify fraud at the Social Security Administration.[]'" (Quoting Yamiche Alcindor & Raquel Coronell, *Top Social Security official steps down after disagreement with DOGE over sensitive data*, CNN (Feb. 17, 2025), https://perma.cc/9ZLL-VLFH). In particular, Leavitt claimed that Musk and the DOGE Team "'suspect that there are tens of millions of deceased people who are receiving fraudulent Social Security payments.[]'" ECF 17, ¶ 68 (quoting Zachary B. Wolf, *Trump and Musk set their sights on Social Security by spreading rumors*, CNN (Feb. 19, 2025), https://perma.cc/YY7H-8XPA).

On February 19, 2025, Howard Lutnick, the Secretary of the Department of Commerce, stated on Fox News: "'Back in October . . . I flew down to Texas, got Elon Musk [to set up DOGE], and here was our agreement: that Elon was gonna cut a trillion dollars of waste[,] fraud and abuse . . . . We have almost $4 trillion in entitlements, and no one's ever looked at it before. You know Social Security is wrong, you know Medicaid and Medicare are wrong . . . .[]'" ECF 17, ¶ 69 (citation omitted).

Also on February 19, 2025, Dudek "issued a press release endorsing DOGE and stating that DOGE 'is a critical part of President Trump's commitment to identifying fraud, waste, and

abuse.[]'" *Id.* ¶ 70 (quoting SOC. SEC. ADMIN., Press Release, *Statement from Lee Dudek, Acting Commissioner, about Commitment to Agency Transparency and Protecting Benefits and Information* (Feb. 19, 2025), https://perma.cc/W33R-QKEZ). And, on February 22, 2025, President Trump claimed that "tens of millions of Americans are improperly receiving Social Security benefits,[] calling Social Security 'the biggest Ponzi scheme of all time . . . It's all a scam, the whole thing is a scam.[]'" ECF 17, ¶ 71 (citations omitted).

Then, on February 28, 2025, Musk appeared on "'The Joe Rogan Experience'—a widely listened to podcast—and proclaimed that 'a basic search of the Social Security database' indicated '20 million dead people [were] marked as alive' and that 'Social Security is the biggest Ponzi Scheme of all time.'" *Id.* ¶ 72 (citation omitted; alteration in ECF 17). According to plaintiffs, "[t]hat claim is false." *Id.* (citing SOC. SEC. ADMIN., Off. of Inspector Gen., *IG Reports: Nearly $72 Billion Improperly Paid; Recommended Improvements Go Unimplemented* (Aug. 19, 2024), https://perma.cc/WR7T-3KZA).

President Trump continued to deride the SSA. On March 4, 2025, in his "his first speech before a joint session of Congress," President Trump "claimed there to be 'shocking levels of incompetence and probable fraud in the Social Security Program.'" ECF 17, ¶ 73 (citation omitted).

According to the Amended Complaint, "SSA leadership has sought to rework the agency." *Id.* ¶ 74. For example, on February 21, 2025, "SSA announced an 'organizational realignment' of its Office of Analytics, Review, and Oversight, which was responsible for addressing recommendations from external monitoring authorities and overseeing fraud detection." *Id.* ¶ 75 (citing SOC. SEC. ADMIN., Press Release, *Social Security Announces Change to Improve Agency Operations and Strengthen Protections* (Feb. 21, 2025), https://perma.cc/3EC7-KARR). On

February 24, 2025, "SSA announced it was closing the agency's Office of Transformation,[] which was dedicated to the digital modernization of SSA programs and services, including improving the agency's website." ECF 17, ¶ 76 (citation omitted). The next day, "SSA shuttered its Office of Civil Rights and Equal Opportunity,[] which had been tasked with overseeing the agency's civil rights, equal employment, harassment prevention, accommodations, and disability services." *Id.* (citation omitted).

Then, on February 27, 2025, "SSA announced that it was implementing an 'agency-wide organizational restructuring that will include significant workforce reductions'[] and began offering buyouts to agency employees.[]" *Id.* ¶ 77 (citations omitted). The following day, "SSA announced it was reducing the agency's workforce by 7,000 and reducing the number of regional SSA offices from ten to four.[]" *Id.* ¶ 78 (citation omitted). But, the Agency "had already been at a fifty-year staffing low.[]" *Id.* (citation omitted). And, on February 28, 2025, the same day that the Agency announced the significant workforce reduction, "twenty senior SSA leaders announced their resignations.[]" *Id.* ¶ 79 (citation omitted). "During this time," plaintiffs say, "DOGE has also been examining SSA's contracting and other systems, posting various cuts to agency contracts on its 'wall of receipts.[]'" *Id.* ¶ 80 (citation omitted). According to plaintiffs, Dudek "has confirmed: DOGE personnel—or, as he called them, 'outsiders who are unfamiliar with nuances of SSA programs'—are calling the shots.[]" *Id.* ¶ 81 (citing Lisa Rein *et al.*, *DOGE is driving Social Security cuts and will make mistakes, acting head says privately*, Wash. Post (Mar. 6, 2025), https://perma.cc/FYY3-QGRR).

D. Exhibits to the Motion

Plaintiffs submitted ten declarations in support of their Motion, and added two more with their Reply. The defendants have submitted two declarations. I summarize some of the

declarations below, because they provide context for the allegations and are important to the resolution of the Motion.

1. Plaintiffs

Tiffany Flick retired from SSA on or about February 16, 2025, after almost 30 years of service at the Agency, where she held a variety of positions. ECF 22-10 ("Flick Declaration"), ¶¶ 1, 2, 45, 46. Most recently, Flick served as the Acting Chief of Staff to Acting SSA Commissioner Michelle King. *Id.* ¶ 2. She assumed that position after serving as Associate Commissioner for Budget, Facilities and Security in the Office of Hearing Operations. *Id.* Flick provides a blistering account of events that unfolded at SSA from late January through the time of her resignation in mid February 2025.

According to Flick, "[t]he importance of privacy is engrained in every SSA employee from day one" and, "[a]long with accurate and timely payment of benefits, attention to privacy is one of SSA's most fundamental duties." *Id.* ¶ 4. Indeed, she points out that "the first regulation adopted by the Social Security Board" in 1937 "outlined the rules regarding privacy and the disclosure of Social Security records." *Id.* Over time, the Privacy Act and other laws and regulations "have further defined [SSA's] responsibilities to ensure the confidentiality of the information the agency collects and holds." *Id.*; *see also id.* ¶ 5. The SSA's privacy protections and data systems are examined annually to help ensure compliance with security policies. *Id.* ¶ 7.

Flick indicates that every SSA employee is required to sign two documents each year. *Id.* ¶ 6. One is the "Systems Sanctions Policy," outlining sanctions for "unauthorized access or disclosure of SSA data." *Id.* The second document is "an annual reminder" about each employee's "duty to protect personally identifiable information, including when SSA employees need to, as a

part of their job, communicate with constituents outside the agency." *Id.* And, "annual information security training is required for all employees." *Id.*

Moreover, Flick explains that when there is "a need to share data between agencies," the SSA must follow "a detailed process," which involves multiple levels of review, including by the General Counsel's office. *Id.* ¶ 8. She states that it "generally takes months" to complete the process, "to ensure [that] the sharing of information accords with all applicable privacy laws and policies of both SSA and the partner agency." *Id.*

On the morning of January 30, 2025, Flick received a call from Dudek, who was then serving as a senior advisor in the Office of Program Integrity, where he worked on anti-fraud measures. *Id.* ¶ 9. Dudek told Flick that some members of DOGE requested to be on-site immediately and wanted to come to SSA Headquarters that day, and that two DOGE associates, Michael Russo and Scott Coulter, would be working at SSA. *Id.* Given Dudek's status as a mid-level employee, Flick asked him why he was communicating with anyone from DOGE. *Id.* ¶ 10. Dudek indicated that DOGE had reached out to him. *Id.* Flick instructed Dudek to "stand down and not have further contact with anyone from DOGE," and that the Commissioner's Office would handle the issue. *Id.* Flick then reported the call to Acting Commissioner King. *Id.* She states, *id.*: "We began to prepare to onboard Mike Russo, but Scott Coulter had not come to the agency prior to February 16, 2025."

Russo came onsite on January 31, 2025, to begin his onboarding process. *Id.* ¶ 11. He joined the Agency as the CIO on February 3. *Id.* Flick recounts that Russo "introduced himself as a DOGE representative to multiple employees on multiple occasions." *Id.*

According to Flick, as soon as Russo joined the SSA, "he requested to bring in a software engineer named Akash Bobba, who was already assisting DOGE in multiple agencies." *Id.* ¶ 13.

But, "there were challenges with Mr. Bobba's background check that took a few days to resolve." *Id.* On February 10, 2025, the Commissioner's Office and the Office of Human Resources "received phone calls and emails from Mr. Russo, DOGE manager Steve Davis, and people who stated they were associated with the White House's Presidential Personnel Office ('PPO') but who were working out of the Office of Personnel Management ('OPM')." *Id.* ¶ 14. These communications "were about onboarding" Bobba and "giving [him] the equipment and credentials he needed to access SSA data before midnight on February 10." *Id*.

Flick recalls that Russo and Davis "grew increasingly impatient over the course of the evening on February 10," and ultimately Bobba was sworn in "over the phone" at around 9 p.m. that evening, "contrary to standard practice." *Id.* ¶ 16. But, she asserts that "the credentialing process necessary for access to the systems would take longer." *Id.* Flick characterizes the request for same-day access for Bobba as "unprecedented" in her time working "for multiple SSA commissioners across multiple administrations . . . ." *Id.* ¶ 15. Nor did she understand "the apparent urgency with which Mr. Bobba needed to be onboarded and given access to SSA's systems and data," which she described as "highly sensitive." *Id*.

"[W]ith daily pressure" from Russo, the CIO's office "tried to rapidly train" Bobba during the week of February 10, 2025, in order "to get him access to SSA data systems . . . ." *Id.* ¶ 23. This was so that Bobba "could work on a special project for Mr. Russo at DOGE's request," and to enable him to "'audit' any of the work of SSA experts." *Id*.

Flick avers that because Bobba's "security training" was "truncated" and done "outside normal processes," *id.* ¶ 24, she does "not believe Mr. Bobba had a sufficient understanding of the sensitive nature of SSA data or the ways to ensure such data's confidentiality." *Id.* ¶ 25. She adds,

id.: "These are complicated systems with complex policies governing very large programs, and it simply is not possible to become proficient within a matter of a few days."

Also on February 10, 2025, Russo contacted several people, including Dudek, and assembled an "internal team to answer questions from DOGE." *Id.* ¶ 17. Because Russo "did not share many details of the questions or his conversations," Flick had "only limited information" on what the assembled team was doing. *Id.* She asserts: "Mr. Russo never fully disclosed to the Commissioner's office the details on what information DOGE wanted and issues it needed to address." *Id.* at 18. But, she understood that it related to fraud. *Id.* She states, *id.*:

> The information DOGE sought seemed to fall into three categories: (1) untrue allegations regarding benefit payments to deceased people of advanced age; (2) concern regarding single Social Security numbers receiving multiple benefits (which is normal when multiple family members receive benefits through one wage-earner); and (3) payments made to people without a Social Security number.

In Flick's view, these concerns were "invalid and based on an inaccurate understanding of SSA's data and programs." *Id.* ¶ 19. She explains, *id.*:

> As to the first [category], SSA's benefits' file contradicts any claim that payments are made to deceased people as old as 150 years. As to the second issue, DOGE seemed to misunderstand the fact that benefits payments to spouses and dependents will be based on the Social Security number of a single worker. As to the third [category], we were simply never given enough information to understand the source of the concern but had never encountered anything to suggest that inappropriate benefit payments were being made to people without a Social Security number.

Nevertheless, the Commissioner's Office "tried to assist" Russo "in the areas related to potential fraud," including by proposing briefings to help Russo and Bobba "understand the many measures the agency takes to help ensure the accuracy of benefit payments, including those measures that help ensure we are not paying benefits to deceased individuals." *Id.* ¶ 20. But, Flick claims that Russo was "completely focused on questions from DOGE officials based on the general myth of supposed widespread Social Security fraud, rather than facts." *Id.*

According to Flick, "Acting Commissioner King requested that Mr. Russo report to her, as the CIO normally would, but he consistently gave evasive answers about his work." *Id.* ¶ 22. But, Flick believed that Russo "was actually reporting to DOGE." *Id.* For example, according to Flick, Russo had conversations with other agencies about data sharing, including the Departments of Treasury, Education, and Homeland Security, and although data sharing with those agencies is "normal," the "lack of transparency" with Acting Commissioner King "is not." *Id.* ¶ 21.

In the meantime, on February 14, 2025, Dudek was placed on administrative leave. *Id.* ¶ 41. This was based on allegations of inappropriate conduct. *Id.*

Flick also provided details concerning Bobba's access to SSA systems and data. Based on Flick's conversations with experts in the CIO's office, she "determined" that Mr. Bobba would have "anonymized and read-only Numident data using a standard 'sandbox' approach," so that he would not have access to other data. *Id.* ¶ 26. She explained that this approach was consistent with the way that SSA handles "any request to review SSA's records for potential fraud, waste, and abuse by oversight agencies . . . or auditors. . . ." *Id.*

To illustrate, Flick explained that for auditors, SSA ordinarily provides data pertaining to a requested scope of review, which the requester would "outline in detail." *Id.* In response, SSA provides "anonymized or sanitized data needed for the type of review being conducted. If problems were identified, then the individual cases would be located and addressed." *Id.*

According to Flick, the access she had determined to provide Bobba would enable him to answer DOGE's "numident-related questions about fraud," as Flick understood them, without exposing personally identifiable information. *Id.* However, because of the expedited basis on which Bobba was granted access, the anonymized file he was provided had "technical glitches that created problems with the data in the file." *Id.* ¶ 27. Bobba reported the problems on February

15, 2025. *Id.* ¶ 28. At the time, she understood that Bobba was working off-site at OPM, pursuant to a telework agreement for Bobba that Russo had approved. *Id.*

Flick asserts that Bobba's work off-site did not align with the typical requirements of SSA's standard telework agreements, which "state that employees need to work in a private location and should be careful to protect systems and data from unauthorized access." *Id.* ¶ 42. Moreover, Flick states that she understood Bobba was not viewing data to which he was given access "in a secure environment because he was living and working at the Office of Personnel Management around other DOGE, White House, and/or OPM employees." *Id.* ¶ 43. She believes that non-SSA may have had access to the SSA data. *Id.* ¶ 28.

As noted, on February 15, 2025, Bobba experienced technical issues with the anonymized Numident file. *Id.* ¶ 28. Rather than waiting for SSA to resolve the technical issues, Russo obtained "an opinion" from the federal Chief Information Officer, a Presidential appointee housed within the Office of Management and Budget, stating that "he could give Mr. Bobba access to all SSA data." *Id.* ¶ 39. And, Russo and "other DOGE officials demanded that Mr. Bobba be given immediate, full access to SSA data in the Enterprise Data Warehouse ('EDW'), which included Numident files, the Master Beneficiary Record ('MBR') files, and the Supplemental Security Record ('SSR') files." *Id.* ¶ 30.

Moreover, Russo "repeatedly stated that Mr. Bobba needed access to 'everything, including source code.'" *Id.* ¶ 36. When the Commissioner's Office tried to determine why Bobba needed full access to the EDW, Russo was "evasive and never provided the kind of detail that SSA typically requires to justify this level of access." *Id.* ¶ 38.

Flick was contacted by SSA staff, who indicated that Russo requested full access to the EDW for Bobba. *Id.* ¶ 40. She instructed the CIO's office not to provide Bobba with such access

until Russo spoke with Acting Commissioner King. *Id.* Flick explained: "[W]e needed to understand why this level of access was necessary to address the specific questions or issues they were looking at." *Id.* Flick avers that SSA's delay in providing Bobba with full access to SSA's data systems "led to the escalation of tensions" over the weekend of February 15 and 16, 2025. *Id.* ¶ 42.

According to Flick, Acting Commissioner King requested additional details from Russo on "why this level of access was necessary for the work [of] Mr. Bobba . . . ." *Id.* ¶ 44. But, she did not receive an answer. *Id.* Instead, on February 16, 2025, Commissioner King "received an email from the White House noting that the President had named Mr. Dudek as the Acting Commissioner," although Flick understood that Dudek was on administrative leave. *Id.* ¶ 45.

Shortly after Acting Commissioner King informed Flick that Dudek had been elevated to Acting Commissioner, Flick retired. *Id.* ¶ 46. Flick claims that, upon her departure, Dudek gave Bobba and "the DOGE team access to at least the EDW database, and possibly other databases." *Id.* ¶ 47.

According to Flick, EDW contains "extensive information about anyone with a social security number, including names, names of spouses and dependents, work history, financial and banking information, immigration or citizenship status and marital status." *Id.* ¶ 31. The Numident file "contains information necessary for assigning and maintaining social security numbers." *Id.* ¶ 32. The MBR and SSR records "contain detailed information about anyone who applies for, or receives, Title II or Title XVI benefits." *Id.* ¶ 33.[12]

[12] Title II and Title XVI presumably refer to the Social Security disability insurance program (Title II of the Social Security Act) and the Supplemental Security Income (SSI) program (Title XVI of the Act). *See* SOC. SEC. ADMIN., *Disability Evaluation Under Social Security*, https://perma.cc/DGN9-5DPB.

Full access, according to Flick, means different levels of permission, depending on the data system. Full access to the EDW, for example, would provide "read" access to most of SSA's data, which would permit a user to copy and paste, export, screenshot, or otherwise compile data for analysis, but does not permit a user to change data. *Id.* ¶ 34. Full access to other SSA systems may also include "write" access, which would permit a user to change the data in the system. *Id.* ¶ 35.

Notably, Flick avers that SSA "would not provide full access [to] all data systems even to [SSA's] most skilled and highly trained experts." *Id.* ¶ 37. She explains, *id.*: "The scope of each official's access is job-dependent . . . ." Of import, she maintains that the request to give Bobba full access to SSA databases "without justifying the 'need to know' this information was contrary to SSA's long-standing privacy protection policies and regulations . . . ." *Id.* ¶ 43. She asserts: "[N]one of these individuals could articulate why Mr. Bobba needed such expansive access." *Id.*

Flick is "deeply concerned" about DOGE's access to SSA systems, given the potential for inappropriate disclosure, and in light of the "rushed" onboarding and training process for Russo and Bobba. *Id.* ¶ 48. Moreover, Flick states that she is "not confident that DOGE associates have the requisite knowledge and training to prevent sensitive information from being inadvertently transferred to bad actors." *Id.* ¶ 49. For Flick, this "concern is elevated" because Bobba is accessing SSA systems in a location that is not "secure . . . ." *Id.* ¶ 43. Specifically, he was working from OPM offices, where he is "surrounded by employees and officials of other agencies and White House components who have . . . never been vetted by SSA or trained on SSA data,

---

Plaintiffs allege that these particular records include "medical information about anyone" who applies for these benefits. ECF 17, ¶ 86(c). When the Court asked government counsel at the hearing if the SSR records contain detailed health information, he responded: "I don't know the answer to that . . . ." ECF 45 at 24.

systems, or programs." *Id.* ¶ 49; *see also id.* ¶ 43. And, she claims that, because of this "non-secure, off-site access, the protections built into SSA's data systems may not work." *Id.* ¶ 49. For example, Flick states that other individuals "could take pictures of the data, transfer it to other locations, and even feed it into AI programs." *Id.* She adds, *id.*: "In such a chaotic environment, the risk of data leaking into the wrong hands is significant."

Although access to the EDW alone would not affect benefit payment systems, *id.* ¶ 50, Flick "witnessed a disregard for critical processes—like providing the 'least privileged' access based on a 'need to know'—and lack of interest in understanding [SSA] systems and programs." *Id.* When "combined with the significant loss of expertise as more and more agency personnel leave," this gives rise to her apprehension regarding whether "SSA programs will continue to function and operate without disruption." *Id.* She adds, *id.*:

> SSA information technology is made up of an incredibly complex web of systems that are extremely reliable in making Social Security and Supplemental Security Income payments. Some of the system[s] operate based on old programming languages that require specialized knowledge. Such systems are vulnerable to being broken by inadvertent user error if SSA's longstanding development, separation of duties, and information security policies and procedures are not followed. That could result in benefits payments not being paid out or delays in payments. I understand that DOGE associates have been seeking access to the "source code" to SSA systems. If granted, I am not confident that such associates have the requisite understanding of SSA to avoid critical errors that could upend SSA systems.

Moreover, Flick contends that, even if DOGE members have only "read" access to SSA systems, they can, and already have, "used SSA data to spread mis/disinformation about the amount of fraud in Social Security benefit programs." *Id.* ¶ 51. She contends that "fraud is rare, and the agency has numerous measures in place to detect and correct fraud." *Id.*

Flick also submitted a Supplemental Declaration. ECF 39-1. She clarifies that several employees of the DOGE Team accessed SSA data systems prior to having signed, finalized detail

agreements from other agencies. *Id.*¶ 3. And, she claims that this "is not in keeping with agency practice because the agency does not consider a detailee to be an employee of SSA until a detail agreement is signed and finalized." *Id.*

In addition, Flick disputes defendants' assertion that the DOGE Team cannot perform its work with anonymized data. She states, *id.* ¶ 4.

> Normally when analysts or auditors review agency data for possible payment issues, including for fraud, the review process would start with access to high-level, anonymized data based on the least amount of data the analyst or auditor would need to know. If a subset of records within that data are flagged as suspicious, the analyst or auditor would access more granular, non-anonymized data to just that subset of files. In my experience, the type of full, non-anonymized access of individual data on every person who has a social security number or receives benefit[s] from Social Security is unnecessary at the outset of any anti-fraud or other auditing project. While agency anti-fraud experts would have access to the types of data that Mr. Russo describes, they also have significant training and expertise in agency programs and how to read and understand the data from agency systems.

Flick also explains that the "need to know" reason for full, non-anonymized access to SSA data systems articulated in this case are "far from sufficiently detailed to justify granting the level of access the DOGE Team now has." She clarifies that thirty to forty Agency employees have access similar to the DOGE Team, out of "roughly 57,000 employees." *Id.* ¶ 7. However, she contends that these thirty to forty employees are "highly skilled and highly trained." *Id.* She states: "I did not observe any DOGE personnel receiving the 'same level of training' as other SSA employees." *Id.*

In addition to the Flick declarations, plaintiffs have submitted declarations from ten other individuals: (1) Ann Widger, the Director of Retirees at AFSCME (ECF 22-1); (2) Sue Conard, a retiree member of AFSCME (ECF 22-2); (3) "John Doe," a retiree member of AFSCME (ECF 22-3); (4) Tamara Imperiale, a retiree member of AFSCME (ECF 22-4); (5) Charles "CK" Williams, a retiree member of AFSCME (ECF 22-5); (6) Richard J. Fiesta, the Executive Director of ARA

(ECF 22-6);[13] (7) Linda Somo, a member of Alliance (ECF 22-7); (8) Bernadette Aguirre, Director of the Retiree Division of AFT (ECF 22-8); (9) David Gray, a retired member of AFT (ECF 22-9); and (10) Kathleen Romig, the Director of Social Security and Disability Policy at the Center on Budget and Policy Priorities (ECF 39-2).[14]

Widger explains, ECF 22-1, ¶ 8: "AFSCME's mission has long included work to ensure that its members have access to Social Security benefits . . . ." She avers that since DOGE was granted access to SSA systems, retiree members have flooded AFSCME with questions, concerns, and fear about the security of their data, their health information, and their benefits. *Id.* ¶¶ 17, 18, 19, 27, 28, 29, 30. They are fearful that their private information will be compromised and/or that they will lose their benefits. *Id.* ¶ 17.

According to Widger, SSA "has in its systems the private medical information of AFSCME members who are applying for or have applied for disability insurance benefits, including about medical conditions that may carry with them a social stigma." *Id.* ¶ 10. She notes: "Medical records for one individual can exceed 1,000 pages." *Id.* Further, she avers, *id.* ¶ 11: "Required medical information includes all prescription and non-prescription medicines the person is currently taking; all health care providers from whom the individual has sought treatment (doctor, hospital, clinic, psychiatrist, nurse practitioner, therapist, physical therapist or other medical

[13] I note that Fiesta was a declarant on behalf of the Alliance in similar litigation in the District of Columbia. *See Alliance for Retired Americans v. Bessent*, 25-CKK-0313, 2025 WL 740401 (D.D.C. Mar. 7, 2025).

[14] Romig is the Director of Social Security and Disability Policy at the Center on Budget and Policy Priorities. She avers that on March 4, 2025, she attended a meeting held by the SSA at which Dudek spoke. ECF 39-3, ¶¶ 1, 2. According to Romig, the news article published by ProPublica describing what was said at the meeting, "is an accurate representation of that meeting." *Id.* at 3–4. But, the Court does not rely on this news article.

professional) and the medical conditions that were treated and evaluated; all medical tests performed by the listed providers (with the enumerated list including HIV and psychological/IQ tests); and other personal health information." By way of example, Widger explains that, for a "mental health disability claim," information "could include notes from psychotherapists and counseling sessions." *Id.* ¶ 12. Widger states, *id.* ¶ 13: "AFSCME members share this information with SSA because they are required to do so to obtain benefits, and they expect the agency to follow the law and keep that data safe and secure." She adds, *id.* ¶ 12: "Information disclosed concerning health conditions like HIV or other STDs can result in stigma, social isolation, job loss, housing loss, and other harms."

In addition, Widger states: "Many AFSCME Retiree members live on limited incomes of Social Security, personal savings, and a modest pension. Many of our retirees are dependent on their direct deposits to get by in a month. If something were to happen with their data and those payments were compromised, it could mean the difference between being able to afford groceries or going without. We are advising our retiree members to run regular credit reports and to keep a close eye on their bank account activity." *Id.* ¶ 24. Relatedly, Widger states, *id.* ¶ 16: "If DOGE is accessing this data for the purpose of 'rooting out fraud,' it may also mean that AFSCME members have essential benefits slashed incorrectly or inadvertently, as DOGE personnel are not equipped to understand the complex SSA systems."

Widger explains that in December 2024, Congress passed the Social Security Fairness Act ("SSFA"), "which fully repealed the Government Pension Offset and Windfall Elimination Provision." *Id.* ¶ 25. The repeal, for which AFSCME advocated "extensively," permits "more than 3.2 million retired public service workers and their spouses to receive additional Social Security Benefits." *Id.* She claims that many AFSCME members are eligible for these benefits,

but are "concerned about DOGE's access at SSA." *Id.* ¶ 26. Those who are eligible will need to submit new paperwork to SSA, but they are hesitant to "provide new information to SSA" to obtain the benefits. *Id.* She states, *id.* ¶ 27: "AFSCME Retiree members have personally told us they are particularly anxious and stressed because, while outside entities have attempted to steal their identities in the past, they must now worry about threats from inside the SSA itself due to DOGE access." She asserts, *id.* ¶ 19: "The volume of communications and the level of fear within those communications leads us to believe that a significant number of retirees, or soon-to-be retirees, who are members of AFSCME will be chilled from applying for much needed benefits out of fear of their data being compromised."

Further, Widger avers that she has personally been in contact with multiple retiree-members of AFSCME. *Id.* ¶¶ 28, 29, 31. For example, one eighty-year-old retiree told Widger that he was "frightened" about who has access to his medical records. *Id.* ¶ 28. Another retiree participates in the Social Security Disability Program ("SSDI") and told Widger that she is "frightened about her medical information being accessible by those who are targeting SSDI for cuts." *Id.* ¶ 29. Other retirees have contacted AFSCME and conveyed "their fear that DOGE access to their data will . . . exacerbate their exposure to fraud and identity theft." *Id.* ¶ 30. AFSCME retirees are "also fearful of retaliation and reprisals based on their roles as union advocates for protecting Social Security and robust retirement benefits." *Id.* ¶ 31. At least one of these retirees has contacted Widger and expressed his concern that his sensitive, personal data may be exposed in a way that could be used to attack and harass him because of his political views. *Id.*

In sum, Widger states, *id.* ¶ 32: "AFSCME retirees depend on Social Security to provide for themselves and their families. The benefits they receive allow them to stay in their homes, buy groceries, and remain financially independent. Social Security allows them to age with dignity.

They are experiencing great distress over the possibility of their private data being used to put the program at risk of substantial cuts. They are worried about DOGE using their personal data to make the case for significant cuts to the program or train their [artificial intelligence] models for personal profit."

Richard J. Fiesta, the Executive Director of the Alliance, avers, ECF 22-6, ¶ 8: "ARA has members who receive Old-Age, Survivors, and Disability Insurance benefits from the [SSA] and from other programs that require SSA to collect or verify data, such as Medicare." For these programs, Fiesta says, SSA "collects and maintains databases with sensitive personal and financial data about ARA's members. This data includes information such as names, Social Security numbers, medical histories, dates and places of birth, home addresses, contact information, and bank account and financial information, including tax information." *Id.* ¶ 9.

Moreover, ARA members "have submitted sensitive medical information to SSA to receive disability benefits, including health records and doctors' evaluations for physical and mental conditions. This information is both highly personal and, if made public, could cause harm to members whose medical conditions may carry stigma (for example, treatment for mental health issues or HIV/AIDS)." *Id.* ¶ 18. Fiesta explains that members of the Alliance "share this data with SSA because they understand that the agency is committed and legally bound to protect the security of their information." *Id.* ¶ 10. But, he asserts that ARA members "did not consent to have their sensitive personal and financial data shared with DOGE, DOGE personnel (including Elon Musk), or any other unauthorized third parties or government 'departments.' They only consented to have their data used for the purposes disclosed by SSA, and the procedures governing the protection of that data, in the agency's System of Record Notices." *Id.* ¶ 12.

According to Fiesta, each year "millions of elderly Americans are the target of financial fraud and other scams", because they are "particularly attractive targets for scammers." *Id.* ¶ 7. This is so, according to Fiesta, because they are "often trusting and polite; might be less technologically adept; and are more likely to have financial savings, own a home, and have good credit." *Id.* He asserts that "one recent FBI report found" that "scams targeting individuals sixty and older led to at least $3.4 billion in losses in 2023." *Id.*

ARA members, according to Fiesta, are concerned with "bad actors" using SSNs to file fraudulent claims for unemployment benefits or to file fake tax returns. *Id.* ¶ 13. Fiesta posits that DOGE's "unfettered access" to SSA data "immediately increased the risk" that ARA "members' sensitive information will be stolen or misused, whether by DOGE personnel or criminal enterprises that gain access to the now unprotected data." *Id.*

Further, Fiesta states that the access to SSA data provided to DOGE personnel will alter the way "at least some ARA members interact with SSA . . . ." *Id.* ¶ 16. For example "some members will be less likely to submit sensitive information online out of fear that such information will be compromised, and will, in turn, be required to travel to local Social Security offices to deal with routine issues—a task that is being made even more burdensome as SSA continues to shutter such offices, requiring members to travel even further than before." *Id.*

In addition, Fiesta states that "thousands" of ARA members recently became eligible for Social Security benefits under the SSFA. *Id.* ¶ 17. To obtain these benefits, however, "members will now have to apply and submit personal and confidential information about themselves and their spouses to SSA." *Id.* But, in light of DOGE's access to "personal and sensitive information," Fiesta claims that some members may choose not to apply. *Id.* And, according to Fiesta, ARA

members "fear that if DOGE personnel are granted more access to SSA's systems, it may cause the interruption of timely payments, which [ARA] members rely on to live." *Id.* ¶ 15.

Bernadette Aguirre is the Director of the Retiree Division of AFT. ECF 22-8, ¶ 1. She states that AFT members participate in Social Security programs, such as OASDI and "other programs for which SSA collects and verifies data," such as Medicare, Children's Health Insurance Program, and Supplemental Nutrition Assistance Program. *Id.* ¶ 7. She notes that "sensitive information" pertaining to these programs, "including [SSNs], bank account numbers, details of personal finances, and personal information" are "contained in SSA record systems." *Id.* ¶ 8. Aguirre states, *id.* ¶ 9: "AFT members share this information with SSA based on their understanding that the agency is legally obligated—and committed—to keeping their data secure." Further, she posits, *id.* ¶ 11: "I am not aware of any AFT member who has requested or authorized DOGE or its representatives to access their personal data or who has consented to the use of this data for any reason other than for the purposes and through the procedures previously disclosed by SSA in its Systems of Record Notices."

Aguirre avers that she has "personally heard from retiree members who send data to SSA that they are concerned about DOGE's access to the private personal and financial information they have provided to SSA." *Id.* ¶ 12. She states: "AFT and its members are also deeply concerned about the possibility that DOGE, if able to further interfere with SSA data systems, may purposefully or even inadvertently disrupt the timely payment of SSA benefits." *Id.* ¶ 15. And, many AFT members "rely on those benefits to survive, and even one missed check could upend their lives." *Id.*

Moreover, Aguirre raises concerns about an increased risk of identity theft and related harms. *Id.* ¶ 13. In particular, she states, *id.*: "The improper disclosure of [private, personal, and

financial information] to DOGE immediately increased the risk of access by external actors, doxing, identity theft, invasion of personal privacy, and financial crimes against AFT members. That risk deepens every day that DOGE has access to AFT members' data. And feeding members' data into unauthorized or unprotected programs running artificial intelligence—as DOGE has done with data seized from other agencies—enhances these risks."

Individual members of all three plaintiff organizations have also expressed similar concerns with respect to DOGE's access to the personal data maintained by SSA, and have articulated that they expected SSA to maintain the privacy of their personal data. *See, e.g.*, ECF 22-2 (Conard Declaration, retiree member of AFSCME), ¶ 10 ("I always expected that the personal data I have submitted, and continue to submit when required, to SSA would remain private and used only to determine whether I was eligible for benefits, and not to be used for any other purpose. I have never consented for DOGE, Elon Musk or any other third party to have access to my . . . confidential information."); ECF 22-5 (Williams Declaration, AFSCME retiree member), ¶ 6 (same); ECF 23-3 (John Doe Declaration, retiree member of AFSCME), ¶ 6 (same); ECF 22-7 (Somo Declaration, retiree member of ARA), ¶ 9 ("When I shared my sensitive information with SSA, it was my understanding that it would be used for the calculation and receipt of government benefits and remain private.").

David Gray, a retired AFT member, recounts that when he applied for Social Security and Medicare, he provided various types of personal information to SSA, including his "name, bank account information, birth date, and Social Security number." ECF 22-9, ¶¶ 5, 6. He avers, *id.* ¶ 6: "When I applied for these programs, I provided this information to an intake person at my local social security office. I was told that it was going to be extremely confidential—that only specific,

qualified people at SSA would have access to it. I shared this information to receive the benefits that I worked so hard for and expected my information to remain private."

Tamara Imperiale is a 60-year-old retiree member of AFSCME. ECF 22-4, ¶¶ 1, 2. She participates in the SSDI program., *id.* ¶ 4, and "depend[s] on it to live." *Id.* ¶ 8. She explains that she was "forced to retire earlier than [she] would have wanted due to an injury [she] sustained while working . . . ." *Id.* ¶ 3. Imperiale avers, *id.* at 4: "I am now anxious and distressed about the access of my private data by DOGE, which the [SSA] stores and which I have submitted to SSA and continue to submit and update to receive SSDI benefits." She asserts, *id.* ¶ 7: "It was my expectation that the personal information I submitted and continue to submit to SSA—including private health information about my disability—would be used only to determine whether I was eligible for benefits, and not disclosed for any other purpose."

Moreover, plaintiffs' members do not want DOGE personnel to have access to their data. ECF 22-9 (Gray), ¶ 8 ("I do not want these people to have access to my data. It's personal and private."); ECF 22-2 (Conard), ¶¶ 7, 8 (stating that it is "very important" to her that her sensitive personal data remain private and that she is "worried about the access by DOGE . . . ."); ECF 22-4 (Imperiale), ¶ 5 ("As a retiree with a disability, it is very important to me that my data remain private.").

In addition, members of each plaintiff have expressed concern about the increased risk of identity theft. *See, e.g.*, ECF 22-3 (John Doe), ¶ 8 (describing his concern that his data could end up in the hands of scammers); ECF 22-7 (Somo), ¶¶ 7, 8, 11 (outlining similar concerns); ECF 22-9 (Gray), ¶¶ 8, 9 (expressing similar concerns). Somo, an ARA member, explained, ECF 22-7, ¶ 7: 'To receive Social Security and Medicare, my husband and I have both submitted extensive information to SSA. Put simply: SSA knows basically everything about us. They know our names.

They know our finances, including our bank account information. They know where we live. They know our [SSNs]. They know everything that a scammer would want to know, to do just about anything a scammer would want to do." And, several members explained that they are already the target of many scams, given their older ages. *See, e.g.*, *id.* ¶ 8 ("As someone over the age of seventy-five, I am constantly the target of scams.").

Plaintiffs' members also express fear that DOGE access to SSA systems will interfere with their receipt of benefits. *See, e.g.*, ECF 22-9 (Gray), ¶ 8 ("I worry that they will mess with my monthly benefits, which I rely on to live."); ECF 22-2 (Conard), ¶ 9 (expressing concern that "individuals who lack expertise or experience in providing Social Security benefits" she receives will now "be in charge of determining [her] eligibility for benefits and safeguarding [her] private information."); ECF 22-4 (Imperiale), ¶ 6 ("I am worried that unfettered access to my data by DOGE and Elon Musk will put my benefits at risk . . . .").

These members also describe the anxiety they are exprerienicng as a result of DOGE's access to their data. ECF 22-9 (Gray), ¶ 10 ("My anxiety is at an all-time high because of the threats to my personal information and benefits that come from DOGE access to sensitive information like my Social Security information. I will remain anxious until people from DOGE are stopped."); ECF 23-3 (John Doe), ¶ 7 (expressing distress and anxiety about DOGE personnel having access to PII, including "current bank account information and [Doe's] entire work and income history."); ECF 22-4 (Imperiale), ¶ 8 ("I am experiencing great distress over the possibility of my private data being accessed by DOGE and potentially by other individuals . . . .").

Some of plaintiffs' members have also expressed concern about providing information to the SSA to obtain SSFA benefits. For example, Williams is "hesitant to provide additional information" to the SSA to establish his eligibility under the SSFA because of DOGE's access to

this data. *See* ECF 22-5, ¶ 7. And, Somo complains, ECF 22-7, ¶ 12: "Because of DOGE's access to SSA databases, I am going to have to think more carefully about submitting my information to SSA. But at the end of the day, what choice do I have? My ability to live is dependent on supplying information to the government, but I am deeply distressed about the threats I face from the breach of my sensitive information. I am in a Catch-22."

2. Defendants[15]

With their Opposition, defendants have submitted the declarations of Michael Russo (ECF 36-1) and Florence Felix-Lawson (ECF 36-2).

Russo has been the Chief Information Officer of the Office of the Chief Information Officer at the SSA since February 3, 2025. ECF 36-1, ¶ 1. He is a "Non-Career Senior Executive reporting directly to SSA's Acting Commissioner, Leland Dudek." *Id*. Felix-Lawson has been the Deputy Commissioner of Human Resources at the SSA since November 17, 2024. ECF 36-2, ¶ 1. She is a "Career Senior Executive reporting directly to SSA's Acting Commissioner, Leland Dudek." *Id*.

As the CIO, Russo is "responsible for oversight of grants of permissions [sic] to access SSA systems," including to SSA's DOGE Team. ECF 36-1, ¶ 2. Russo explains that, pursuant to E.O. 14,158, "there exists within SSA a 'DOGE [T]eam' responsible for 'implementing the President's DOGE agenda.' *Id.* § 3(c)." *Id.* ¶ 4. He asserts that the "SSA DOGE Team currently consists of ten SSA employees: four SSA special government employees (Employees 1, 4, 6, and 9) and six detailees to SSA from other government agencies and offices (Employees 2, 3, 5, 7, 8,

[15] As noted, defendants have not identified the names of the government employees who have been provided access to the SSA data at issue. In similar cases, however, the defendants have identified government employes by name. *See*, *e.g.*, *See Alliance for Retired Americans*, 2025 WL 740401, at *4–6; *American Federation of Teachers et al.*, 2025 WL 582063, at *2–3.

and 10)." *Id.* ¶ 4. But, "[t]o protect the privacy of these individuals, and to avoid exposing them to threats and harassment," Russo has not provided their names. *Id.*

Russo contends that the "overall goal of the work performed by SSA's DOGE Team is to detect fraud, waste and abuse in SSA programs and to provide recommendations for action to the Acting Commissioner of SSA, the SSA Office of the Inspector General, and the Executive Office of the President." *Id.* ¶ 5. He also describes the particular data access granted to each employee, as well as the stated need for the data, discussed in more detail, *infra*.

As the Deputy Commissioner of Human Resources, Felix-Lawson is "responsible for leading and overseeing human resource services to the agency, including but not limited to appointing and onboarding new personnel, including regular and special government employees and detailees." ECF 36-2, ¶ 2. She repeats some of the information in the Russo Declaration. *Compare*, *e.g.*, ECF 36-1, ¶¶ 4, 7 *with* ECF 36-2, ¶¶ 4, 7.[16] She also provides the dates when each DOGE Team member was brought onto the SSA DOGE Team, as well as additional details regarding their duties, training, and background investigations. I discuss this information in further detail, *infra*.

IV. Overview of the Statutory Framework

A. Administrative Procedure Act

The Administrative Procedure Act provides a cause of action against an "agency" or "an officer or employee thereof" to any "person . . . adversely affected or aggrieved by agency action within the meaning of a relevant statute." 5 U.S.C. § 702. It waives the sovereign immunity of

[16] Russo asserts that Employee 1 was granted access to certain SSA data on February 12, 2025. ECF 36-1, ¶ 7(a). Employee 1 is a SSA special government employee. *Id.* ¶ 7; ECF 36-2, ¶ 5. Yet, according to Felix-Lawson, Employee 1 was not appointed until February 13, 2025. ECF 36-2, ¶ 5. Although the initial disclosure to Employee 1 consisted of anonymized data, it appears that the data was disclosed to Employee 1 before he/she was an SSA employee.

the United States for "relief other than money damages" in such an action. *Id.*; *Medical Imaging & Technology Alliance v. Library of Congress*, 103 F.4th 830, 836 (D.C. Cir. 2024).

The APA provides for judicial review only for a "final agency action for which there is no adequate remedy in a court." *See* 5 U.S.C. § 702; *see also id.* ("A person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof."); *Abbott Labs. v. Gardner*, 387 U.S. 136, 140–41 (1967) (quoting 5 U.S.C. § 704); *Ergon-W. Va., Inc. v. EPA*, 896 F.3d 600, 609 (4th Cir. 2018); *Roland v. U.S. Citizenship & Immigration Servs.*, 850 F.3d 625, 629 n.3 (4th Cir. 2017); *Friends of Back Bay v. U.S. Army Corps of Eng'rs*, 681 F.3d 581, 586 (4th Cir. 2012).

The requirements under the APA are addressed in more detail, *infra*.

B. Privacy Act

The Privacy Act of 1974 (the "Act"), 5 U.S.C. § 552a, "came into being in conjunction with 1974 legislation amending the Freedom of Information Act (FOIA)." *Londrigan v. Fed. Bureau of Investigation*, 670 F.2d 1164, 1169 (D.C. Cir. 1981). The Act "had its genesis in a growing awareness that governmental agencies were accumulating an ever-expanding stockpile of information about private individuals that was readily susceptible to both misuse and the perpetuation of inaccuracies that the citizen would never know of, let alone have an opportunity to rebut or correct." *Id.* It "was designed to provide individuals with more control over the gathering, dissemination, and accuracy of agency information about themselves." *Greentree v. U.S. Customs Serv.*, 674 F.2d 74, 76 (D.C. Cir. 1982). "The Act gives agencies detailed instructions for managing their records and provides for various sorts of civil relief to individuals aggrieved by failures on the Government's part to comply with the requirements." *Doe v. Chao*, 540 U.S. 614, 618 (2004).

In passing the Privacy Act in 1974, Congress made several findings that are noteworthy. Congress proclaimed: "The right to privacy is a personal and fundamental right protected by the Constitution of the United States[.]" Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(4), 88 Stat. 1896. Congress also found: "The privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by federal agencies[.]" *Id.* § 2(a)(1). It also said: "The increasing use of computers and sophisticated information technology, while essential to the efficient operations of the government, has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information[.]" *Id.* § 2(a)(2); *see Tankersley v. Almand*, 837 F.3d 390, 395 (4th Cir. 2016) (same). And, Congress stated: "In order to protect the privacy of individuals identified in information systems maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies." *Id.* § 2(a)(5).

The identified purposes of the Privacy Act were, *inter alia*, "to provide certain safeguards for an individual against an invasion of personal privacy by requiring federal agencies, except as otherwise provided by law, to— . . . (2) permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used or made available for another purpose without his consent; . . . (4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information[.]" *Id.* §§ 2(b)(2), (b)(4).

The Senate Report is also instructive. It states that the purpose of the law "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." Senate Rep. No. 1183, 93d Cong., 2d Sess. (1974). The law was "designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies." *Id.*

To that end, the Act establishes "certain minimum standards for handling and processing personal information maintained in the data banks and systems of the executive branch, for preserving the security of the computerized or manual system, and for safeguarding the confidentiality of the information." *Id.* In particular, it requires "every department and agency to insure, by whatever steps they deem necessary" that, *inter alia*, (1) "they take certain administrative actions to keep account of the employees and people and organizations who have access to the system or file, and to keep account of the disclosures and uses made of the information"; and (2) "they establish rules of conduct with regard to the ethical and legal obligations in developing and operating a computerized or other data system and in handling personal data, and take action to instruct all employees of such duties[.]" *Id.*

Under the Privacy Act, to the extent possible, agencies that collect information directly from individuals are to inform individuals of the purpose and authority for that collection. 5 U.S.C. § 552a(e)(2)–(3). The statute enacts additional requirements for agencies that maintain a "system of records," or maintain the information they collect such that information can be retrieved "by the name of [an] individual or by some identifying number, symbol, or other identifying particular." *Id.* § 552a(a)(5).

For example, agencies must continuously ensure that their systems of records are accurate and complete to the degree "necessary to assure fairness to the individual[s]" whose information has been recorded. 5 U.S.C. § 552a(e)(5). Individuals maintain the right to access and review all records "pertaining to" themselves in the agency's system, *id.* § 552a(d)(1), and to request an amendment if they identify an error. *Id.* § 552a(d)(2). If a request to review relevant records or to correct a record is denied, the individual may bring suit in federal district court and obtain an injunction ordering the agency to comply. *Id.* §§ 552a(d)(3), (g)(1)(A)–(B), (g)(2)–(3). And, if the agency makes an adverse determination as to an individual because of an inaccuracy in its records, the Act allows the individual to sue for damages. *Id.* §§ 552a(g)(1)(C), (g)(2)(4).

Relevant here, the Act prohibits federal agencies from sharing records about individuals, except under certain limited circumstances. It states, in part, 5 U.S.C. § 552a (italics added):

> **(b) Conditions of disclosure.**--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, unless disclosure of the record would be--
>
> **(1)** 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*.

The term "record" is broadly 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[.]" 5 U.S.C. § 552a(a)(4).

The SSA regulations define "disclosure" as "making a record about an individual available to . . . another party." 20 C.F.R. § 401.25. The Privacy Act allows disclosure for "a routine use." 5 U.S.C. § 552a(b)(3). A "routine use" is a use of a record "for a purpose which is compatible with

the purpose for which it was collected." *Id.* § 552a(a)(7). And, each time an agency "establish[es] or revis[es]" a system of records, it must publish a System of Records Notice ("SORN") in the Federal Register detailing, among other things, "each routine use of the records contained in the system, including the categories of users and the purpose of such use." *Id.* § 552a(e)(4)(D).

The Act also provides for private enforcement of violations of the provisions. *See Univ. of California Student Ass'n v. Carter*, No. CV 25-354 (RDM), __ F. Supp. 3d __, 2025 WL 542586, at *2 (D.D.C. Feb. 17, 2025). In particular, it provides a "comprehensive remedial scheme" for injuries arising from the inappropriate dissemination of private information. *Wilson v. Libby*, 535 F.3d 697, 703 (D.C. Cir. 2008). Although individual government employees are not subject to civil suit for damages, an individual "may bring a civil action against the agency" for failure "to comply with any . . . provision of" the Act if the individual suffers "an adverse effect" due to that violation. 5 U.S.C. § 552a(g)(1).

Monetary damages are available only to individuals. *See id.* § 552a(g)(4); *see also Sussman v. U.S. Marshals Serv.*, 494 F.3d 1106, 1122 (D.C. Cir. 2007). Prospective relief is reserved for Amendment or Access Actions. 5 U.S.C. § 552a(g)(2), (3).

The Act also establishes criminal penalties for willful violations of its requirements. *See* 5 U.S.C. § 552a(i). It is a federal crime for any agency officer or employee willfully to disclose a protected record "in any manner to any person or agency not entitled to receive it," *id.* § 552a(i)(1), or to maintain a system of records "without meeting the notice requirements" provided in the Act, *id.* § 552a(i)(2). It is also a federal crime for any person to "request[ ] or obtain[ ] any record concerning an individual from an agency under false pretenses." *Id.* § 552a(i)(3).

C. Internal Revenue Code

Like the Privacy Act, the Internal Revenue Code (the "Code") controls disclosure of individuals' personal information, both within and outside the government.

The Code provides that, as a "general rule," tax "[r]eturns and return information shall be confidential." 26 U.S.C. § 6103(a) (capitalization altered). Moreover, it states, *id.*:

> [E]xcept as authorized by [the Code] . . . no officer or employee of the United States, . . . [and] no other person . . . who has or had access to returns or return information under [various Code provisions providing for that access], shall disclose any return or return information obtained by him in any manner in connection with his service as such an officer or an employee or otherwise or under the provisions of this section.

The Internal Revenue Code provides for private enforcement for any knowing or negligent inspection or disclosure of tax returns or return information. 26 U.S.C. § 7431(a). The Code permits affected taxpayers to bring an action against the United States for damages of $1,000 or more. *Id.* But, the United States is not liable for any inspection or disclosure that the taxpayer requests or that results from "a good faith, but erroneous, interpretation" of the Code's confidentiality requirements. *Id.* § 7431(b).

It is a felony for "any officer or employee of the United States . . . willfully to disclose to any person, except as authorized by [the Code], any return or return information." *Id.* § 7213; *see also* 18 U.S.C. § 1905. And, any federal officer or employee convicted of such a violation "shall, in addition to any other punishment, be dismissed from office or discharged from employment." 26 U.S.C. § 7213(a)(1).

D. Federal Information Security Modernization Act

The Federal Information Security Modernization Act of 2014 is intended to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." 44 U.S.C. § 3551(1). As

Congress recognized in FISMA, "the highly networked . . . Federal computing environment" faces significant "information security risks," including the threat of "unauthorized access, use, disclosure, disruption, modification, or destruction of" government information. 44 U.S.C. §§ 3551, 3553; *see also Kaspersky Lab, Inc. v. United States Dep't of Homeland Sec.*, 909 F.3d 446, 457 (D.C. Cir. 2018).

FISMA requires the SSA to develop, document, and implement an Agency-wide information security program. 44 U.S.C. § 3554(b). The SSA Commissioner is responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of agency information and information systems. *Id.* § 3554(a)(1)(A). FISMA also requires that the Office of the Inspector General, or an independent external auditor as determined by the Inspector General, annually evaluate the SSA's information security program and practices to determine their effectiveness. *Id.* §§ 3555(a)(1) and (b)(1).

V. Standing

The parties vigorously dispute whether plaintiffs have standing to pursue their claims. The matter of standing is a "threshold jurisdictional question." *Dreher v. Experian Info. Sols., Inc.*, 856 F.3d 337, 343 (4th Cir. 2017); *see Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921 (4th Cir. 2022). "The standing inquiry asks whether a plaintiff ha[s] the requisite stake in the outcome of a case . . . ." *Deal v. Mercer Cty Bd. of Educ.*, 911 F.3d 183, 187 (4th Cir. 2018).

A. Legal Standard

It is a bedrock principle that Article III of the Constitution "confines the federal judicial power to the resolution of 'Cases' and 'Controversies.'" *TransUnion LLC v. Ramirez*, 594 U.S. 413, 423 (2021); *see Murthy v. Missouri*, 603 U.S. 43, 56 (2024); *see also Fed. Election Comm'n*

v. Cruz, 596 U.S. 289, 295 (2022) ("The Constitution limits federal courts to deciding 'Cases' and 'Controversies.'") (quoting Art. III, § 2); *Carney v. Adams*, 592 U.S. 53, 58 (2020) (recognizing that Article III requires "a genuine, live dispute between adverse parties . . ."); *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 408 (2013) ("Article III of the Constitution limits federal courts' jurisdiction to certain 'Cases' and 'Controversies.'"); *Lewis v. Cont'l Bank Corp.*, 494 U.S. 472, 477 (1990) (It is fundamental that Article III of the Federal Constitution confines the federal courts to adjudicating "actual, ongoing cases or controversies."); *Opiotennione v. Bozzuto Mgmt. Co.*, __ F.4th __, 2025 WL 678636, at *2 (4th Cir. Mar. 4, 2025) ("Article III of the constitution limits the judicial power of the United States to 'Cases' and 'Controversies.'"); *Laufer v. Naranda Hotels, LLC*, 60 F.4th 156, 161 (4th Cir. 2023) (same).

Indeed, "'no principle is more fundamental to the judiciary's proper role in our system of government than the constitutional limitation of federal-court jurisdiction to actual cases or controversies.'" *Spokeo, Inc. v. Robins*, 578 U.S. 330, 337 (2016) (quoting *Raines v. Byrd*, 521 U.S. 811, 818 (1997)). "Continued adherence to the case-or-controversy requirement of Article III maintains the public's confidence in an unelected but restrained Federal Judiciary . . . . For the federal courts to decide questions of law arising outside of cases and controversies would be inimical to the Constitution's democratic character." *Arizona Christian School Tuition Organization v. Winn*, 563 U.S. 125, 133 (2011); *see DaimlerChrysler Corp. v. Cuno*, 547 U.S. 332, 341 (2006) ("[T]he constitutional limitation of federal-court jurisdiction to actual cases or controversies" is "fundamental to the judiciary's proper role in our system of government[.]").

A federal court may resolve only "a real controversy with real impact on real persons . . . ." *American Legion v. American Humanist Assn.*, 588 U.S. 29, 87 (2019). Relevant here, "Federal courts can only review statutes and executive actions when necessary 'to redress or prevent actual

or imminently threatened injury to persons caused by . . . official violation of law.'" *Murthy*, 603 U.S. at 56 (citing *Summers v. Earth Island Institute*, 555 U.S. 488, 492 (2009)). In the absence of a case or controversy, "the courts have no business deciding [the case] . . . ." *DaimlerChrysler Corp.*, 547 U.S. at 341. Therefore, "federal courts do not adjudicate hypothetical or abstract disputes." *TransUnion*, 594 U.S. at 423. Nor do the courts "exercise general legal oversight" of other government branches, *id.*, or render "advisory opinions." *Id.* at 424. And, when there is no case or controversy, "the court's subject matter jurisdiction ceases to exist . . . . " *S.C. Coastal Conservation League v. U.S. Army Corps. of Eng'rs*, 789 F.3d 475, 482 (4th Cir. 2015); *see Gardner v. GMAC, Inc*., 796 F.3d 390, 395 (4th Cir. 2015) (same).

A "case or controversy exists only when at least one plaintiff" establishes standing to sue. *Murthy*, 603 U.S. at 57 (citing *Raines*, 521 U.S. at 818). Thus, "the doctrine of standing [serves] as a means to implement" the case or controversy requirement. *Laufer*, 60 F.4th at 161; *see TransUnion LLC*, 594 U.S. at 423 ("For there to be a case or controversy under Article III, the plaintiff must have . . . standing."); *Spokeo, Inc.*, 578 U.S. at 338 ("Standing to sue is a doctrine rooted in the traditional understanding of a case or controversy."); *Raines*, 521 U.S. at 818 ("One element of the case-or-controversy requirement" is that a plaintiff must establish standing to sue).

To establish standing under Article III of the Constitution, a plaintiff must satisfy three well established elements: "(i) that he suffered an injury in fact that is concrete, particularized, and actual or imminent; (ii) that the injury was likely caused by the defendant; and (iii) that the injury would likely be redressed by judicial relief." *TransUnion LLC*, 594 U.S. at 423 (citing *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560–561 (1992)); *see Students for Fair Admissions, Inc. v. President & Fellows of Harvard Coll.*, 600 U.S. 181, 199 (2023); *Cruz*, 596 U.S. at 296; *Susan B. Anthony List v. Driehaus*, 573 U.S. 149, 168 (2014); *Clapper*, 568 U.S. at 409; *Fernandez v.*

RentGrow, Inc., 116 F.4th 288, 294 (4th Cir. 2024); *Laufer*, 60 F.4th at 161; *Maryland Shall Issue, Inc. v. Hogan*, 971 F.3d 199, 210 (4th Cir. 2020); *Sierra Club v. U.S. Dep't of the Interior*, 899 F.3d 260, 284 (4th Cir. 2018); *Cahaly v. Larosa*, 796 F.3d 399, 406 (4th Cir. 2015). Requiring a plaintiff to demonstrate these three elements "ensures that federal courts decide only the 'rights of individuals,' and that federal courts exercise 'their proper function in a limited and separated government.'" *TransUnion LLC*, 594 U.S. at 423 (citations omitted).

And, "a plaintiff must demonstrate standing separately for each form of relief sought." *Friends of the Earth, Inc. v. Laidlaw Envtl. Servs. (TOC), Inc.*, 528 U.S. 167, 185 (2000); *see Trans Union LLC*, 594 U.S. at 431 (Plaintiffs "must demonstrate standing for each claim that they press and for each form of relief that they seek (for example, injunctive relief and damages)"); *Garey*, 35 F.4th at 922 (same); *see also MSP Recovery Claims, Series LLC v. Lundbeck LLC*, __ F. 4th __, 2025 WL 610305, at *5 (4th Cir. Feb. 26, 2025); *Episcopal Church in S.C. v. Church Ins. Co. of Vt.*, 997 F.3d 149, 154 (4th Cir. 2021).

In general, "standing in no way depends on the merits of the plaintiff's contention that particular conduct is illegal." *Warth v. Seldin*, 422 U.S. 490, 500 (1975); *see Equity In Athletics, Inc. v. Dep't of Educ.*, 639 F.3d 91, 99 (4th Cir. 2011) ("This court assumes the merits of a dispute will be resolved in favor of the party invoking our jurisdiction in assessing standing . . . ."). The *Laufer* Court said, 60 F.4th at 161: "A district court may limit its standing inquiry to the allegations of the complaint or, if there are any material factual disputes, it may conduct an evidentiary hearing."[17]

[17] At the pleading stage, to establish standing, a plaintiff must "'clearly allege facts demonstrating'" an injury in fact. *Opiotennione*, 2025 WL 678636, at *2 (citation omitted). When standing is challenged on the pleadings, "a court 'accept[s] as valid the merits of [the plaintiff's] legal claims.'" *Laufer*, 60 F.4th at 161 (quoting *Cruz*, 596 U.S. at 298) (alterations in *Laufer*); *see Deal*, 911 F.3d at 187 (stating that the court accepts "'as true all material allegations of the

Here, the plaintiffs are organizations, not individuals. An organization can assert two types of standing. *See Students for Fair Admissions, Inc.*, 600 U.S. at 199; *Warth*, 422 U.S. at 511; *S. Walk at Broadlands Homeowner's Ass'n, Inc. v. OpenBand at Broadlands, LLC*, 713 F.3d 175, 182 (4th Cir. 2013). First, an organization "may have standing in its own right to seek judicial relief from injury to itself and to vindicate whatever rights and immunities the association itself may enjoy." *Warth*, 422 U.S. at 511. And, "in attempting to secure relief from injury to itself the association may assert the rights of its members, at least so long as the challenged infractions adversely affect its members' associational ties." *Id.* Plaintiffs do not claim this type of standing.

It is the second kind of associational standing that has been asserted here. The Supreme Court has recognized that "there may be circumstances where it is necessary to grant a third party standing to assert the rights of another." *Kowalski v. Tesmer*, 543 U.S. 125, 129-30 (2004). "[A]n association may have standing solely as the representative of its members." *Warth,* 422 U.S. at 511; *see Hunt v. Wash. St. Apple Advert. Comm'n*, 432 U.S. 333, 343 (1977) ("[A]n association has standing to bring suit on behalf of its members.").[18]

---

complaint and construe[s] the complaint in favor of the complaining party.'") (citation omitted); *see Button v. Nat'l Bd. of Exam'rs in Optometry, Inc.*, 892 F.3d 613, 620 (4th Cir. 2018).

[18] In *Students for Fair Admissions, Inc.*, 600 U.S. at 199, the Supreme Court referred to this form of standing as "organizational" standing. It seems, however, that this doctrine is typically called "associational" standing. *See*, *e.g.*, *United Food & Com. Workers Union Loc. 751 v. Brown Grp., Inc.*, 517 U.S. 544, 552 (1996); *see also, e.g., Food & Drug Admin. v. Alliance for Hippocratic Med.*, 602 U.S. 367, 398–404 (2024) (Thomas, J., concurring) (repeatedly referring to the doctrine as "associational standing"); *Thole v. U. S. Bank N.A*, 590 U.S. 538, 565 (2020) (Sotomayor, J., dissenting) (referring to the doctrine as "associational standing"); *see also People for Ethical Treatment of Animals, Inc. v. Tri-State Zoological Park of W. Maryland, Inc.*, 843 F. App'x 493, 495 (4th Cir. 2021); Wright & Miller, Federal Practice and Procedure, *Organizational and Associational Standing*, § 8345 (2d ed.) (June 2024 update). Therefore, when referring to a suit filed by an organization on behalf of its members, I shall refer to the form of standing as "associational" standing.

To have so called "representational" or "associational" standing, an organization must demonstrate that (a) "'its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit.'" *Students for Fair Admissions, Inc.*, 600 U.S. at 199 (quoting *Hunt*, 432 U.S. at 343); *see S. Walk at Broadlands Homeowner's Ass'n, Inc.*, 713 F.3d at 184 (same); *Equity In Athletics, Inc.*, 639 F.3d at 99 (same). To show that its members would have standing, an organization "must 'make specific allegations establishing that at least one *identified member* had suffered or would suffer harm.'" *S. Walk at Broadlands Homeowner's Ass'n, Inc.*, 713 F.3d at 184 (quoting *Summers,* 555 U.S. at 498) (emphasis in *S. Walk at Broadlands*).

Injury in fact is the "'[f]irst and foremost' of standing's three elements." *Spokeo, Inc.*, 578 U.S. at 338 (citing *Steel Co. v. Citizens for Better Environment*, 523 U.S. 83, 103 (1998)). "[A]n injury in fact is 'an invasion of a legally protected interest' which is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Opiotennione*, 2025 WL 678636, at *2 (quoting *Lujan*, 504 U.S. at 560) (internal quotation marks omitted); *see also Monsanto Co. v. Geertson Seed Farms*, 561 U.S. 139, 149 (2010) (requiring the plaintiff to allege a "concrete, particularized, and actual or imminent" injury). Therefore, under Article III, "a party invoking the jurisdiction of a federal court [must] seek relief for a personal, particularized injury." *Hollingsworth v. Perry*, 570 U.S. 693, 715 (2013).

"Concreteness and particularity are two different requirements that each must be met." *Opiotennione*, 2025 WL 678636, at *2. "[A]n injury is 'particularized' if it 'affect[s] the plaintiff in a personal and individual way.'" *Id.* (quoting *Spokeo, Inc.*, 578 U.S. at 339) (second alteration in *Opiotennione*; internal quotation marks omitted). A concrete injury is one that is "'real, and not

abstract.'" *TransUnion LLC*, 594 U.S. at 417 (citation omitted). "'[F]inancial harm is a classic and paradigmatic form of injury in fact.'" *Md. Shall Issue, Inc.*, 971 F.3d at 210) (citations omitted).

But, of relevance here, "[v]arious intangible harms can also be concrete." *TransUnion, LLC*, 594 U.S. at 425. The Supreme Court has said, *id.*: "Chief among them are injuries with a close relationship to harms traditionally recognized as providing a basis for lawsuits in American courts. Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." (citing, *inter alia*, *Davis v. Federal Election Comm'n*, 554 U.S. 724, 733 (2008) (disclosure of private information); *Gadelhak v. AT&T Services, Inc.*, 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.) (intrusion upon seclusion)); *see also Krakauer v. Dish Network, L.L.C.*, 925 F.3d 643, 653 (4th Cir. 2019) ("Intrusions upon personal privacy were recognized in tort law and redressable through private litigation.").

"Reputational harm can be a concrete injury, but only if the misleading information was brought to the attention of a third party who understood its defamatory significance." *Fernandez*, 116 F.4th at 292. And, "[t]he fact that an injury may be suffered by a large number of people does not of itself make that injury a nonjusticiable generalized grievance." *Spokeo, Inc.*, 578 U.S. at 339 n.7.

Of import here, the existence of an applicable statute that authorizes legal action under certain circumstances does not automatically create standing. "Congress's determination that a cause of action exists does not displace [the] 'irreducible constitutional minimum' of standing." *Krakauer*, 925 F.3d at 652 (citation omitted). To be sure, Congress is "well positioned to identify intangible harms that meet minimum Article III requirements," so "its judgment is . . . instructive and important." *Id.* at 341. Nevertheless, "plaintiffs cannot establish a cognizable injury simply

by pleading a statutory violation." *Garey*, 35 F.4th at 921; *see Raines*, 521 U.S. at 820 n.3 ("It is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing."). "Private litigation, even if authorized by statute to serve a range of public ends, must vindicate the plaintiffs' interests, rather than serve solely [as] a vehicle for ensuring legal compliance." *Krakauer*, 925 F.3d at 653. Thus, "Article III standing requires a concrete injury even in the context of a statutory violation." *Spokeo, Inc.*, 578 U.S. at 341; *see TransUnion*, 594 U.S. at 426.

When plaintiffs proceed under a statutory cause of action, they can establish a cognizable injury by "identif[ying] a close historical or common-law analogue for their asserted injury," for which courts have "traditionally" provided a remedy. *TransUnion LLC*, 594 U.S. at 424. In other words, "[c]entral to assessing concreteness is whether the asserted harm has a 'close relationship' to a harm traditionally recognized as providing a basis for a lawsuit in American courts—such as physical harm, monetary harm, or various intangible harms . . . ." *Id*. at 417 (quoting *Spokeo, Inc.*, 578 U. S. at 340–41). Although there need not be "an exact duplicate in American history and tradition," a federal court is not entitled to "loosen Article III based on contemporary, evolving beliefs about what kinds of suits should be heard in federal courts." *TransUnion LLC*, 594 U.S. at 424–25.

As discussed, an injury in fact must also be actual or imminent. The concepts of actual, ongoing injury or imminent injury are "disjunctive." *Deal*, 911 F.3d at 189. Ongoing injuries are, "by definition, actual injuries for purposes of Article III standing." *Id.* The imminence requirement is a "'somewhat elastic concept.'" *Clapper*, 568 U.S. at 409 (citation omitted). Its "'purpose'" is "'to ensure that the alleged injury is not too speculative for Article III purposes—that the injury is *certainly* impending.'" *Id.* (citation omitted) (emphasis in *Clapper*).

A threatened injury can also satisfy Article III standing. *Beck v. McDonald*, 848 F.3d 262, 271 (4th Cir. 2017); *see South Carolina v. United States*, 912 F.3d 720, 726 (4th Cir. 2019). However, the Supreme Court has "repeatedly reiterated that 'threatened injury must be *certainly impending* to constitute injury in fact,' and that '[a]llegations of *possible* future injury' are not sufficient." *Clapper*, 568 U.S. at 409 (quoting *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990)) (emphasis and second alteration in *Clapper*).

The second component of standing concerns traceability. This means that the injury in fact must be "fairly traceable to the challenged conduct of the defendant." *Md. Shall Issue*, 971 F.3d at 210. "For an injury to be traceable, 'there must be a causal connection between the injury and the conduct complained of' by the plaintiff." *Air Evac EMS, Inc. v. Cheatham*, 910 F.3d 751, 760 (4th Cir. 2018) (quoting *Lujan*, 504 U.S. at 560). However, "the defendant's conduct need not be the last link in the causal chain . . . ." *Air Evac EMS, Inc.*, 910 F.3d at 760; *see also Lexmark Int'l, Inc. v. Static Control Components, Inc.*, 572 U.S. 118, 134 n.6 (2014) ("Proximate causation is not a requirement of Article III standing . . . ."). "[W]here the plaintiff suffers an injury that is 'produced by [the] determinative or coercive effect' of the defendant's conduct 'upon the action of someone else,'" the traceability requirement is satisfied. *Lansdowne on the Potomac Homeowners Ass'n, Inc. v. OpenBand and Lansdowne, LLC*, 713 F.3d 187, 197 (4th Cir. 2013) (quoting *Bennett v. Spear*, 520 U.S. 154, 169 (1997)).

To satisfy the third element of standing, redressability, a plaintiff "'must show that it is likely, as opposed to merely speculative, that the injury will be redressed by a favorable [judicial] decision.'" *Deal*, 911 F.3d at 189 (quoting *Sierra Club*, 899 F.3d at 284). The "very essence" of the redressability requirement is that "[r]elief that does not remedy the injury suffered cannot bootstrap a plaintiff into federal court." *Steel Co.*, 523 U.S. at 107. But, the "burden imposed by

this requirement is not onerous." *Deal*, 911 F.3d at 189. For example, plaintiffs "'need not show that a favorable decision will relieve [their] every injury.'" *Id.* (citation omitted). "Rather, plaintiffs 'need only show that they personally would benefit in a tangible way from the court's intervention.'" *Id.* (quoting *Sierra Club*, 899 F.3d at 284).

"To determine whether an injury is redressable, a court will consider the relationship between 'the judicial relief requested' and the 'injury' suffered." *California v. Texas*, 593 U.S. 659, 671 (2021) (citation omitted). Notably, the "second and third standing requirements—causation and redressability—are often 'flip sides of the same coin.'" *Food & Drug Admin. v. All. for Hippocratic Med.*, 602 U.S. 367, 380–81 (2024) (quoting *Sprint Commc'ns Co. v. APCC Services, Inc.*, 554 U.S. 269, 288 (2008)). "If a defendant's action causes an injury, enjoining the action or awarding damages for the action will typically redress that injury." *Food & Drug Admin.*, 602 U.S. at 380.

B. The Contentions

Plaintiffs posit, ECF 17, ¶ 89: "SSA has collected and stored extensive personal and financial information about Plaintiffs' members, including their Social Security numbers, names and addresses, taxable income, and contributions to Social Security." Moreover, "many" of their members "have highly sensitive medical information on file with SSA, including members whose medical records may contain information that carries a stigma." *Id.* ¶ 90.

According to plaintiffs, "SSA Defendants are required by law to protect the sensitive personal and financial information that they collect and maintain about individuals from unnecessary and unlawful disclosure." *Id.* ¶ 92. In their view, "[t]he decision to grant DOGE personnel access to the extensive records that SSA maintains—and any future decisions to do so—

without obtaining or even requesting the consent of . . . Plaintiffs' members, violates those requirements and upends the reliance these members had on their data being secure." *Id.* ¶ 94.

In addition, plaintiffs claim, *id.* ¶ 95: "Plaintiffs' members—senior citizens—are also among the most targeted for and vulnerable to scams seeking or using their sensitive financial and medical information." They assert, *id.* ¶ 97: "Defendants' actions have . . . harmed Plaintiffs' members by depriving them of privacy protections guaranteed by federal law and by making their information available for, and subject to, investigation by DOGE and scammers. This harm is exacerbated by the attendant risk that this information, still being improperly disclosed, is more easily accessed and abused by malicious actors."

On the basis of these and other allegations, plaintiffs contend that their members have suffered an injury in fact because they have "three concrete, particularized, and actual or imminent injuries," ECF 39 at 7: "(1) an invasion of privacy akin to intrusion upon seclusion, (2) exposure to an increased and non-speculative risk of identity theft, and (3) an increased likelihood of disruption in benefit payments."

As to the first alleged injury in fact, plaintiffs argue that their members "'obvious[ly]'" have a legitimate expectation of privacy in the information SSA has collected about them, which includes "where they live, what benefits they receive, their medical histories, and their bank information." *Id.* at 8 (citation omitted; alteration in ECF 39). And, in plaintiffs' view, "Defendants' unauthorized disclosure of Plaintiffs' data is, as an objective matter, highly offensive." *Id.*

As to the second alleged injury in fact, plaintiffs argue, *id.*: "An agency's 'failure to adequately secure its databases' creates the sort of 'substantial risk' that constitutes a 'concrete, particularized, and actual injury' for Article III standing." (Quoting *In re U.S. Off. Of Pers. Mgmt.*

Data Sec. Breach Litig., 928 F.3d 42, 54–55 (D.C. Cir. 2019)). Plaintiffs highlight that SSA's "record systems house among the most sensitive PII available" and the "sensitive nature of that data is what led Congress to protect against its misuse . . . ." ECF 39 at 10. Yet, plaintiffs posit, *id.*: "[T]he public record is replete with examples of DOGE personnel at other agencies being reckless with sensitive information.[]" (Citation omitted). Therefore, plaintiffs argue that defendants' "actions 'push the threatened injury of future identity theft beyond the speculative to the sufficiently imminent . . . .'" *Id.* (quoting *Beck*, 848 F.3d at 274).

Plaintiffs also argue that their members are "injured via [the threat of] disruption of life-sustaining benefits payments." *Id.* at 11 (emphasis omitted). According to plaintiffs, defendants' actions increase the likelihood of a disruption in the receipt of benefits on which their members rely "to live." *Id.* They point out that Dudek has "recently admitted that he 'doesn't know' whether DOGE's use of SSA data systems means the agency 'is going to break something'" and that DOGE personnel are 'unfamiliar with the nuances of [the Agency].[]'" *Id.* (citations omitted; alteration in ECF 39). Moreover, SSA employees have stated that "SSA tech systems 'seem to be crashing nearly every day, leading to more delays in serving beneficiaries.[]'" *Id.* (citation omitted). Thus, plaintiffs assert, *id.*: "This is exactly the type of injury that allows Plaintiffs to pursue 'forward-looking, injunctive relief.'" (citation omitted).

In addition, plaintiffs maintain that their individual members need not participate in the litigation. *Id.* at 12. As a general matter, plaintiffs argue that they seek injunctive relief under the APA and, therefore, "both the claim and relief generally do not require the participation of individual members." *Id.* They assert: "[C]ourts have repeatedly permitted groups asserting associational standing to challenge Privacy Act violations." *Id.* at 13 (citing cases).

Defendants insist that plaintiffs lack standing to pursue their claims. ECF 36 at 9. They posit, *id.* at 10: "The standing inquiry is especially rigorous when a plaintiff seeks to enjoin the executive branch . . . ." (Citing *Murthy*, 603 U.S. at 76).[19] Accordingly, defendants urge the Court to "deny Plaintiffs' Motion without further inquiry." ECF 36 at 9.

According to defendants, plaintiffs fail to satisfy "at least prongs one and three of the representational-standing inquiry." ECF 36 at 11. They assert, *id.* at 12: "Plaintiffs' theory of injury-in-fact is that their members have provided various forms of information to SSA with the expectation of confidentiality and privacy, and that Defendants' actions in allowing certain USDS employees to access those records violates members' reasonable expectations." In defendants' view, "[t]hat theory fails" because a statutory violation, "by itself, is not a cognizable Article III injury." *Id.* Moreover, defendants contend, *id.* at 13: "Access to information—if unaccompanied by disclosure of that information—is not a cognizable intangible harm." (Citing cases). In this regard, defendants note, *id.*: "Plaintiffs do not contend that their members were victims of any disclosure of their SSA information to non-government actors." They add, *id*. at 13 n.3: "Even if Plaintiffs were not required to show that their private information was disseminated to the public, the absence of any evidence that the information has been seen outside of SSA and a handful of USDS employees is fatal to their claim of Article III injury."

Further, defendants assert, *id.* at 13: "Were it enough for a plaintiff to establish standing simply by alleging that the holder of her personal information used it in a manner contrary to her subjective expectations, the limits the Supreme Court has carefully established to govern when disclosure of information constitutes injury-in-fact, including the requirement to identify a historical analogue, would be obliterated." They state: "Because USDS's mere access to SSA data

[19] A review of the citation does not reflect the government's assertion.

is not a physical, monetary, or cognizable harm, [plaintiffs] cannot establish injury-in-fact for Article III standing." *Id.* at 13–14.

In addition, defendants argue that plaintiffs fail to establish the "crucial" causation element of standing. *Id.* at 14. They spend little time addressing the issue, but illustrate their point with reference to the identity theft concerns of plaintiffs' members. *Id.* Claiming that plaintiffs have not shown "'a nonspeculative increased risk of identity theft,'" defendants argue that plaintiffs have failed to demonstrate causation as to all claims. *Id.*

As to the third prong of representational standing, defendants contend that the participation of individual members is necessary for the Privacy Act claims (Counts I and II). *Id.* In defendants' view, "a plaintiff cannot satisfy [this] prong of the representational-standing inquiry simply by stating that it seeks only injunctive relief." *Id.* at 15. They point out that the "Privacy Act does not provide for injunctive relief for disclosure claims and requires specific disclosures with respect to specific persons; in other words, the violations themselves are individualized." *Id.* Privacy Act claims, defendants say, "are specific and personal to individual persons." *Id.* They posit: "Plaintiffs must show that neither the claims they brought nor the relief they have sought 'requires the participation of individual members in the lawsuit.'" *Id.* (quoting *S. Walk at Broadlands*, 713 F.3d at 184).

In sum, defendants argue that "[b]ecause the Privacy Act requires 'individualized determinations' to establish violations, the participation of individual members is required—and Plaintiffs lack representational standing." ECF 36 at 15.

C. Analysis

1. Interruption of Benefits

I decline to spill ink on plaintiffs' claim of standing based on a potential interruption of Social Security benefits. This is precisely the abstract, speculative, and hypothetical concern that does not pass muster under Article III.

2. Identity Theft

The heightened concern of plaintiffs' members regarding possible identity theft arising from a potential data breach exposing their personal information, all due to the unfettered access to PII provided by SSA to the DOGE Team, is insufficient to establish standing. This amount to a "one-step removed, anticipatory" concern, *Murthy*, 603 U.S. at 57, for which plaintiffs seek "forward-looking relief." *Id.* at 58. But, "[a]n allegation of future injury may suffice [only] if the threatened injury is certainly impending, or there is a substantial risk that the harm will occur." *Susan B. Anthony List*, 573 U.S. at 158 (internal quotation marks omitted); *see also Murthy*, 603 U.S. at 58. Plaintiffs "must show a substantial risk that, in the near future," they will suffer injury. *Murthy*, 603 U.S. at 44. The allegations here are worrisome, but they do not satisfy this requirement.

I recognize that the case of *New York v. Trump*, 25-JAV-01144, 2025 WL 573771 (S.D.N.Y. Feb. 21, 2025), reaches a different result. There, nineteen states filed suit against President Trump, the U.S. Department of Treasury, and Treasury Secretary Bessent, challenging access to financial and other information provided to members of the DOGE Team by the United States Department of Treasury. *Id.* at *1. The disbursements included funding to state governments for Medicaid, FEMA, education, and foster care programs. *Id.* at *2. And, payment files contained Social Security and bank account numbers as well as federal tax return information.

Id. at *7. The court granted a preliminary injunction that, *inter alia*, enjoined the Treasury Department from granting any DOGE affiliates access to any payment record or payment system containing personally identifiable information and/or confidential financial information of the payees. *Id.* at *27.

Relevant here, the court found that the plaintiff-states had standing to sue. The court said: "Plaintiffs have adequately alleged both past harm in the unauthorized disclosure of the States' confidential financial information to the DOGE Team, *and the risk of future harm*, in the risk of exposure of their confidential information to officials of USDS/DOGE and to the public through potential hacking." *Id.* at *12 (emphasis added). As to future harm, the court explained, *id.*: "Courts have routinely found that plaintiffs have standing to seek injunctive relief where inadequate cybersecurity measures put their confidential information at risk of disclosure."

The court reasoned that there "is a realistic danger that the rushed and ad hoc process that has been employed to date by the Treasury DOGE Team has increased the risk of exposure of the States' information." *Id*. In reaching this conclusion, the court noted that one member of the Treasury DOGE Team was mistakenly granted "'read/write permissions instead of read-only'" permission. *Id.* (citation omitted). As the court put it, *id.*: "The critical sensitivity of the information contained in the [Bureau of the Fiscal Service] payment systems, which includes the PII and confidential information of both the States and millions of their residents, requires more than a band-aid approach to cybersecurity."

The hurried manner in which the Treasury DOGE Team was granted access to Treasury systems mirrors the rushed manner in which at least some members of the SSA DOGE Team were granted access to SSA systems. *See* ECF 22-10 (Flick Decl.), ¶¶ 15, 16, 23, 24, 27, 29, 40, 48 (repeatedly referencing the "rushed nature" of the onboarding and training of Bobba and Russo).

For example, several members of the SSA DOGE Team were granted access to SSA systems before their background checks were completed or their inter-agency detail agreements were finalized. *See* ECF 36-2, ¶¶ 5, 11, 15. Flick also raised concerns regarding Bobba's offsite access to SSA systems, which could increase the risk of the data falling into the hands of unauthorized persons. *See* ECF 22-10, ¶¶ 28, 43, 49.

But, I am guided by *Beck*, 848 F.3d 262. There, the personal information of the plaintiffs was actually compromised because of a data breach. Even so, the Court said "the mere theft" of personal information, "without more, cannot confer Article III standing." *Id.* at 275. It found no Article III injury from the "increased risk of future identity theft . . . ." *Id.* at 267. To obtain Article III standing on these grounds, the Court stated that plaintiffs' allegations must go "beyond the speculative to the sufficiently imminent." *Id.* at 274.

The Supreme Court has "repeatedly reiterated" that "'[a]llegations of *possible* future injury' are not sufficient" and that a "'threatened injury must be *certainly impending* to constitute injury in fact.'" *Clapper*, 568 U.S. at 409 (quoting *Whitmore*, 495 U.S. at 158) (emphasis and second alteration in *Clapper*). At this juncture, I am not prepared to speculate that the actions at issue will result in a data breach, and that a breach will necessarily result in identity theft. This concern is not sufficient to satisfy the demands of Article III.

However, this does not end the inquiry. Plaintiffs also claim that they have standing because their members' injuries are similar to the common-law tort of intrusion upon seclusion. ECF 39 at 7. I turn to address this contention.

3. Intrusion Upon Seclusion

As noted, in *TransUnion*, 594 U.S. at 424, the Supreme Court clarified that plaintiffs challenging a statutory violation can establish standing by "identif[ying] a close historical or

common-law analogue for their asserted injury," for which courts have "traditionally" provided a remedy. The Supreme Court and other courts have explicitly recognized that intrusion upon seclusion is an intangible harm "with a close relationship" to a harm "traditionally recognized as providing a basis for lawsuits in American courts." *TransUnion LLC*, 594 U.S. at 425; *see also Garey*, 35 F.4th at 921; *Gadelhak*, 950 F.3d at 462 (Barrett, J.). And, in the context of related cases involving disclosure of PII by federal agencies, several courts have recently concluded that an injury akin to what plaintiffs allege here has a close relationship to the harm associated with the tort of intrusion upon seclusion. *See Alliance for Retired Americans v. Bessent*, 25-CKK-0313, 2025 WL 740401, at *16 (D.D.C. Mar. 7, 2025); *American Federation of Teachers, et al., v. Bessent, et al.*, 25-DLB-0430, 2025 WL 582063, at *6 (D. Md. Feb. 24, 2025); *cf. New York v. Trump*, 2025 WL 455406, at *12.

"'Intrusion upon seclusion is one of the torts under invasion of privacy.'" *Neal v. United States*, 599 F. Supp. 3d 270, 306 (D. Md. 2022) (quoting *Demo v. Kirksey*, PX-18-00716, 2018 WL 5994995, at *3 (D. Md. Nov. 15, 2018)). The Restatement (Second) of Torts § 652B (1977) (October 2024 update) ("Restatement") defines intrusion upon seclusion 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 privacy, if the intrusion would be *highly offensive to a reasonable person*." (Emphasis added); *see Furman v. Sheppard*, 130 Md. App. 67, 73, 744 A.2d 583, 585 (2000) (Intrusion upon seclusion occurs where there is an "intentional intrusion upon the solitude or seclusion of another or his private affairs or concerns that would be highly offensive to a reasonable person."); *see also Lipscomb v. Aargon Agency, Inc.*, PWG-13-2751, 2014 WL 5782040, at *2 (D. Md. Nov. 5, 2014); *Gamble v. Fradkin & Weber, P.A.*, 846 F. Supp. 2d 377, 383 (D. Md. 2012); *Bailer v. Erie Ins. Exch.*, 344 Md. 515, 525–26,

687 A.2d 1375, 1380-81 (1997); *Mitchell v. Balt. Sun Co.*, 164 Md. App. 497, 522, 883 A.2d 1008, 1022 (2005).

"Conduct that a particular plaintiff finds offensive, but that would not offend a reasonable person, cannot establish intrusion upon seclusion." *Neal*, 599 F. Supp. 3d at 306; *see also Whye v. Concentra Health Servs., Inc.*, ELH-12-3432, 2013 WL 5375167, at *14 (D. Md. Sept. 24, 2013), *aff'd*, 583 Fed. App'x 159 (4th Cir. 2014). Rather, intrusion upon seclusion requires a "'substantial'" intrusion, judged by an objective reasonableness standard; it is irrelevant whether a particular plaintiff subjectively found conduct to be highly offensive. *Whye*, 2013 WL 5375167, at *14 (quoting Restatement § 652B, cmt. d).

"A legitimate expectation of privacy is the touchstone of the tort of intrusion upon seclusion." *Fletcher v. Price Chopper Foods of Trumann, Inc.*, 220 F.3d 871, 877 (8th Cir. 2000). And, "[a]n intrusion upon seclusion claim requires that the matter into which there was an intrusion is entitled to be private and is kept private by the plaintiff." *Barnhart v. Paisano Pubs., LLC*, 457 F. Supp. 2d 590, 593 (D. Md. 2006).

The Restatement provides several useful illustrations pertaining to the tort of intrusion upon seclusion. For example, it explains that an intrusion upon seclusion may occur by an "investigation or examination into [the plaintiff's] private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents." Restatement § 652B cmt. b. And, relevant here, the Restatement contemplates that inspection of certain private records can qualify as intrusion upon seclusion. *See id.* On the other hand, "there is no liability for 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.* cmt. c.

The government argues that the alleged injuries of plaintiffs' members are not comparable to the harm associated with intrusion upon seclusion because their PII has been shared only with other government employees, and not the public. ECF 36 at 13. But, intrusion upon seclusion "does not depend upon any publicity given to the person whose interest is invaded or to his affairs." Restatement § 652B cmt. a (1977). In other words, "[t]he intrusion itself makes the defendant subject to liability, even though there is no publication . . . ." *Id.* § 652B cmt. b.

Moreover, the claim that plaintiffs' members suffered no injury in fact because the protected information was disclosed only to government employees carries no water. The SSA alone has "roughly 57,000" employees. ECF 39-1, ¶ 7. And, more broadly, the federal government is the largest employer in the United States. *Federal Employers*, U.S. DEP'T LABOR, https://perma.cc/RJ3F-XNXN. The harms associated with intrusion on seclusion do not dissipate merely because PII is accessed only by government employees who were not entitled to access the information. *See, e.g.*, *Parks v. U.S. IRS,* 618 F.2d 677, 683 (10th Cir. 1980) (concluding that plaintiffs had standing to sue for a Privacy Act violation, although there was only an intra-agency disclosure, because "plaintiffs are the objects or the subjects of the disclosure and the allegation is that they suffered a personal invasion").[20]

Defendants rely, *inter alia*, on the Supreme Court's decision in *TransUnion, LLC*, 594 U.S. 413, and the Fourth Circuit's decision in *O'Leary v. TrustedID, Inc.*, 60 F.4th 240 (4th Cir. 2023), to support their position.[21]

---

[20] In the case of the government, this means, in theory, that plaintiffs would have no claim if the entire SSA workforce, consisting of thousands of people, obtained access to the PII.

[21] Many of the authorities cited by the government in support of its argument do not involve the tort of intrusion upon seclusion. *See*, *e.g.*, ECF 36 at 12, 13 (citing Restatement (Second) of Torts § 652D (1977) ("Publicity Given to Private Life"); *Hunstein v. Preferred Collection & Mgmt. Servs., Inc.*, 48 F.4th 1236, 1245 (11th Cir. 2022) (en banc) (same); *Dreher v. Experian Info. Sols., Inc.*, 856 F.3d 337, 345 (4th Cir. 2017) (plaintiff proposed no common law analogue

In *TransUnion, LLC*, 594 U.S. 413, a class of 8,185 individuals filed suit against TransUnion, a credit reporting agency, seeking damages for violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681 *et seq*. *Id.* at 417. TransUnion compiled and sold consumer reports, containing personal and financial information, to banks, landlords, and car dealerships "that request information about the creditworthiness of individual consumers." *Id.* at 419. It also used a software product that compared names with individuals listed on the U.S. Treasury Department's Office of Foreign Assets Control ("OFAC"). *Id.* In particular, OFAC maintains a list of "'specially designated nationals'" believed to pose a threat to America's national security, such as terrorists, drug traffickers, and other serious criminals. *Id.* Because it is generally unlawful to transact business with any person on the OFAC list, TransUnion created the "OFAC Name Screen Alert to help businesses avoid transacting with individuals on OFAC's list." *Id.*

The system generated "many false positives," however, as many "law-abiding Americans happen to share a first and last name" with someone on OFAC's list. *Id.* at 420. The named plaintiff, Ramirez, was one of them. When he sought to buy a car at a dealership, his name was flagged as a "potential match" on the OFAC list. *Id.* As a result, the car dealership refused to sell the vehicle to him. *Id.* The plaintiffs filed suit, alleging that TransUnion "failed to use reasonable procedures to ensure the accuracy of their credit files, as maintained internally by TransUnion." *Id.* at 417.[22]

---

for his alleged Fair Credit Reporting Act injury, and the Court could not find one; no discussion of intrusion upon seclusion)).

[22] Two other claims were lodged by all 8,185 class members. *TransUnion, LLC*, 594 U.S. at 418. In those claims, the plaintiffs alleged "formatting defects in certain mailings sent to them by TransUnion." *Id.* However, only the named plaintiff, Ramirez, demonstrated that the alleged formatting errors caused him any concrete harm. *Id.* Therefore, the Court determined that he was the only class member with Article III standing to pursue the formatting defect claims. *Id.*

As to 1,853 members of the class, such as Ramirez, "TransUnion provided misleading credit reports to third-party businesses." *Id.* at 417 But, the "internal credit files of the other 6,332 class members were *not* provided to third-party businesses . . . ." *Id.* (emphasis in *TransUnion*).

To determine whether the class members had standing to recover monetary damages, the Supreme Court assessed "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." *Id.* at 424 (quoting *Spokeo, Inc.*, 578 U.S. at 341 (2016)). The Court had "no trouble" concluding that the 1,853 class members whose credit reports were published to third parties containing OFAC alerts that misleadingly labeled them as potential terrorists, drug traffickers, or serious criminals "suffered a concrete harm that qualifies as an injury in fact." *Id.* at 432. The Court reasoned that the publication to a third party of a credit report bearing a misleading OFAC alert shared a "'close relationship'" to the harm associated with the tort of defamation. *Id.* However, because the credit reports of the remaining 6,332 class members were never disseminated to third parties, they did not suffer concrete harm for purposes of Article III. *Id.* at 433.

The Court explained that "[p]ublication is 'essential to liability' in a suit for defamation." *Id.* at 434 (citation omitted). As the Court put it, *id.*: "[T]here is 'no historical or common-law analog where the mere existence of inaccurate information, absent dissemination, amounts to concrete injury.'" (Citation omitted). Thus, "[t]he mere presence of an inaccuracy in an internal credit file, if it is not disclosed to a third party, causes no concrete harm." *Id.*

The class members advanced an additional contention based on "*risk of future harm.*" *Id.* at 435 (emphasis in *TransUnion*). They argued, *id.*: "[T]he existence of misleading OFAC alerts in their internal credit files exposed them to a material risk that the information would be disseminated in the future to third parties and thereby cause them harm." The Court rejected that

argument as well. Nevertheless, it said, *id.*: "*[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." (Emphasis added). The plaintiffs did not seek injunctive relief, however. And, they did not "factually establish a sufficient risk of future harm to support Article III standing." *Id.* at 437–38. Accordingly, the Court concluded that these class members did not have standing.

The class members also argued for the first time before the Supreme Court that TransUnion "published" their information internally. *Id.* at 434 n.6. The Court stated that the "new argument" was "forfeited" but in any event was unavailing. It reasoned, *id.*: "Many American courts did not traditionally recognize intra-company disclosures as actionable publications for purposes of the tort of defamation." *Id.* Although the government relies on this quote, ECF 36 at 13, the Court's statement pertained to the tort of defamation, not intrusion upon seclusion.

Of significance, *TransUnion* recognizes that, for purposes of standing, a concrete harm can be intangible. *TransUnion*, 594 U.S. at 425. And, it mentioned intrusion upon seclusion as a traditionally recognized harm. *Id*. But, the alleged harm in *TransUnion* was reputational harm, akin to the tort of defamation. And, for class members for whom there was no dissemination of information, there was no harm. The harm did not concern privacy interests stemming from sensitive PII, such as medical records and tax return information.

In *O'Leary*, 60 F.4th 240, the Fourth Circuit considered whether the plaintiff, Brady O'Leary, had standing to bring suit under South Carolina's Financial Identity Fraud and Identity Theft Protection Act, S.C. Code Ann. § 37-20-180 ("SC Act"). *Id.* at 241. The SC Act prohibited "'requir[ing] a consumer to use his social security number or a portion of it containing six digits or more to access an Internet web site, unless a password or unique personal identification number

or other authentication device is also required to access the Internet web site.'" *Id.* (citation omitted; alteration in *O'Leary*).

Equifax, a nonparty to the case, was subject to a data breach. *Id.* Equifax engaged its subsidiary, defendant TrustedID, Inc., "to use TrustedID's website to inform customers whether they were impacted by the data breach." *Id.* The plaintiff visited TrustedID's website to learn whether his data had been compromised. *Id.* The website required O'Leary to enter his six-digit SSN, but it did not use "any other safety precautions." *Id.* After entering his SSN, O'Leary was informed that he was not impacted by Equifax's data breach. *Id.* But, he alleged that TrustedID "shared the six digits of his SSN with Equifax." *Id.*

O'Leary filed suit against TrustedID in state court, "alleging that TrustedID's practice of requiring six digits of consumers' SSNs violated the [SC] Act and South Carolina's common-law right to privacy." *Id.* at 241. The case was removed to federal court under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). *Id.* Thereafter, the plaintiff amended his complaint, adding a negligence claim. *Id.* TrustedID moved to dismiss, pursuant to Fed. R. Civ. P. 12(b)(6). *Id.* While that motion was pending, the plaintiff filed a motion to "Determine Subject Matter Jurisdiction Or, in the Alternative, to Remand." *Id.* at 242. He took no position as to whether he had standing, but the defendant argued that the plaintiff had sufficiently alleged standing. *Id.*

At the hearing, TrustedID referred to the alleged injury as "'an invasion of privacy or intrusion upon seclusion.'" *Id.* (citation omitted). And, O'Leary "said he was injured when TrustedID 'intentionally [took] personal identifying information and monetiz[ed] it in some way.'" *Id.* (citation omitted; alterations in *O'Leary*). The district court determined that O'Leary had alleged "'an intangible concrete *harm* in the manner of an invasion of privacy,' which the court said was 'enough to give [it] subject-matter jurisdiction at this early stage of the case.'" *Id.*

(citations omitted; alteration and emphasis in *O'Leary*). Accordingly, the district court determined that the plaintiff had standing. But, it dismissed his claims pursuant to Fed. R. Civ. P. 12(b)(6). *Id.* The plaintiff appealed only the district court's decision to dismiss the case for failure to state a claim. *Id.*

On appeal, the Fourth Circuit concluded that the plaintiff "alleged only a bare statutory violation and no Article III injury." *Id.* The Court explained, *id.* at 243: "The intangible harm of enduring a statutory violation, standing alone, typically won't suffice under Article III—unless there's separate harm (or a materially increased risk of another harm) associated with the violation." Extrapolating, *inter alia*, from cases involving the Fair and Accurate Credit Transactions Act ("FACTA"), 15 U.S.C. § 1681 *et seq.*, as well as data breach cases, the Fourth Circuit said, *id.* at 244: "Article III excludes plaintiffs who rely on an abstract statutory privacy injury unless it came with a nonspeculative increased risk of identity theft." But, O'Leary had not alleged, "even in a speculative or conclusory fashion," that "entering six digits of his SSN on TrustedID's website has somehow raised his risk of identity theft." *Id.* In sum, the Court determined that "O'Leary relies entirely on a mere procedural violation of a statute, which Article III rejects." *Id.* at 245.

The Court also concluded that O'Leary had not alleged "an injury with a 'close relationship' to a traditional or common-law analog", because "he appears to rely on some abstract privacy interest in his SSN itself." *Id.* (citation omitted). It considered two traditional analogs for intangible harms that confer standing: intrusion upon seclusion and disclosure of private information. *Id.* at 245–46.

The Court defined intrusion upon seclusion as a cause of action "'against defendants who invade[ ] the private solitude of another.'" *Id.* at 245 n.2 (quoting *Gadelhak*, 950 F.3d at 462). It

acknowledged that the Supreme Court in *TransUnion* "mention[ed] intrusion upon seclusion as a traditionally recognized harm that provides a basis for lawsuits in federal court." *O'Leary*, 60 F.4th at 245 (citing *TransUnion*, 594 U.S. at 425). It noted that *TransUnion* cited "as an example then-Judge Barrett's holding in *Gadelhak* that receiving unwanted text messages (which violated the Telephone Consumer Protection Act of 1991) could be a concrete injury in fact, as it closely relates to intrusion upon seclusion." *Id.* at 245 (citing *Gadelhak*, 950 F.3d at 462). And, the Fourth Circuit acknowledged that it, too, had recognized that "violations involving unwanted calls under the Telephone Consumer Protection Act are concrete injuries in fact, based on federal courts' traditional protection of 'privacy interests in the home.'" *O'Leary*, 60 F.4th at 245 (quoting *Krakauer*, 925 F.3d at 653).

However, the Court concluded that O'Leary's alleged injury did not bear a close relationship to intrusion upon seclusion. *O'Leary*, 60 F.4th at 245. Specifically, O'Leary alleged that he "chose to hand over his partial SSN '[i]n exchange for' finding out whether he was impacted by Equifax's data breach." *Id.* (citation omitted; alteration in *O'Leary*). And, the Fourth Circuit said, *id.*: "It's the unwanted intrusion *into the home* that marks intrusion upon seclusion, and O'Leary hasn't pleaded anything that closely relates to that." (Emphasis added).

With respect to disclosure of private information, the Court recognized that it "can be another traditional analog for intangible harms that confer standing[.]" *Id.* at 246 (citing *Davis*, 554 U.S. 733). However, neither party had advanced that argument. *Id.* at 246. The parties' silence on this theory, the Court said, was "likely for good reason." *O'Leary*, 60 F.4th at 246.

The Court reviewed *Davis*, noting that it "held that a self-financed political candidate had standing to challenge a statute that would require him to disclose to the government when he spent more than $350,000 in personal funds on his campaign," because it "implicated the candidate's

privacy of association guaranteed by the First Amendment." *Id.* (citing *Davis*, 554 U.S. at 733, 744). But, the Court determined that O'Leary's "associational rights" were not impacted. It said, 60 F.4th at 246: "And he (voluntarily) disclosed his partial SSN to TrustedID, not to the government." In conclusion, the Court said, *id.*: "O'Leary hasn't adequately pled that he was injured by the alleged statutory violation at all—much less in a way that closely relates to a traditional analog for a federal lawsuit."

Defendants point to the *O'Leary* Court's determination that the tort of intrusion upon seclusion is inapplicable because it is the "unwanted intrusion into the home that marks intrusion upon seclusion." *O'Leary*, 60 F.4th at 245. But, as indicated, the Court also defined intrusion upon seclusion as a cause of action "'against defendants who invade[ ] the private solitude of another.'" *Id.* at 245 n.2 (quoting *Gadelhak*, 950 F.3d at 462). In turn, *Gadelhak* cited the Restatement, which does not limit intrusion upon seclusion to the home.

Gadelhak is instructive. There, in an opinion for the Seventh Circuit authored by then Judge Barrett, the court concluded that "unwanted text messages can constitute a concrete injury-in-fact for Article III purposes." 950 F.3d at 463. In reaching that conclusion, the *Gadelhak* Court observed, *id.* at 462: "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.'" The court reasoned that "irritating intrusions," such as persistent telephone calls and unwanted text messages, "pose the same *kind* of harm that common law courts recognize . . . ." *Id*. at 462–63 (emphasis in original). Of import here, the unwanted text messages did not involve the home. Nevertheless, Judge Barrett wrote, *id.* at 462: "The harm posed by unwanted text messages is analogous to that type of intrusive invasion of privacy", *i.e.*, intrusion on seclusion.

In any event, *O'Leary* is factually distinguishable. Moreover, the government overlooks other Fourth Circuit cases that lend support to the conclusion that invasion of privacy (including the form known as intrusion upon seclusion) is a proper analog here.

In *Garey*, 35 F.4th 917, the Fourth Circuit considered whether plaintiffs had standing to sue for an alleged violation of the Driver's Privacy Protection Act ("DPPA"), 18 U.S.C. § 2721 *et seq*. The statute provides a private cause of action against "'[a] person who knowingly obtains, discloses or uses personal information, from a motor vehicle record,' for an impermissible purpose." *Id.* at 920 (citing 18 U.S.C. § 2724(a)). The defendants, personal injury lawyers, obtained motor vehicle accident reports from North Carolina law enforcement agencies or "private data brokers," *id.* at 919, which contained names and home addresses of the drivers. *Id.* at 919–20. The defendants used the personal information in the reports "to mail unsolicited attorney advertising materials to the drivers involved in those crashes." *Id.* at 920; *see also id.* at 919.

The *Garey* Court determined that plaintiffs' allegation that their "privacy [was] invaded by Defendants' knowingly obtaining his or her name and address from a motor vehicle record for an impermissible purpose in violation of law" constituted a "legally cognizable privacy injury." *Id.* at 922. It reasoned that the alleged harm was "closely related to the invasion of privacy, which has long provided a basis for recovery at common law." *Id.* at 921. Therefore, the Fourth Circuit concluded that the DPPA's private right of action satisfied Article III. *Id.* at 922.[23]

[23] The *Garey* Court also determined that the group of plaintiffs seeking injunctive relief did not have standing because there was no evidence they were subject to imminent or certainly impending harm. *Garey*, 35 F.4th at 923. The Court observed that a plaintiff can meet "'the injury-in-fact requirement for prospective relief' either by demonstrating 'a sufficiently imminent injury in fact' or by demonstrating 'an ongoing injury'. . . ." *Id.* at 922 (quoting, *inter alia*, *Deal*, 911 F.3d at 189). The Court agreed with the district court that plaintiffs did not show that they were "'subject to any imminent harm.'" *Id.* at 922. Specifically, because the plaintiffs "narrowed their case" to the unlawful "obtaining" of protected information, rather than using or disclosing, and the "obtaining of [plaintiffs'] personal information is a *fait* accompli," there was no "ongoing

In reaching its conclusion, the *Garey* Court cited *Krakauer*, 925 F.3d 643. *Krakauer* involved the Telephone Consumer Protection Act of 1991 ("TCPA"), 47 U.S.C. § 227, which, among other things, prohibits telephone calls to residential phone numbers on the national "Do-Not-Call" registry. *Id.* at 648. The TCPA provides a private right of action for violations of the statute. *Id.* at 649. The plaintiffs filed a class action lawsuit, alleging that the defendant's sales representatives "routinely flouted" the TCPA *Id.* at 648. The Fourth Circuit concluded that the private right of action "plainly satisfies the demands of Article III." *Id.* at 653. It said, *id.*: "Our legal traditions . . . have long protected privacy interest in the home." But, more broadly, the Court also said, citing the Restatement: "Intrusions upon personal privacy were recognized in tort law and redressable through private litigation." *Id.*

Moreover, in the context of related cases involving agency disclosures of confidential information to DOGE Teams, at least three federal courts have recently found standing based on the analogs of intrusion upon seclusion or public disclosure of private information.

In *Alliance for Retired Americans*, 2025 WL 740401, Judge Kollar-Kotelly, of the United States District Court for the District Court of Columbia, found that three plaintiff-organizations had standing to sue the Department of Treasury and Treasury Secretary Scott Bessent, among other defendants, on behalf of their members. There, DOGE personnel were provided access to systems of records maintained by the Department of Treasury that contained sensitive and personal information. such as routing and bank account numbers, as well as information about individual credit and debit card numbers. *Id.* at *5–8, *16.

---

or imminent injury." *Id.* at 923. The Court added that the "mere possibility" of a "future 'obtaining' violation cannot support injunctive relief. *Id.*; *see City of Los Angeles v. Lyons*, 461 U.S. 95, 103 (1983) (stating that "past wrongs do not in themselves amount to that real and immediate threat of injury" needed for prospective relief). Here, plaintiffs have alleged an on-going injury, which distinguishes the instant case from *Garey*. *See* ECF 17, ¶¶ 2, 94, 97.

Notably, the court rejected the argument that the plaintiffs lacked standing because the members' information was shared only within the government, and not to the public. The court acknowledged that a "lack of public exposure supports an argument that the harm that Plaintiffs describe is not analogous to the reputational harm caused by defamation." *Id.* at *15. But, it explained that a defendant can be liable for intrusion upon seclusion without any publication. *Id.* at *16. And, the court concluded that the alleged injury of plaintiffs' members—the same one alleged by plaintiffs here—"bears a close relationship to the harm essential to an intrusion upon seclusion at common law." *Id.*

In particular, the court found that the plaintiffs' members had a reasonable expectation of privacy in the records at issue because, *inter alia*, it is "entirely reasonable for [plaintiffs'] members to rely on the explicit statutory protections provided by the Privacy Act and the Internal Revenue Code." *Id.* Further, she found that the intrusion at issue would be highly offensive to a reasonable person, pointing, among other things, to "the sensitivity of the information at issue." *Id.* at *17.

In *American Federation of Teachers et al.*, 2025 WL 582063, Judge Boardman of this Court reached the same conclusion. In particular, Judge Boardman concluded that the plaintiffs, five organizations and six individuals, had standing to sue the Department of Education, among other defendants, because the alleged harm—DOGE affiliates' unauthorized access to sensitive PII of the plaintiffs or their members—resembled the tort of intrusion upon seclusion. *Id.* at *6. The information included, *inter alia*, "bank account numbers; Social Security numbers; dates of birth; physical and email addresses; disability status; income and asset information; marital status; demographic information . . . ." *Id.*

Judge Boardman concluded that the "unauthorized disclosure of this massive amount of personal information can be considered an 'unwanted intrusion into the home that marks intrusion upon seclusion.'" *Id.* (quoting *O'Leary*, 60 F.4th at 246). And, she rejected the argument that the plaintiffs did not have standing because the information was only provided to government employees. *American Federation of Teachers et al.*, 2025 WL 582063, at *6. In doing so, she distinguished the tort of intrusion upon seclusion from the tort of public disclosure of private information. *Id.* She also relied on the purpose of the Privacy Act, which, as noted earlier, includes "'prevent[ing] the kind of illegal, unwise, overbroad, investigation and record surveillance of law abiding citizens produced in recent years from actions of some overzealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies.'" *Id.* (quoting *Doe v. DiGenova*, 779 F.2d 74, 84 (D.C. Cir. 1985)) (alteration in *American Federation of Teachers*).

As discussed earlier, in *New York v. Trump*, 2025 WL 573771, the court granted the requests of nineteen states for a preliminary injunction which, *inter alia*, enjoined the Treasury Department from granting any DOGE affiliates access to any of its payment systems. *Id.* at *27. Relying on the Second Circuit's decision in *Bohank v. Marsh & McLennan Companies, Inc.*, 79 F.4th 276 (2d Cir. 2023), the court found that the plaintiff-states had standing to sue. Specifically, the court reasoned that the plaintiffs adequately alleged "past harm in the unauthorized disclosure of [their] confidential financial information to the DOGE Team . . . ." *New York v. Trump*, 2025 WL 573771, at *12. The court analogized the case to *Bohank*, in which the Second Circuit concluded that "'exposure of [the plaintiff's] private PII to unauthorized third parties' bore a 'close relationship to a well-established common-law analog: public disclosure of private facts.'" *Id.* at *11 (quoting *Bohnak*, 79 F.4th at 285).

Applying the principles gleaned from the cases discussed above to the allegations here, I conclude that the wholesale access to SSA records that the Agency has provided to the DOGE Team is sufficiently analogous to the tort of intrusion upon seclusion. There is an expectation of privacy with respect to the PII. And, the unrestricted access to PII that SSA provided to the DOGE Team, without specified need, and/or without adequate training, detail agreements, and/or background investigations of all DOGE Team members, discussed *infra*, would be highly offensive to an objectively reasonable person.

To be sure, plaintiffs cannot establish a cognizable injury in fact merely by pleading a statutory violation of the Privacy Act. But, the Supreme Court has made clear that the judgment of Congress remains "instructive and important." *Spokeo, Inc.*, 578 U.S. at 341; *see TransUnion LLC*, 594 U.S. at 425 ("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."). By enacting the Privacy Act, the Social Security Act, FISMA, and the Internal Revenue Code, Congress has recognized, in general, that improper access to or disclosure of personally identifiable information—even to government employees—poses a harm to legitimate privacy interests.

Upon review of the tort of intrusion on seclusion, it is clear that plaintiffs' members have expressed that they expected their data, maintained by SSA, to remain private. *See, e.g.*, ECF 22-2 (Conard), ¶ 10 ("I always expected that the personal data I have submitted, and continue to submit when required, to SSA would remain private and used only to determine whether I was eligible for benefits, and not to be used for any other purpose."); ECF 22-5 (Williams), ¶ 6 (same); ECF 22-3 (Doe), ¶ 6 (same); ECF 22-4 (Imperiale), ¶ 5 ("As a retiree with a disability, it is very

important to me that my data remain private."); ECF 22-9 (Gray), ¶¶ 6, 8 (expectation that data would remain "confidential", and data is "personal and private.").

Moreover, the expectation of privacy as to this information is objectively reasonable. "The question of what kinds of conduct will be regarded as a 'highly offensive' intrusion is largely a matter of social conventions and expectations." J. Thomas McCarthy, *The Rights of Publicity and Privacy* § 5.1(A)(2) (1993). In enacting the Privacy Act, concerning the government's collection of personal information, Congress recognized that the "right to privacy is a personal and fundamental right . . . ." Pub. L. No. 93-579, § 2(a)(4), 88 Stat. 1896.

The expectation of privacy shared by plaintiffs' members is objectively reasonable. It is almost self-evident that, in our society, PII, such as SSNs, medical information, and certain financial records, are regarded as private, sensitive, and confidential information.[24] Indeed, in some jurisdictions the disclosure of "medical records amounts to a per se intrusion into seclusion if the records contain sensitive materials." *Sabrowski v. Albani-Bayeux, Inc.*, 124 F. App'x 159, 161 (4th Cir. 2005) (citing *Toomer v. Garrett,* 574 S.E.2d 76 (N.C. Ct. App. 2002)). The enactment of the Health Insurance Portability and Accountability Act ("HIPPA"), 29 U.S.C. § 1181 *et seq*.,

[24] Just as the Court was about to submit this Memorandum Opinion for filing, the news reported that the SSNs of some 200 people were included in the release of files concerning the death of President John F. Kennedy. *See* William Wan, et al., *Social Security Numbers and Other Private Information Unmasked in JFK Files*, WASH. POST (Mar. 19, 2025), https://perma.cc/C4VG-PY9F. The reaction to the disclosure is telling, and underscores the expectation of privacy associated with SSNs. "It's absolutely outrageous," said former Trump campaign lawyer Joseph diGenova, whose information was disclosed. *Id*. Mary Ellen Callahan, former Chief Privacy Officer at the Department of Homeland Security, aptly stated, *id.*: "Social Security is literally the keys to the kingdom to everybody. It's absolutely a Privacy Act violation."

Here, the access to private information includes SSNs, but also other personal data. Although the access was made to the DOGE Team, and not (yet) disseminated publicly, the reaction to the disclosure of SSNs in regard to the Kennedy files supports the conclusion here that there is an expectation of privacy with respect to SSNs.

is a reflection of societal views as to the sanctity of medical information. HIPPA "is the primary federal law which was passed to ensure an individual's right to privacy over medical records." *United States v. Elliott*, 676 F. Supp. 2d. 431, 436 (2009). Although HIPPA does not apply to the government, *see* 45 C.F.R. §§ 160.102, 164.104, the statute speaks to the expectation of privacy in medical records that is engrained in our culture.

The evidentiary "psychotherapist-patient privilege" also illustrates the importance of confidentiality that our society attaches to health matters. The privilege is "'rooted in the imperative need for confidence and trust'" between a physician and patient in regard to discussions concerning health issues. *Jaffee v. Redmond*, 518 U.S. 1, 10 (1996); *see also id.* at 12 (noting that "all 50 States and the District of Columbia have enacted into law some form of psychotherapist privilege."). Some of those kinds of discussions are likely contained in the wide swath of information collected by SSA in certain circumstances. *See* ECF 17 (Widger Decl.), ¶ 12 (medical records can include "notes from psychotherapist and counseling sessions").

The information that SSA holds, such as birth and marriage records, SSNs, tax and earnings records, and health records are typically found in equivalents to "private and personal mail," a "wallet," a "safe," or at home. Restatement § 652B cmt. b. Unauthorized or improper access is a "highly offensive" intrusion. *See Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 710 (D.C. 2009) (stating that "conduct giving rise to unauthorized viewing of personal information such as a plaintiff's Social Security number and other identifying information can constitute an intrusion that is highly offensive to any reasonable person"); *Toomer*, 574 S.E.2d at 90 ("The unauthorized examination of the contents of one's personnel file, especially where it includes sensitive information such as medical diagnoses and financial information, like the unauthorized opening and perusal of one's mail, would be highly offensive to a reasonable person.").

Therefore, I am satisfied that the harm alleged here is akin to the tort of intrusion upon seclusion. *See TransUnion LLC*, 594 U.S. at 424–25 (recognizing that there need not be "an exact duplicate in American history and tradition"). It follows that the invasion of privacy harm alleged by plaintiffs satisfies the injury in fact requirement of Article III.

4. Other Elements of Associational Standing

In addition to injury in fact, the remaining requirements of the first element of associational standing—whether the individual members would have standing to sue in their own right—are also met here. Defendants' actions have caused injury to plaintiffs' members, and the members' injuries would be redressable by judicial relief. *See Lujan*, 504 U.S. at 561; *see also Food & Drug Admin*.. 602 U.S. at 380 ("If a defendant's action causes an injury, enjoining the action or awarding damages for the action will typically redress that injury."); *Massachusetts v. EPA*, 549 U.S. 497, 525 (2007) ("[A] plaintiff satisfies the redressability requirement when he shows that a favorable decision will relieve a discrete injury to himself. He need not show that a favorable decision will relieve his *every* injury.") (cleaned up; emphasis in original). Defendants do not argue otherwise.[25]

As discussed, the second element of associational standing requires that the interests the organization "'seeks to protect are germane to the organization's purpose.'" *Students For Fair Admissions, Inc.*, 600 U.S. at 199 (citation omitted). Plaintiffs posit that among their "organizational goals is ensuring that their members have access to and are able to benefit from well run programs by SSA, making the privacy interests it seeks to protect via this lawsuit germane to its purpose." ECF 21-1 at 21 n.32. Defendants do not dispute this element.

[25] Defendants dispute causation in the context of the alleged injury in fact of an increased risk of identity theft. ECF 36 at 14. Because I do not reach that issue, I need not address defendants' argument.

All three plaintiff-organizations seek to ensure protection of their members to Social Security benefits. ECF 22-1 (Widger Decl.), ¶¶ 7, 8; ECF 22-6 (Fiesta Decl.), ¶ 3; ECF 22-8 (Aguirre Decl.), ¶¶ 3, 5. Each plaintiff has members for whom SSA holds personal, sensitive information, such as bank account numbers, medical information, tax information, and home addresses. ECF 22-1 (Widger Decl.), ¶¶ 10–13; ECF 22-6 (Fiesta Decl.), ¶ 9; ECF 22-8 (Aguirre Decl.), ¶ 8. And, in view of the access provided to the DOGE Team, plaintiffs' members are now subject to an ongoing invasion of privacy, which has made at least some members anxious and distressed, *see, e.g.*, ECF 22-3 (Doe Decl.),¶ 7; ECF 22-4 (Imperiale Decl.), ¶ 8; ECF 22-7 (Somo Decl.), ¶¶ 11, 13; ECF 22-9 (Gray Decl.), ¶ 10, and concerned about pursuing benefits under the SSFA. *See* ECF 22-1 (Widger Decl.), ¶ 26; ECF 22-6 (Fiesta Decl.), ¶ 17; *see also* ECF 22-5 (Williams Decl.), ¶ 7; ECF 22-7 (Somo Decl.), ¶ 12. I am satisfied that the interests plaintiffs seek to protect are "'germane'" to plaintiffs' organizational purposes.

The third element of associational standing requires that "'neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit.'" *Students for Fair Admissions, Inc.*, 600 U.S. at 199 (citation omitted). "'[I]ndividual participation' is not normally necessary when an association seeks prospective or injunctive relief for its members . . . ." *United Food & Com. Workers Union Loc. 751 v. Brown Grp., Inc.*, 517 U.S. 544, 546 (1996) (quoting *Hunt*, 432 U.S. at 343).

Defendants assert that the participation of plaintiffs' individual members is necessary for Counts I and II, which implicate the Privacy Act. ECF 36 at 14. This argument is founded on two primary grounds, *id.* at 15: (1) the Privacy Act does not provide for injunctive relief for disclosure claims; and (2) Privacy Act claims are "specific and personal to individual persons."

Plaintiffs seek declaratory and injunctive relief. In *Warth*, 422 U.S. at 515, the Court distinguished associational standing when "a declaration, injunction, or some other form of prospective relief" is sought, and associational standing when "an association seeks relief in damages for alleged injuries to its members." As to the latter, "whatever injury may have been suffered is peculiar to the individual member concerned, and both the fact and extent of injury would require individualized proof." *Id.* at 515–16. But, as to the former, individual participation is ordinarily not necessary because "it can reasonably be supposed that the remedy, if granted, will inure to the benefit of those members of the association actually injured." *Id.* at 515.

Defendants are correct that the Privacy Act does not provide for injunctive relief for disclosure claims. *See* 5 U.S.C. § 552a(g). However, in *Doe v. Chao*, 435 F.3d 492, 504 n.17 (4th Cir. 2006), the Fourth Circuit indicated in dicta that, pursuant to the APA, a plaintiff may pursue injunctive relief for a disclosure claim under the Privacy Act. And in dicta, the Supreme Court has alluded to the same conclusion. *Doe v. Chao*, 540 U.S. at 619 n.1 ("The Privacy Act says nothing about standards of proof governing equitable relief that may be open to victims of adverse determinations or effects, although it may be that this inattention is explained by the general provisions for equitable relief within the [APA] . . . .").

As to defendants' second argument, this prong of the "associational standing test is best seen as focusing on . . . matters of administrative convenience and efficiency, not on elements of a case or controversy within the meaning of the Constitution." *United Food & Com. Workers Union Loc. 751*, 517 U.S. at 557. As a matter of judicial economy, lawsuits filed by each of plaintiffs' members would be more burdensome on the Court than adjudicating the one case filed by plaintiffs on behalf of their members.

Again, this case involves sweeping access to PII, and the challenged conduct pertains to most if not all of plaintiffs' members, representing masses of people. If plaintiffs' members were to bring suit on their own behalf, the courts would be flooded. And, the challenged conduct would generally implicate the same facts, the same defendants, and the same data systems that were made available to DOGE personnel. Because plaintiffs do not seek monetary damages with respect to their Privacy Act claims, the participation of individual members is not necessary to resolve this case.

Notably, the government has not identified a case where a court concluded that a plaintiff-organization did not have associational standing to assert a Privacy Act claim on the ground that participation of individual members was necessary. But, plaintiffs have identified several cases in which judges have concluded that a plaintiff-organization had standing to bring a Privacy Act claim on behalf of its members. ECF 39 at 14 (citing, *inter alia*, *Democratic Party of Virginia v. Brink*, 599 F. Supp. 3d 346, 356 (E.D. Va. 2022); *Nat'l Ass'n of Letter Carriers, AFL-CIO v. U.S. Postal Serv.*, 604 F. Supp. 2d 665, 671–72 (S.D.N.Y. 2009)).

In sum, I conclude that plaintiffs have standing to pursue their claims.[26]

VI. APA Claims[27]

Plaintiffs primarily pursue claims under the APA. *See* Counts I, III, IV, V. They contend that SSA's conduct is unlawful, arbitrary, and capricious because SSA is "sharing the public's data without even acknowledging the seismic shift in agency policy." ECF 21-1 at 26.

[26] I express no opinion as to whether plaintiffs have standing to pursue their Appointments Clause claim. That issue has not been raised by either side.

[27] I incorporate here the statutory overview set forth earlier.

Defendants counter that plaintiffs' APA claims fail for three main reasons: (1) plaintiffs fail to identify a final agency action subject to judicial review, (2) plaintiffs have no right to interfere with the day-to-day operations of the Agency, and (3) plaintiffs have an adequate remedy at law available to them under the Privacy Act if, in fact, a violation has occurred.

A. Judicial Review of APA Claims

Section 702 of the APA provides, in part: "A person suffering legal wrong because of agency action, or adversely affected or aggrieved by agency action within the meaning of a relevant statute, is entitled to judicial review thereof." 5 U.S.C. § 702; *see also id.* § 794 (permitting review of "Agency action made reviewable by statute and final agency action for which there is no other adequate remedy in a court").

"The APA establishes a 'basic presumption of judicial review' of agency action." *Lovo v. Miller*, 107 F.4th 199, 205 (4th Cir. 2024) (quoting *Lincoln v. Virgil*, 508 U.S. 182, 190 (1993) (internal quotation marks and citation omitted)); *see Weyerhaeuser Co. v. U.S. Fish & Wildlife Serv.*, 586 U.S. 9, 22 (2018) ("The Administrative Procedure Act creates a basic presumption of judicial review [for] one 'suffering legal wrong because of agency action.'") (citation and some internal quotations omitted; alteration in *Weyerhaeuser*); *see also Casa de Maryland v. U.S. Dep't of Homeland Sec.*, 924 F.3d 684, 697 (4th Cir. 2019); *Speed Mining, Inc. v. Fed Mine Safety & Health Review Comm'n*, 528 F.3d 310, 316 (4th Cir. 2008). The presumption of judicial review "may be rebutted only if the relevant statute precludes review, 5 U.S.C. § 701(a)(1), or if the action is 'committed to agency discretion by law,' § 701(a)(2)." *Weyerhaeuser Co.*, 586 U.S. at 23; *see Gonzalez v. Cuccinelli*, 985 F.3d 357, 366 (4th Cir. 2021). The latter exception is read "quite narrowly." *Weyerhaeuser Co.*, 586 U.S. at 23; *accord Citizens to Pres. Overton Park, Inc. v. Volpe*, 401 U.S. 402, 410 (1971), *abrogated by Califano v. Sanders*, 430 U.S. 99 (1977). This

applies "in those rare instances where 'statutes are drawn in such broad terms that in a given case there is no law to apply.'" *Id.* (quoting *Lincoln*, 508 U.S. at 191); *see also Heckler v. Chaney*, 470 U.S. 821, 830 (1985) (judicial review is unavailable if the statute provides "no judicially manageable standards . . . for judging how and when an agency should exercise its discretion"); *see also Speed Mining, Inc.*, 528 F.3d at 317.

"The APA provides that a reviewing court is bound to 'hold unlawful and set aside agency action' for certain specified reasons, including whenever the challenged act is 'arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law.'" *Friends of Back Bay*, 681 F.3d at 586–87 (quoting 5 U.S.C. § 706(2)(A)); *see United States v. Bean*, 537 U.S. 71, 77 (2002). Review under the APA is highly deferential, and the agency action enjoys a presumption of validity. *Ohio Valley Envtl. Coal. v. Aracoma Coal Co.*, 556 F.3d 177, 192 (4th Cir. 2009) (citing *Natural Res. Def. Council, Inc. v. EPA*, 16 F.3d 1395, 1400 (4th Cir. 1993)).

Notably, "the power of . . . agencies is circumscribed by the authority granted," and courts are "entrusted" with "protect[ing] justiciable individual rights against administrative action fairly beyond the granted powers." *Stark v. Wickard*, 321 U.S. 288, 309–10 (1944). In other words, "Agencies must operate within the legal authority conferred by Congress, and when those limits are transgressed, an individual may seek recourse in the Article III courts." *Medical Imaging & Technoloy Alliance*, 103 F.4th at 838.

As the D.C. Circuit has said, "Congress's 'historic practice' of providing for judicial review of administrative action reflects the importance of an independent check on the exercise of executive power." *Med. Imaging & Tech. All.*, 103 F.4th at 839 (quoting *Bowen v. Michigan Acad. of Fam. Physicians*, 476 U.S. 667, 670–73 (1986)). Unless Congress makes a decision to withhold

judicial review, "courts have the power and the duty to review agency action for conformity with the law." *Med. Imaging & Tech. All.*, 103 F.4th at 839.

The Fourth Circuit has set forth limitations on judicial review. The Court has said: "Review is available only when acts are discrete in character, required by law, and bear on a party's rights and obligations. The result is a scheme allowing courts to review only those acts that are specific enough to avoid entangling the judiciary in programmatic oversight, clear enough to avoid substituting judicial judgments for those of the executive branch, and substantial enough to prevent an incursion into internal agency management." *City of New York v. U.S. Dep't of Defense*, 913 F.3d 423, 432 (4th Cir. 2019) (citing *Norton v. Southern Wilderness Alliance ("SUWA")*, 542 U.S. 55, 64–65 (2004)). "In determining whether a 'meaningful standard' for reviewing agency discretion exists, courts consider the particular language and overall structure of the statute in question, as well as 'the nature of the administrative action at issue.'" *Speed Mining, Inc.*, 528 F.3d at 317 (internal citations omitted) (quoting 470 U.S. at 830 and *Drake v. FAA*, 291 F.3d 59, 70 (D.C. Cir. 2002)).

B. Final Agency Action

Under the APA, the federal government waives sovereign immunity for a suit brought by "'a person suffering legal wrong because of agency action'" who seeks to obtain relief "'other than money damages.' 5 U.S.C. § 702." *City of New York*, 913 F.3d at 430. "The term 'action' as used in the APA is a term of art that does not include all conduct" of the government. *Vill. Of Bald Head Island v. U.S. Army Corps. Of Eng'rs*, 714 F.3d 186, 193 (4th Cir. 2013). 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). As Judge Bredar recently noted, the term "'agency action' is a capacious term, 'cover[ing] comprehensively every manner

in which an agency may exercise its power.'" *Maryland, et al. v. United States Dep't of Agriculture, et al.*, JKB-25-0748, 2025 WL 800216, at *11 (D. Md. Mar. 13, 2025) (quoting *Whitman v. Am. Trucking Ass'ns*, 531 U.S. 457, 478 (2001)) (alteration in *United States Dep't of Agriculture*).

The APA limits judicial review to "final agency action for which there is no other adequate remedy in a court." 5 U.S.C. § 704; *see Lovo*, 107 F.4th at 205; *City of New York*, 913 F.3d at 430–31; *NAACP v. Bureau of the Census*, 945 F.3d 183, 189 (4th Cir. 2019); *Clear Sky Car Wash LLC v. City of Chesapeake*, 743 F.3d 438, 445 (4th Cir. 2014); *Golden & Zimmerman LLC v. Domenech*, 599 F.3d 426, 432–33 (4th Cir. 2010).[28] Indeed, a court lacks subject matter jurisdiction if the plaintiff challenges an "agency action" that is not "fit for review." *City of New York*, 913 F.3d at 430.

Under *Bennett v. Spear*, 520 U.S. 154 (1997), an agency action is final if it (1) "mark[s] the consummation of the agency's decisionmaking process" and (2) is an action "by which rights or obligations have been determined, or from which legal consequences will flow." *Id.* at 177-78; *see Biden v. Texas*, 597 U.S. 785, 808 (2022). Notably, courts take a "'pragmatic' approach . . . to finality." *U.S. Army Corps of Engineers v. Hawkes Co.*, 578 U.S. 590, 599 (2016) (quoting *Abbott Labs.,* 387 U.S. at 149); *see Her Majesty the Queen in Right of Ontario v. U.S. E.P.A.*, 912 F.2d 1525, 1531 (D.C. Cir. 1990) (noting that the finality requirement is applied in a "'flexible and pragmatic way'").

[28] The requirement of final agency action applies to plaintiffs' APA claims, but not to their *ultra vires* claim or Privacy Act claim in Count II. For example, Judge Bredar noted in *Maryland, et al. v. United States Dep't of Agriculture, et al.*, 2025 WL 800216, at *11 n.4, that "the right of action for an *ultra vires* claim flows from the federal courts' equity jurisdiction, not from the APA."

The finality requirement ensures that judicial intervention does not deny an agency the "opportunity to correct its own mistakes and to apply its expertise." *Federal Trade Comm'n. v. Standard Oil Co. of California*, 449 U.S. 232, 242 (1980); *see also Univ. of Medicine & Dentistry of New Jersey v. Corrigan*, 347 F.3d 57, 69 (3d Cir. 2003). It also avoids "piecemeal review," which is "inefficient" and might prove to be "unnecessary" upon the agency's completion of its process. *Standard Oil Co. of California*, 449 U.S. at 242. Notably, the APA does not allow a court to review an agency's "day-to-day operations." *Lujan v. Nat'l Wildlife Fed'n*, 497 U.S. 871, 899 (1990).

The scope of judicial review is limited in "two important respects." *City of New York*, 913 F.3d at 431. First, the plaintiff must "identify specific and discrete governmental conduct, rather than launch a 'broad programmatic attack' on the government's operations." *Id.* at 431 (quoting *SUWA*, 542 U.S. at 64). The Fourth Circuit has explained, *City of New York*, 913 F.3d at 431: "This distinction between discrete acts, which are reviewable, and programmatic challenges, which are not, is vital to the APA's conception of the separation of powers. Courts are well-suited to reviewing specific agency decisions, such as rulemakings, orders, or denials. [Courts] are woefully ill-suited, however, to adjudicate generalized grievances asking us to improve an agency's performance or operations."

Second, "the definition of 'agency action' is limited to those governmental acts that determin[e] rights and obligations.'" *Id.* (quoting *Clear Sky Car Wash LLC,* 743 F.3d at 445 (alteration in *City of New York*). The Fourth Circuit has explained, *City of New York*, 913 F.3d at 431: "This limitation ensures that judicial review does not reach into the internal workings of the government, and is instead properly directed at the effect that agency conduct has on private parties." In order to satisfy the requirement, "a party must demonstrate that the challenged act had

'an immediate and practical impact,' *Golden & Zimmerman LLC v. Domenech*, 599 F.3d 426, 433 (4th Cir. 2010), or 'alter[ed] the legal regime' in which it operates." *Id.* (citing *Bennett*, 520 U.S. at 178).

"The core question is whether the agency has completed its decisionmaking process, and whether the result of that process is one that will directly affect the parties." *Franklin v. Massachusetts*, 505 U.S. 788, 797 (1992) (plurality opinion); *see Flue-Cured Tobacco Cooperative Stabilization Corp. v. EPA*, 313 F.3d 852, 858 (4th Cir. 2002) ("[T]he critical issue is whether the [agency's action] gives rise to legal consequences, rights, or obligations.").

To satisfy the consummation element, the challenged agency action need not be reduced to writing. *See, e.g.*, *Her Majesty the Queen in Right of Ontario*, 912 F.2d at 1531 (noting that "the absence of a formal statement of the agency's position . . . is not dispositive); *R.I.L-R v. Johnson*, 80 F. Supp. 3d 164, 184 (D.D.C. 2015) ("Agency action, however, need not be in writing to be final and judicially reviewable."). Indeed, a "contrary rule would allow an agency to shield its decisions from judicial review simply by refusing to put those decisions in writing.'" *R.I.L-R*, 80 F. Supp. 3d at 184 (citation omitted). And, agency action has legal consequences if it "alters the legal regime[.]" *Bennett*, 520 U.S. at 178; *see Hawkes*, 578 U.S. at 598–99; *Nat'l Res. Def. Council v. EPA*, 643 F.3d 311, 320 (D.C. Cir. 2011).

C. The Contentions

Plaintiffs maintain that they "clearly challenge the decision of 'SSA and its acting officials' to 'open[] [SSA] data systems to unauthorized personnel from [DOGE] in violation of applicable laws and with disregard for the privacy interests' of millions of Americans." ECF 39 at 13 (quoting ECF 17, ¶¶ 2, 86, 101, 114, 122). In their view, the decision of the SSA Defendants to "approve DOGE's request for access to certain agency record systems and the PII on those data systems"

constitutes an "agency action" because it is a "final disposition," both "discrete" and "circumscribed." ECF 39 at 14 (citing *SUWA*, 542 U.S. at 62). Moreover, plaintiffs insist that they do not challenge the day-to-day operations of the SSA, including "the fact of SSA's onboarding of Mr. Bobba or other DOGE associates." ECF 39 at 14.

Defendants argue that no final agency action is implicated here. ECF 36 at 16. Instead, defendants characterize the access provided by SSA to the DOGE Team as "precisely the day-to-day operations the Supreme Court in *Lujan* advised not to sweep into the APA's ambit." *Id.* at 19.

According to defendants, their "declarations demonstrate [that] no new finalized policy has been implemented—or existing policy definitively changed—as SSA continues to onboard employees where needed in a workaday application of previous standards." *Id.* at 20.[29] Further, defendants argue that plaintiffs have failed to "demonstrate how providing a new employee with system access necessary to his or her function 'consummat[es]' the hiring agency's decision-making process in such a way that legal consequences flow to Plaintiffs." ECF 36 at 20.[30]

The defense also asserts, *id.* at 17: "It is unclear, for example, whether the alleged wrongful action is the provision of access to Mr. Bobba, the provision of access to Mr. Bobba and to other

[29] Defendants are inconsistent regarding the number of employees who have signed the Acknowledgement of SSA Information Security and Privacy Awareness Training. Defendants' brief states the number is nine, *see* ECF 36 at 6, while the Felix-Lawson Declaration states that ten employees have signed it. ECF 36-2, ¶ 13. Felix-Lawson also "outlines how each individual associated with SSA's DOGE team has been onboarded with SSA" and also that her office "is working to ensure all onboarding requirements are met." *Id.* ¶¶ 3, 17; *see also* ECF 39 at 14 n.11.

[30] Defendants' citation to *Sierra Club v. E.P.A.*, 955 F.3d 56, 63 (D.C. Cir. 2020), is misplaced. *See* ECF 36 at 20. There, the court found that there was no final agency action where the agency's action ""impose[d] no obligations, prohibitions or restrictions on regulated entities," and "[did] not subject them to new penalties or enforcement risks." *Sierra Club*, 955 F.3d at 63. But, the court was evaluating whether *agency guidance statements* constituted final agency actions. *Id.* ("When deciding whether guidance statements meet prong two, this Court has considered factors including . . .").

employees, or the advent of a new—or change to an existing—formal agency policy regarding access to agency informational systems, or sharing of data from those systems." And, they explain that without clear identification, "it is impossible to examine such alleged action under the APA's standards or to craft meaningful preliminary relief." *Id*.

Defendants add, *id.* at 19: "Agencies make thousands of such decisions every day, whenever they decide to open an e-mail account for an employee, to staff an employee on a particular matter, or that an employee has the relevant training to access systems or participate in certain programs. A court could not review such decisions without bringing within the scope of the APA virtually every aspect of an agency's relationship with its employees, a result the "final agency action" limitation of the APA is designed to prevent."

Moreover, defendants argue that the actions identified by plaintiffs "are both tentative and interlocutory in nature," and not final, as required. ECF 36 at 19. They claim that plaintiffs "have not identified: (1) whether additional government employees will be involved in implementing the DOGE Agenda at SSA; (2) what the status of those employees will be (*i.e.* detailees from USDS, direct hires at SSA, or detailees from other agencies); and (3) what systems they will have access to." *Id*.

D. Analysis

In my view, the government misses the mark in claiming that no final agency action is implicated here and, in effect, that it is merely business as usual at SSA. Contrary to SSA's well entrenched policy and practice, Dudek made the unprecedented decision to provide the DOGE Team with non-anonymized access to virtually all SSA records. And, when he did so, some of the DOGE Team members were not yet entitled to access, because they either were not properly detailed to SSA, or had not been vetted or adequately trained, or necessary work documents were

not signed. Moreover, there was no demonstrated need for access to such a massive quantity of PII. At best, there was only a vague and conclusory assertion that access to the entirety of SSA's systems of records was needed to root out fraud.

SSA's decision to provide such access upended the longstanding policy and practice that had governed SSA with respect to access to PII. The Agency's wholesale provision of access to the PII of millions of Americans, under the circumstances alleged here, is a sea change that falls within the ambit of a final agency action.

Venetian Casino Resort, L.L.C. v. E.E.O.C., 530 F.3d 925 (D.C. Cir. 2008), is instructive. There, the employer, the operator of a casino, sought an injunction to bar the Equal Employment Opportunity Commission ("EEOC") from releasing without notice confidential documents that the employer provided during various EEOC investigations. The EEOC claimed that the employer's claims were not cognizable under the APA because the EEOC's disclosure policy as to the confidential information was not a final agency action and because the matter of disclosure is committed to the discretion of the agency and thus not reviewable. *Id.* at 931.

As the court explained, the employer was challenging the agency decision to adopt a policy of disclosing confidential information without notice. *Id.* The D.C. Circuit concluded: "Adopting a policy of permitting 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.'" *Id.* at 931.[31] Nothing in *Venetian* was specific to *third-party* access to the information. The same logic applies here.

[31] The court had previously determined that the plaintiff had standing because it had demonstrated "a substantial probability that the alleged disclosure policy will harm its concrete and particularized interest in retaining the confidentiality of protected information." *Venetian Casino Resort, L.L.C. v. E.E.O.C.*, 409 F.3d 359, 367 (D.C. Cir. 2005).

As Russo avers: "In the case of DOGE team data access, data access to the DOGE team was first approved by SSA's Acting Commissioner [Dudek]." ECF 36-1 ("Russo Decl."), ¶ 6. And, he concedes that on February 12, 2025 and February 20, 2025, access to personally identifiable information was granted with respect to SSA's MBR, SSR, Numident, and Treasury Payment Files. *Id.* ¶ 7. Thus, the access concerned virtually all data and records systems maintained by SSA, despite a longstanding policy and practice at SSA of guarding the confidentiality and privacy of PII, except as needed.

Flick's detailed Declaration, which is unrefuted, bolsters the conclusion that the access that SSA provided constitutes a dramatic change in policy at SSA. She attests that "[t]he importance of privacy is engrained in every SSA employee from day one" and, "[a]long with accurate and timely payment of benefits, attention to privacy is one of SSA's most fundamental duties." ECF 22-10, ¶ 4. To that end, employees are required to sign documents every year acknowledging their duty to protect PII and are also required to attend annual information security training. *Id.* ¶ 6.

Critically, the DOGE Team received far broader access than what is automatically afforded when SSA records are reviewed "for potential fraud, waste, and abuse by oversight agencies . . . or auditors. . . ." ECF 22-10, ¶ 26. Flick avers that typically, "when analysts or auditors review agency data for possible payment issues, including for fraud, the review process would start with access to high-level, anonymized data based on the least amount of data the analyst or auditor would need to know." ECF 39-1, ¶ 4. Then, if a subset of the data are "flagged as suspicious, the analyst or auditor would access more granular, non-anonymized data to just that subset of files." *Id*. She also insists that "the type of full, non-anonymized access of individual data on every person who has a social security number or receives benefit from Social Security is unnecessary at the outset of any anti-fraud or other auditing project." *Id*.

Indeed, Flick avers that SSA "would not provide full access to all data systems even to our most skilled and highly trained experts." ECF 22-10, ¶ 37. Rather, she asserts that the scope of access requires a "'need to know.'" *Id.* ¶ 43. She explains that the "need to know" reason for full, non-anonymized access to SSA data systems articulated in this case are "far from sufficiently detailed to justify granting the level of access the DOGE Team now has." ECF 39-2, ¶ 5.

More than just the scope of the access, it is clear that the SSA has made a change to what requirements need to be met by employees to obtain such broad access. Flick provides several examples of occurrences that reflect that Dudek's decision to authorize the DOGE Team to obtain access to the SSA data systems is at odds with SSA's earlier policy and practices. According to Flick, the onboarding process for one of the DOGE Team employees was "contrary to standard practice," ECF 22-10, ¶ 16, and the speed at which access to systems was provided was "unprecedented." *Id.* ¶ 15.

Flick makes clear, and the timeline included in declarations submitted by defendants, discussed *infra*, confirms, that several employees of the DOGE Team accessed SSA data systems prior to having signed finalized detail agreements from other agencies. ECF 39-2, ¶ 3. According to Flick, this "is not in keeping with agency practice because the agency does not consider a detailee to be an employee of SSA until a detail agreement is signed and finalized." *Id.* And, defendants' declarations demonstrate that, currently, some of the background investigations for some DOGE Team members are still pending. Yet, they were provided access to PII in the SSA data systems. *See* ECF 36-2, ¶ 15.[32]

[32] The declarations of Russo and Felix-Lawson glaringly fail to specify dates when the DOGE Team members completed "Privacy Training" or "Ethics Training," or when they signed "Acknowledgement of SSA Information Security and Privacy Awareness Training." *See* ECF 36-1, ¶ 21; ECF 36-2, ¶ 13. This raises the specter that the requirements had not been met when access was provided.

Although not cited by the parties, SSA's policy of respecting privacy is consistent with federal regulations governing the Social Security Administration, which admonish SSA employees to be mindful of their responsibilities under the Privacy Act. The Employee Standards of Conduct for SSA state, 20 C.F.R. Pt. 401, App. A(a):

> All SSA employees are required to be aware of their responsibilities under the Privacy Act of 1974, 5 U.S.C. 552a. . . . Instruction on the requirements of the Act and regulation shall be provided to all new employees of SSA. In addition, supervisors shall be responsible for assuring that employees who are working with systems of records or who undertake new duties which require the use of systems of records are informed of their responsibilities. Supervisors shall also be responsible for assuring that all employees who work with such systems of records are periodically reminded of the requirements of the Privacy Act and are advised of any new provisions or interpretations of the Act.

SSA's regulations also provide that "Systems Employees shall: (a) Be informed with respect to their responsibilities under the Privacy Act; . . . [and] (c) Disclose records within SSA only to an employee who has a *legitimate need to know* the record in the course of his or her official duties." 20 C.F.R. Pt. 401, App. A(d)(1) (emphasis added).

Dudek's decision to provide the DOGE Team with access to all SSA record systems, and to do so without signed detail agreements, adequate training, completed background investigations, and/or executed work forms for all DOGE Team members, and without actual "need," "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.'" *Venetian Casino Resort, L.L.C.*, 530 F.3d at 931. In granting the DOGE Team access to records in the manner alleged, SSA veered far from principles that have been the mainstay of the Agency. The decision to do so qualifies as a final agency action.

E. No Other Adequate Remedy

Plaintiffs assert that "nothing absent an injunction will prevent Defendants' ongoing disclosure of and access to the data in question." ECF 21-1 at 23. But, both plaintiffs and defendants agree that the Privacy Act does not provide for injunctive relief for disclosure claims. *See* ECF 21-1 at 23 (plaintiffs); ECF 36 at 15 (defendants).

Defendants argue that the APA provides for judicial review only in circumstances where there is no other adequate remedy. *See* ECF 36 at 22. But, defendants contend that "the Privacy Act provides a 'comprehensive remedial scheme' for injuries arising out of the inappropriate dissemination of private information about individuals." *Id.* (quoting *Wilson*, 535 F.3d at 703). Therefore, they contend that plaintiffs "cannot use the APA to circumvent the Privacy Act's carefully drawn limitations on the types of relief they can seek." ECF 36 at 22.

Review under the APA is limited to "final agency action for which there is no other adequate remedy in a court." 5 U.S.C. § 704. And, the statute "makes it clear that Congress did not intend the general grant of review in the APA to duplicate existing procedures for review of agency action." *Bowen v. Massachusetts,* 487 U.S. 879, 903 (1988). Plaintiffs "may advance an APA claim as well as another type of claim only if the APA claim does not duplicate 'existing procedures for review of an agency action.'" *Cent. Platte Nat. Res. Dist. v. U.S. Dep't of Agric.*, 643 F.3d 1142, 1148 (8th Cir. 2011) (citing *Radack v. U.S. Dep't of Justice,* 402 F.Supp.2d 99, 104 (D.D.C. 2005)).

Courts have stated that an adequate alternative remedy "does not need to provide relief 'identical' to that available to a party under the APA—it must merely be of the 'same genre.'" *Westcott v. McHugh*, 39 F. Supp. 3d 21, 33 (D.D.C. 2014) (quoting *Garcia v. Vilsack*, 563 F.3d 519, 522 (D.C. Cir. 2009)); *see also El Rio Santa Cruz Neighborhood Health Ctr., Inc. v. U.S.*

Dep't of Health & Hum. Servs., 396 F.3d 1265, 1272 (D.C. Cir. 2005). Where courts have held that a plaintiff could not also bring an APA claim to obtain relief for an agency's alleged Privacy Act violation, it has been where the Privacy Act provided the kind of relief plaintiff sought. *See, e.g.*, *Westcott*, 39 F. Supp. 3d 21 (no APA claim because Privacy Act permits removal or revision of memorandum of reprimand contained in official military records); *Poss v. Kern*, No. 23-CV-2199 (DLF), 2024 WL 4286088, at *6 (D.D.C. Sept. 25, 2024) (no APA claim when seeking "removal and deletion of the allegedly defamatory report from DOD's database"); *Haleem v. U.S. Dep't of Def.*, No. CV 23-1471 (JEB), 2024 WL 230289, at *14 (D.D.C. Jan. 22, 2024) ("The Privacy Act and FOIA thus provide adequate remedies to compel responses to his requests and the production of withheld records, meaning Plaintiff cannot premise an APA claim on Defendants' alleged failure to respond to such requests or produce such records."); *Harrison v. BOP*, 248 F. Supp. 3d 172, 182 (D.D.C. 2017) (finding no APA claim because Privacy Act provided relief when agency failed to provide requested records); *Wilson v. McHugh*, 842 F. Supp. 2d 310, 320 (D.D.C. 2012) (finding no APA claim because Privacy Act applied when agency refused to withdraw a press release).

The injunctive relief sought by plaintiffs here is not available under the Privacy Act. And, the Supreme Court has stated: "The Privacy Act says nothing about standards of proof governing equitable relief that may be open to victims of adverse determinations or effects, although it may be that this inattention is explained by the general provisions for equitable relief within the Administrative Procedure Act (APA), 5 U.S.C. § 706." *Doe v. Chao*, 540 U.S. at 619 n.1.

I conclude that plaintiffs are not barred from seeking relief under the APA.

VII. Temporary Restraining Order

Plaintiffs seek a TRO to enjoin DOGE's access to SSA's data systems. The purpose of a TRO is to "preserve the status quo only until a preliminary injunction hearing can be held." *Hoechst Diafoil Co. v. Nan Ya Plastics Corp.*, 174 F.3d 411, 422 (4th Cir. 1999) (quotation omitted). A TRO is "an extraordinary remedy that may only be awarded upon a clear showing that the plaintiff is entitled to such relief." *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 22 (2008).

Alternatively, plaintiffs seek a stay under 5 U.S.C. § 705. Pursuant to 5 U.S.C. § 705, a reviewing court may stay "agency action" pending judicial review "to prevent irreparable injury." The standards for granting a TRO, a preliminary injunction, and a § 705 stay are essentially the same. *Casa de Maryland, Inc. v. Wolf*, 486 F. Supp. 3d 928, 949–50 (D. Md. 2020) (citing cases); *Maags Auditorium v. Prince George's Cty., Md.*, 4 F. Supp. 3d 752, 760 n.1 (D. Md. 2014) ("The standard for a temporary restraining order is the same as a preliminary injunction."), *aff'd*, 681 F. App'x 256 (4th Cir. 2017).

The party seeking a TRO must demonstrate that: (1) he is likely to succeed on the merits; (2) he is likely to suffer irreparable harm in the absence of preliminary relief; (3) the balance of equities tips in his favor; and (4) an injunction is in the public interest. *Winter*, 555 U.S. at 20; *see Frazier v. Prince George's Cty., Md.*, 86 F. 4th 537, 543 (4th Cir. 2023) (same). The plaintiff must satisfy each requirement as articulated. *Real Truth About Obama, Inc. v. Fed. Election Comm'n*, 575 F.3d 342, 347 (4th Cir. 2009).

To meet the first requirement, the plaintiffs must "clearly demonstrate that [they] will likely succeed on the merits," rather than present a mere "grave or serious question for litigation." *Real Truth About Obama, Inc.*, 575 F.3d at 346–47. But, plaintiffs "need not establish a 'certainty of

success.'" *Di Biase v. SPX Corp.*, 872 F.3d 224, 230 (4th Cir. 2017) (quoting *Pashby v. Delia*, 709 F.3d 307, 321 (4th Cir. 2013)).

Simply "providing sufficient factual allegations to meet the [Fed. R. Civ. P.] 12(b)(6) standard of *Twombly* and *Iqbal*" does not meet the rigorous standard required for a TRO. *Allstate Ins. Co. v. Warns*, CCB-11-1846, 2012 WL 681792, at *14 (D. Md. Feb. 29, 2012). However, the court need only find that a plaintiff is likely to succeed on one of his claims in order for this factor to weigh in favor of a TRO. *PFLAG, Inc. v. Trump*, ___ F. Supp. 3d. ___, BAH-25-337, 2025 WL 510050, at *12 (D. Md. Feb. 14, 2025); *Nat'l Council of Nonprofits v. Off. of Mgmt. & Budget*, __ F. Supp. 3d. ___, No. 25-239 (LLA), 2025 WL 368852, at *9 (D.D.C. Feb. 3, 2025); *Profiles, Inc. v. Bank of Am. Corp.*, 453 F. Supp. 3d 742, 747 (D. Md. 2020).

"To establish irreparable harm, the movant must make a 'clear showing' that it will suffer harm that is 'neither remote nor speculative, but actual and imminent.'" *Mountain Valley Pipeline, LLC v. 6.56 Acres of Land, Owned by Sandra Townes Powell*, 915 F.3d 197, 216 (4th Cir. 2019) (quoting *Direx Israel, Ltd. v. Breakthrough Medical Group*, 952 F.2d 802, 812 (4th Cir. 1991)). In other words, the plaintiffs must show that harm is not just a mere possibility, but that harm is truly irreparable and cannot be remedied at a later time with money damages. "[T]he harm must be irreparable, meaning that it 'cannot be fully rectified by the final judgment after trial.'" *Mountain Valley Pipeline, LLC*, 915 F.3d at 216 (quoting *Stuller, Inc. v. Steak N Shake Enters.*, 695 F.3d 676, 680 (7th Cir. 2012)).

Irreparable harm "is suffered when monetary damages are difficult to ascertain or are inadequate." *Multi–Channel TV Cable Co. v. Charlottesville Quality Cable Operating Co.*, 22 F.3d 546, 551 (4th Cir. 1994) (quoting *Danielson v. Loc. 275, Laborers Int'l Union of N. Am., AFL-CIO*, 479 F.2d 1033, 1037 (2d Cir. 1973)). A plaintiff may also establish irreparable harm

when its costs are unrecoverable due to the government's sovereign immunity. *See Wages & White Lion Invs., L.L.C. v. U.S. Food & Drug Admin.*, 16 F.4th 1130, 1142 (5th Cir. 2021); *City of New York*, 913 F.3d at 430; *see also Portée v. Morath*, No. 1:23-CV-551-RP, 683 F.Supp.3d 628, 636 (W.D. Tex. July 21, 2023) ("[C]laims for money damages against state entities and officials are generally barred by sovereign immunity, which makes Portée's harm irreparable for purposes of seeking preliminary injunctive relief."); *Texas v. U.S. Dep't of Homeland Sec.*, 700 F. Supp. 3d 539, 546 (W.D. Tex. 2023).

"'There is generally no public interest in the perpetuation of unlawful agency action.'" *Louisiana v. Biden*, 55 F.4th 1017, 1035 (5th Cir. 2022) (quoting *Texas v. Biden*, 10 F.4th 538, 560 (5th Cir. 2021)). To the extent an agency's acts facilitate rather than prevent unlawful conduct, such acts implicate the "substantial public interest 'in having governmental agencies abide by the federal laws that govern their existence and operations.'" *Texas v. United State*s, 40 F.4th 205, 229 (5th Cir. 2022) (quoting *League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 12 (D.C. Cir. 2016)). Indeed, "the 'public undoubtedly has an interest in seeing its governmental institutions follow the law. . . .'" *Roe v. Dep't of Defense*, 947 F.3d 207, 230–31 (4th Cir. 2020) (quoting district court).

When a TRO will "adversely affect a public interest . . . the court may . . . withhold relief until a final determination of the rights of the parties, though the postponement may be burdensome to the plaintiff." *Weinberger v. Romero–Barcelo*, 456 U.S. 305, 312–13 (1982). In fact, "courts . . . should pay particular regard for the public consequences in employing th[is] extraordinary remedy." *Id.* at 312.

In addition to the public interest determination, the balance of equities must tip in favor of the movants in order for a TRO to be granted. *Winter*, 555 U.S. at 20. Courts must weigh any

potential harm to the nonmoving party, and also any potential harm to the public if relief is granted. *Continental Group Inc. v. Amoco Chems. Corp.*, 614 F.2d 351, 356–57 (3d Cir. 1980).

These final two factors—balance of the equities and weighing the public interest—"merge when the Government is the opposing party." *Nken v. Holder*, 556 U.S. 418, 435 (2009). But, a court "may not collapse this inquiry with the first *Winter* factor." *Maryland, et al. v. United States Dep't of Agriculture, et al.*, 2025 WL 800216; *see USA Farm Lab, Inc. v. Micone*, 2025 WL 586339, at *4 (4th Cir. Feb. 24, 2025) (explaining that it is "circular reasoning" to argue that a government "program is against the public interest because it is unlawful" and that such argument "is nothing more than a restatement of their likelihood of success argument").

"Crafting a preliminary injunction [or TRO] is an exercise of discretion and judgment, often dependent as much on the equities of a given case as the substance of the legal issues it presents." *Trump v. Int'l Refugee Assistance Project*, 582 U.S. 571, 579 (2017); *see Roe*, 947 F.3d at 231. But, a court should "'mold its decree to meet the exigencies of the particular case.'" *Roe*, 947 F.3d at 231 (citation omitted). Moreover, a court must ensure that the TRO is "'no more burdensome to the defendant than necessary to provide complete relief to the plaintiffs.'" *Madsen v. Women's Health Ctr., Inc.*, 512 U.S. 753, 765 (1994) (discussion preliminary injunction) (citation omitted).

Under Fed. R. Civ. P. 65(b)(2), a TRO expires after fourteen days. But, it may be extended for a "like period" for good cause. *Id*.

A. Likelihood of Success on the Merits

1. Privacy Act

a. Zone of Interests

In order to bring a statutory claim, plaintiffs must satisfy the zone of interest test. Specifically, plaintiffs must demonstrate that the "'interest sought to be protected by the complainant is arguably within the zone of interests to be protected or regulated by the statute or constitutional guarantee in question.'" *Bennett*, 520 U.S. at 163 (quoting *Ass'n of Data Processing Serv. Organizations, Inc. v. Camp*, 397 U.S. 150, 153 (1970)). In other words, the zone-of-interests test asks "whether the statute grants the plaintiff the cause of action that he asserts." *Bank of Am. Corp. v. Miami*, 581 U.S. 189, 196–97 (2017); *see Lexmark Int'l, Inc.*, 572 U.S. at 127 ("Whether a plaintiff comes within the zone of interests" turns on "whether a legislatively conferred cause of action encompasses a particular plaintiff's claim") (internal quotation marks omitted)). However, when the plaintiff asserts a cause of action under the APA, the inquiry focuses on the relevant zone of interest defined by the substantive statute, not the APA. *See Block v. Cmty. Nutrition Inst.*, 467 U.S. 340, 345–48 (1984); *Am. Inst. of Certified Pub. Accountants v. IRS*, 746 F. App'x. 1, 7 (D.C. Cir. 2018) (collecting cases); *Mendoza v. Perez*, 754 F.3d 1002, 1017 (D.C. Cir. 2014).

The "zone-of-interests limitation" applies to "all statutorily created causes of action." *Lexmark Int'l, Inc.*, 572 U.S. at 129. However, unlike standing and ripeness, the test is not jurisdictional because "'the absence of a valid . . . cause of action does not implicate . . . the court's statutory or constitutional power to adjudicate the case.'" *Id.* at 128 (quoting *Verizon Md. Inc. v. Pub. Serv. Comm'n of Md.*, 535 U.S. 635, 642–43 (2002)). Moreover, the zone-of-interests test "is not meant to be especially demanding." *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 567 U.S. 209, 225 (2012) (quoting *Clarke v. Sec. Industry Ass'n*, 479 U.S. 388,

399 (1987)). The Supreme Court has explained that it "always conspicuously" includes the word "'arguably' in the test to indicate that the benefit of any doubt goes to the plaintiff." *Patchak*, 567 U.S. at 225. In other words, the "test forecloses suit only when a plaintiff's 'interests are so marginally related to or inconsistent with the purposes implicit in the statute that it cannot reasonably be assumed that Congress intended to permit the suit.'" *Id.* (citation omitted).

As discussed, the Privacy Act only protects information regarding individuals, which the statute defines as "a citizen of the United States or an alien lawfully admitted for permanent residence." 5 U.S.C. § 552a(a)(2); s*ee also New York et al. v. Trump*, 2025 WL 573771, at *15. And, plaintiffs' members "are no doubt individuals whose information is protected by the Privacy Act from unlawful disclosure." *Id.* at *16. In my view, the claims fall within the zone of interests.

b. Access to SSA Records

The Privacy Act limits disclosure of records. *See* 5 U.S.C. § 552a. The defendants suggest that mere access does not constitute disclosure of them.

The Privacy Act does not define the word "disclosure." But, SSA has done so in its regulations. "[D]isclosure" is defined as "making a record about an individual available to or releasing it to another party." 20 C.F.R. § 401.25. And, the Office of Management and Budget Guidelines state: "A disclosure may be either the transfer of a record or the granting of access to a record." Off. of Mgmt. & Bdgt., Exec. Off. of Pres., Guidelines, 40 Fed. Reg. 28948, 28953 (July 9, 1975). OPM defines "disclosure" to "mean[] 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.

Other courts have generally interpreted "disclosure" "'liberally to include not only the physical disclosure of the records, but also the accessing of private records.'" *American*

Federation of Teachers et al., 2025 WL 582063, at *9 n.8 (citing *Wilkerson v. Shinseki*, 606 F.3d 1256, 1268 (10th Cir. 2010)); *see Tolbert-Smith v. Chu*, 714 F. Supp. 2d 37, 43 (D.D.C. 2010) (construing "disclosure" to include "plac[ing] records . . . on a server accessible by other federal employees and members of the public"); *cf. Wilborn v. Dep't of Health & Human Servs.*, 49 F.3d 597, 600–01 (9th Cir. 1995) ("[T]he Privacy Act, if it is to be given any force and effect, must be interpreted in a way that does not 'go[] against the spirit' of the Act" (quoting *MacPherson v. IRS*, 803 F.2d 479, 481 (9th Cir. 1986)), *abrogated on other grounds by Doe v. Chao*, 540 U.S. 614. But, even when courts that have interpreted the term to require "more than mere transmission of records" they "have suggested that disclosure occurs when 'information has been exposed in a way that would facilitate easy, imminent access.'" *American Federation of Teachers et al.*, 2025 WL 582063, at *9 n.8 (citing *In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 29 (D.D.C. 2014)).

c. DOGE is an Agency

In their Reply, plaintiffs raise the question of whether DOGE is an agency. Plaintiffs state: "DOGE was established (1) by an Executive Order, (2) in the Executive Office of the President ('EOP'), and (3) separate from the few EOP components courts have deemed agencies." ECF 39 at 17.

During the hearing, defendants took the position that DOGE is not an agency.[33] This is curious. If DOGE is not an agency, then its employees cannot be detailed from DOGE to the SSA under the Economy Act. This is because the Economy Act only grants an agency the authority to

[33] Defendants claimed that because the plaintiffs raised the matter of DOGE's status for the first time in the Reply, defendants had not had the opportunity to address this question in their briefing. This makes no sense. If defendants wanted to assert that DOGE is not an agency, they could have (and should have) raised it in their Opposition.

detail a federal employee to another agency. ECF 39 at 17 (quoting 31 U.S.C. § 1535(a)); *see also id.* at 18. It follows that the DOGE Team would have no right of access to SSA records.

Other courts have recently concluded, in well reasoned opinions, that USDS (*i.e.*, DOGE) is an agency. An answer to this question is not dispositive here. But, I will address the issue briefly.

In a case evaluating whether USDS is an agency subject to FOIA, the district court considered whether "the entity in question 'wielded substantial authority independently of the President.'" *CREW*, 2025 WL 752367, at *10 (quoting *Citizens for Resp. & Ethics in Wash. v. Off. of Admin.*, 566 F.3d 219, 222 (D.C. Cir. 2009)) (citation omitted).[34] Judge Cooper observed that "the relevant executive orders appear to endow USDS with substantial authority independent of the President," and recent statements by President Trump and Mr. Musk, as well as news reports, "suggest that the President and USDS leadership view the department as wielding decision-making authority to make cuts across the federal government." *CREW*, 2025 WL 752367 at *11. The court "conclude[d] that in practice, USDS is likely exercising substantial independent authority much greater than other EOP components held to be covered by FOIA." *Id.*[35]

In *American Fed'n of Lab. & Cong. of Indus. Organizations v. Dep't of Lab.*, No. CV 25-0339 (JDB), 2025 WL 542825, at *3 (D.D.C. Feb. 14, 2025), the government took the view that USDS falls within the Economy Act's definition of agency. Borrowing from FOIA's definition of an agency, Judge Bates concluded that USDS "wield[s] substantial authority independently of

[34] The plaintiffs rested their argument on the contention that DOGE is not agency but did not contest the issue of whether the employees had a "need" for these records.

[35] The court recognized that "much, though by no means all, of the evidence supporting its preliminary conclusion that USDS is wielding substantial independent authority derives from media reports" but noted that USDS did not contest "any of the factual allegations suggesting its substantial independent authority" in briefing or at oral argument. *Id.* at 12.

the President." *Id.* (quoting *Elec. Priv. Info. Ctr. v. Presidential Advisory Comm'n on Election Integrity*, 266 F. Supp. 3d 297, 315 (D.D.C. 2017)). The court noted that "it is apparent that USDS is coordinating teams across multiple agencies with the goal of reworking and reconfiguring agency data, technology, and spending." *American Fed'n of Lab. & Cong. of Indus. Organizations*, 2025 WL 542825, at *3. Curiously, defendants' counsel took the position at the TRO hearing that USDS is an agency under the Economy Act but not under FOIA, the Privacy Act, or the APA. This, according to the court, rendered it "a Goldilocks entity: not an agency when it is burdensome but an agency when it is convenient." *Id*.

I agree with Judge Bates and Judge Cooper. Guided by case law, and without the benefit of briefing on the issue, I am satisfied, for the purposes of this opinion, that DOGE is an agency with the meaning of the Privacy Act. Were I to rule otherwise, I would be compelled to conclude that disclosure of SSA records to the DOGE Team constituted a violation of the Privacy Act, because members of the DOGE Team could not qualify as employees of an agency detailed to SSA.

d. Authorization

Relevant here, the Privacy Act prohibits agencies from disclosing any records contained in systems of records, unless an exception applies. 5 U.S.C. § 552a(b). Defendants assert that 5 U.S.C. § 552a(b)(1) applies here. They claim that the members of the DOGE Team are employees of the SSA and that the plaintiffs' records were not disseminated outside SSA.

The Executive Order directs the heads of each federal agency to "establish within their respective agencies a DOGE Team of at least four employees" within 30 days. *See Alliance for Retired Americans v. Bessent*, 2025 WL 740401, at *4 (citing Exec. Order No. 14,158 § 3(c)). These employees may include "Special Government Employees." *Id.* As relevant here, a Special

Government Employee is a temporary "officer or employee" who is "retained, designated, appointed, or employed to perform, with or without compensation . . . temporary duties either on a full-time or intermittent basis" for a limited period of time. 18 U.S.C. § 202(a).[36]

Currently, defendants claim there are ten members of the DOGE Team working at SSA. Defendants concede that seven of the ten employees have and have had access to personally identifiable information contained in SSA data systems. ECF 36 at 7.

Specifically, Employee 1 is a software engineer, appointed as an expert, and a special government employee under 5 U.S.C. § 3109 and 5 C.F.R. Part 304. ECF 36-2, ¶ 5. His duties purportedly relate to improper payments and SSA's Death Master File, or records maintained by SSA on deceased individuals. *Id*. Felix-Lawson states: "SSA is currently working with the Small Business Administration (SBA) to effectuate an interagency agreement for Employee 1 to be detailed temporarily to SBA." *Id*. Although Employee 1's background investigation is still pending, *id.* ¶ 15, Russo states that Employee 1 has access to PII from MBR, SSR, Numident, and Treasury payment files showing SSA payments. ECF 36-1, ¶ 7. In other words, Employee 1 has access to SSA records even though his detail agreement and background investigation are incomplete.

Employee 2 is a Senior Advisor ((Program Specialist AD-0301-00) and serves as the DOGE Team lead. ECF 36-2, ¶ 8. His interagency detailing agreement from NASA is not yet finalized and his background investigation is still pending. *Id*.; *see also id.* ¶ 15. Although Employee 2 has had no access to "any SSA programmatic data or systems," he has accessed SSA personnel data provided to him by Human Resources. ECF 36-1 (Russo Decl.), ¶ 13. He is

[36] Special Government Employees are exempt from some of the ethics rules that apply to most federal employees. *See* 18 U.S.C. §§ 203, 205, 207–209.

responsible for consulting on the SSA's workforce plans, including but not limited to reorganization and hiring. *Id*. As with Employee 1, his access to PII was premature.

Employee 3 is a Schedule C Policy Advisor, detailed from the Department of Labor to SSA. ECF 36-2, ¶ 6. His duties relate to improper payments and SSA's Death Master File. *Id*. His background investigation is complete. *Id.* ¶ 15. Like Employee 1, he has access to PII from MBR, SSR, Numident, and Treasury payment files showing SSA payments. ECF 36-1, ¶ 8. He also has access to the National Directory of New Hire Data, maintained on SSA's network for Office of Child Support Services. *Id.* ¶ 15.

Employee 4 was appointed as an expert, special government employee. ECF 36-2, ¶ 11. His duties currently relate to improper payments and death data. *Id*. His background investigation is still pending. *Id.* ¶ 15. However, he has not yet been granted access to SSA data or PII or access to systems containing such information. ECF 36-1, ¶ 16.

Employee 5 is an engineer detailed from the United States DOGE Service to SSA. ECF 36-2, ¶ 7. He is subject to an Interagency Agreement with U.S. Digital Service (now U.S. DOGE Service), which authorizes his work to include, but does not limit work to, increasing efficiency and the modernization of SSA IT infrastructure and systems, detecting waste, fraud, and abuse. *Id*. His background investigation is complete. *Id.* ¶ 15. Like Employees 1 and 3, he has access to PII from MBR, SSR, Numident, and Treasury payment files showing SSA payments. ECF 36-1, ¶ 9. He has also apparently been granted access to "several other databases but never accessed the data in them." *Id*.

Employee 6 was appointed as an expert, and is a special government employee. ECF 36-2, ¶ 11. His duties currently relate to improper payments and death data. *Id*. His background

investigation is still pending. *Id.* ¶ 15. But, he has not been granted access to SSA data or PII or access to systems containing such information. ECF 36-1, ¶ 16.

Employee 7 is described as a detailee from Department of Labor ("DOL") to SSA, but the detailing agreement is not yet finalized. ECF 36-2, ¶ 11. His duties relate to improper payments. *Id*. And, despite the fact that his background investigation is still pending, *id.* ¶ 15, he was granted access to "SSA Systems." ECF 36-1, ¶ 14. According to Russo, Employee 7 has so far only accessed Numident. He was apparently granted access because "his work involves analysis of improper payments relating to death records maintained in the Numident." *Id*. However, "[a]ll other access initially granted has since been revoked pending review of further data access needs." *Id*.[37] Like Employee 3, he also has access to the National Directory of New Hire Data, maintained on SSA's network for Office of Child Support Services. *Id.* ¶ 15.

Employee 8 is an engineer, detailed from OPM to SSA, whose duties relate to improper payments and death data. ECF 36-2, ¶ 10. His background investigation is complete. *Id.* ¶ 15. And, like Employees 1, 3, and 5, he has access to PII from MBR, SSR, Numident, and Treasury payment files showing SSA payments. ECF 36-1, ¶ 12.

Employee 9 was appointed as an expert, and is a special government employee. ECF 36-2, ¶ 11. His duties relate to improper payments and death data. *Id*. Although his background investigation is still pending, *id.* ¶ 15, Employee 9 has access to PII from MBR, SSR, Numident, and Treasury payment files showing SSA payments. ECF 36-1, ¶ 11. In other words, access to the records appears premature.

[37] On March 5, 2025, the SSA "began onboarding" Employee 7, although the detail agreement from the DOL is pending. ECF 36-2, ¶ 12. On March 11, 2025, in the midst of the briefing for the Motion, Employee 7 "was granted access to SSA systems." ECF 36-1, ¶ 14. But, by the time the defendants' brief was filed on March 12, 2025 at 4:03 p.m., Employee 7's access had been revoked, pending review of further data access needs. *Id*.

Employee 10 is a software engineer, detailed from the Office of the Administrator at the General Services Administration to SSA. ECF 36-2, ¶ 9. His duties include "supporting the leadership team with the assessment and enhancement of internal processes and operational procedures" by "focusing on identifying inefficiencies and areas for improvement and ensuring that the administrative and programmatic functions align with the best practices for effectiveness and accountability." *Id*. His background investigation is complete. *Id.* ¶ 15. And, like Employees 1, 3, 5, 8, and 9, he has access to PII from MBR, SSR, Numident, and Treasury payment files showing SSA payments. ECF 36-1, ¶ 10.

As noted, defendants claim that the members of the DOGE Team are employees of the SSA and that the plaintiffs' records were not disseminated outside SSA. But, based on the current record, it does not seem that this is true for all employees identified by defendants. Employees 1 and 9, for example, do not have finalized detail agreements, nor are their respective background investigations complete. Yet, both were granted access to PII in the SSA data systems. And, the background investigation for Employee 9 has not been completed. Yet, this employee also has the same access.

During the hearing, the Court asked counsel for the government if the "detail agreement[s] were effectuated before the access was provided." ECF 45 at 20. Counsel sidestepped the question, answering: "All of the detail arrangements are complete." Counsel did not say they were complete before access was provided, however. *Id*. The Court rephrased, asking if the agreements were complete when "the disclosures were first made or access provided." *Id.* Counsel for the government responded that he "believe[d]" that was the case but would need to follow up. *Id*. Thus, it is unclear whether all members of the DOGE Team were SSA employees at the time access was granted.

e. Need

Under the Privacy Act, access to the records is permitted to Agency employees only when there is "a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). The critical question here is whether the access to records that SSA provided to the DOGE Team violated the Privacy Act because of a lack of "need" for the data.

The issue of need is perhaps the central issue in the case. Defendants maintain that those employees who have access to virtually all SSA data "need" the information to perform their work. As discussed, *infra*, the statute does not define the term "need." And, neither side has provided the Court with any helpful discussion concerning this statutory requirement in the Privacy Act.

Other than recent cases involving access by DOGE affiliates to the PII in the records of other government agencies, the Court can find no precedent with similar facts interpreting the "need" requirement. But, Judge Boardman recently concluded in a case with facts similar to those here that "the alleged unauthorized disclosure of millions of records . . . appear[ed] to be unlawful." *American Federation of Teachers et al.*, 2025 WL 582063, at *11.

Cases interpreting the "need" requirement typically consider need as "need to know" and ask "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." *Doe v. U.S. Dep't of Justice,* 660 F. Supp. 2d 31, 44–46 (D.D.C. 2009). Interestingly, these cases typically involve the disclosure of records concerning a single person or a small number of people, and not access to a massive quantity of records for untold millions of people. *See, e.g., deLeon v. Wilkie*, No. CV 19-1250 (JEB), 2020 WL 210089, at *8 (D.D.C. Jan. 14, 2020) (finding "need to know" exception was met in disclosure of single plaintiff's personnel records); *Walia v. Napolitano*, 986 F. Supp. 2d 169, 186–87 (E.D.N.Y. 2013), *on reconsideration in part* (Feb. 4, 2014) (finding "need

to know" exception was not met in disclosure of single plaintiff's personnel records); *Middlebrooks v. Mabus*, No. 1:11CV46 LMB/TCB, 2011 WL 4478686, at *5 (E.D. Va. Sept. 23, 2011) (finding that "internal disclosures of plaintiff's record to key senior agency personnel were permissible"); *Viotti v. U.S. Air Force,* 902 F.Supp. 1331, 1337 (D. Colo. 1995) (holding that disclosure of information about acting head of political science department to "political science department staff" not improper "as a matter of law" under need to know exception).

As noted, the term "need" is not defined in the Privacy Act. This implicates principles of statutory construction, which the parties have not addressed.

Generally, "[w]hen faced with a statutory provision, 'the starting point for any issue of statutory interpretation . . . is the language of the statute itself.'" *Redeemed Christian Church of God (Victory Temple) Bowie, Md. v. Prince George's Cty., Md.*, 17 F.4th 497, 508 (4th Cir. 2021) (quoting *D.B. v. Cardall*, 826 F.3d 721, 734 (4th Cir. 2016)) (alteration in original); *see Groff v. Dejoy*, 600 U.S. 447, 468 (2023) (stating that "statutory interpretation must 'begi[n] with,' and ultimately heed, what a statute actually says") (citation omitted) (alteration in *Groff*); *Murphy v. Smith*, 583 U.S. 220, 223 (2018) ("As always, we start with the specific statutory language in dispute."); *Pharmaceutical Coalition for Patient Access v. United States*, 126 F. 4th 947, 953 (4th Cir. 2025) ("Statutory interpretation begins with the text of the statute."); *Williams v. Carvajal*, 63 F.4th 279, 285 (4th Cir. 2023) ("As always, an issue of statutory interpretation begins with the text."); *Navy Fed. Credit Union v. LTD Fin. Servs., LP*, 972 F.3d 344, 356 (4th Cir. 2020) ("'As in all statutory construction cases,' we start with the plain text of the provision.") (quoting *Marx v. General Revenue Corp.*, 568 U.S. 371, 376 (2013)); *see also McAdams v. Robinson*, 26 F.4th 149, 156 (4th Cir. 2022); *United States v. Bryant*, 949 F.3d

168, 174–75 (4th Cir. 2020); *Othi v. Holder*, 734 F.3d 259, 265 (4th Cir. 2013); *Ignacio v. United States*, 674 F.3d 252, 254 (4th Cir. 2012).

A statute "means what it says." *Simmons v. Himmelreich*, 578 U.S. 621 (2016); *see United States v. Cohen*, 63 F.4th 250, 253 (4th Cir. 2023). "'[A]bsent ambiguity or a clearly expressed legislative intent to the contrary,'" courts apply the "plain meaning" of the statute. *United States v. Abdelshafi*, 592 F.3d 602, 607 (4th Cir. 2010) (quoting *United States v. Bell*, 5 F.3d 64, 68 (4th Cir. 1993)); *see United States v. George*, 946 F.3d 643, 645 (4th Cir. 2020) ("When interpreting a statute, courts must 'first and foremost strive to implement congressional intent by examining the plain language of the statute.'") (quoting *Abdelshafi*, 592 F.3d at 607). A court determines a statute's plain meaning by referencing the "ordinary meaning [of the words] at the time of the statute's enactment." *United States v. Simmons*, 247 F.3d 118, 122 (4th Cir. 2001); *see also HollyFrontier Cheyenne Refining, LLC v. Renewable Fuels Ass'n*, 594 U.S. 382, 388 (2021); *Wisconsin Cent. Ltd v. United States*, 585 U.S. 274, 277 (2018). Courts may "not resort to legislative history to cloud a statutory text that is clear." *Ratzlaf v. United States*, 510 U.S. 135, 147–48 (1994); *see Raplee v. United States*, 842 F.3d 328, 332 (4th Cir. 2016) ("If the meaning of the text is plain . . . that meaning controls.").

Moreover, "'the words of a statute must be read in their context and with a view to their place in the overall statutory scheme.'" *West Virginia v. EPA*, 597 U.S. 697, 721 (2022); *see Gundy v. United States*, 588 U.S. 128, 141 (2019) (quoting *Nat'l Ass'n of Home Builders v. Defs. of Wildlife*, 551 U.S. 644, 666 (2007)); *see also United States v. Hansen*, 599 U.S. 762, 775 (2023) ("When words have several plausible definitions, context differentiates among them."); *King v. Burwell*, 576 U.S. 473, 486 (2015); *Pharmaceutical Coalition for Patient Access*, 126 F. 4th at 953. Critically, however, "the text and structure" of the statute is not analyzed in "a

vacuum. . . . Rather, [a court] must interpret the statute with reference to its history and purpose as well." *Bryant*, 949 F.3d at 174–75 (4th Cir. 2020) (citing *Abramski v. United States*, 573 U.S. 169, 179 (2014) and *Gundy*, 588 U.S. at 141).

Terms in a statute that are not defined are "'interpreted" in accordance with "their ordinary, contemporary, common meaning.'" *Sandifer v. U.S. Steel Corp.*, 571 U.S. 220, 227 (2014) (citation omitted); *see Holly Frontier Cheyenne Refining, LLC*, 594 U.S. at 388; *George*, 946 F.3d at 645; *see also Tankersley*, 837 F.3d at 395 ("Where Congress has not defined a term, we are "bound to give the word its ordinary meaning unless the context suggests otherwise.") (citation omitted). Need would seem to be a word that even a child would grasp. But, courts may "consult dictionaries" to decipher a term's ordinary or plain meaning. *In re Constr. Supervision Servs., Inc.*, 753 F.3d 124, 128 (4th Cir. 2014); *see also Navy Fed. Credit Union*, 972 F.3d at 356; *Blakely v. Wards,* 738 F.3d 607, 611 (4th Cir. 2013).

Relying on the Privacy Act, defendants assert that the employees on the DOGE Team "have a need for the records to which they have access in the performance of their duties." ECF 36 at 24. They state: "As an overarching matter, the DOGE Team exists under Executive Order 14,158 to modernize technology and to 'maximize efficiency and productivity.'" *Id.* (quoting Exec. Order 14,158 § 4). In addition, the DOGE Team at the SSA is "charged with 'detect[ing] fraud, waste and abuse in SSA programs,' and with 'provid[ing] recommendations for action to the Acting Commissioner of SSA, the SSA Office of the Inspector General, and the Executive Office of the President.'" ECF 36 at 24 (quoting ECF 36-1, Russo Decl., ¶ 5).

In considering the meaning of "need," the parties did not reference the legislative history of the Act. But, it is informative. *See, e.g.*, *Bryant*, 949 F.3d at 174–75. It shows that one of the identified purposes of the Privacy Act was "to provide certain safeguards for an individual against

an invasion of personal privacy by requiring federal agencies, except as otherwise provided by law, to— . . . (4) collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose, that the information is current and accurate for its intended use, and that adequate safeguards are provided to prevent misuse of such information[.]" Privacy Act of 1974, Pub. L. No. 93-579, § 2(b)(4), 88 Stat. 1896. And, Congress found that, "[i]n order to protect the privacy of individuals identified in information systems maintained by federal agencies, it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies." *Id.* § 2(a)(5).

The Senate Report is also instructive. It states that the law was "designed to prevent the kind of illegal, unwise, overbroad, investigation and record surveillance of law-abiding citizens produced in recent years from actions of some over-zealous investigators, and the curiosity of some government administrators, or the wrongful disclosure and use, in some cases, of personal files held by Federal agencies." Senate Rep. No. 1183, 93d Cong., 2d Sess. (1974). Relevant here, the bill established "certain minimum standards for handling and processing personal information maintained in the data banks and systems of the executive branch, for preserving the security of the computerized or manual system, and for safeguarding the confidentiality of the information." *Id.* To this end, it required "every department and agency to insure, by whatever steps they deem necessary" that, *inter alia*, (1) "they take certain administrative actions to keep account of the employees and people and organizations who have access to the system or file, and to keep account of the disclosures and uses made of the information"; and (2) "they establish rules of conduct with regard to the ethical and legal obligations in developing and operating a

computerized or other data system and in handling personal data, and take action to instruct all employees of such duties[.]" *Id.*

Because the word "need" is not defined, I may also consult the dictionary, even though the word "need" is part of everyday parlance. In dictionaries, "need" can be defined as "a requirement, necessary duty, or obligation, or a lack of something wanted or deemed necessary," "urgent want, as of something requisite," or "a condition marked by the lack of something requisite." RANDOM HOUSE COLLEGE DICTIONARY at 890 (rev. ed.1980); *see also Need,* American Heritage Dictionary, https://perma.cc/M32F-ZVM2 (defining "need" as "[s]omething required or wanted; a requisite" and "[n]ecessity; obligation").

However, it seems clear that, in context, and under Social Security Administration regulation 20 C.F.R. Pt. 401, App. A, discussed earlier, the term "need" actually refers to "need to know." *See American Federation of Teachers, et al.,* 2025 WL 582063, at *10. According to Black's Law Dictionary, "need-to-know basis" is defined as follows: "A justification for restricting access to information to only those with a clear and approved reason for requiring access—used as a means of protecting confidential information that affects a range of interests, from national security to trade secrets to the attorney-client privilege." *Need-to-know basis*, Black's Law Dictionary, at 1194 (12th ed. 2024).

At the Motion hearing, the Court repeatedly questioned government counsel to explain the "need" for the breadth of access to SSA records that was provided to the DOGE Team. Counsel offered no meaningful explanation as to why the DOGE Team was in "need" of unprecedented, unfettered access to virtually SSA's entire data systems in order to accomplish the goals of modernizing technology, maximizing efficiency and productivity, and detecting fraud, waste, and abuse.

For example, the Court asked counsel for the government: "[W]hat was the mission and what was the need? What was the purpose in providing access to all of this information?" ECF 45 at 23. The Court again pressed about why the DOGE Team would "need" the scope of information at issue here. *Id.* at 24, 38. And, toward the end of the hearing, the Court once again gave the government the opportunity to explain the "need for all of those records." *Id.* at 84.

Besides cursory, circular statements about members of the DOGE Team in need of all SSA data because of their work to identify fraudulent or improper payments, counsel provided no explanation as to why or how the particular records correlated to the performance of job duties. *See, e.g.*, *id.* at 21–22 ("The goal is to review . . . the Social Security Administration's records to see if there are improper or fraudulent payments. Naturally if one is looking for improper or fraudulent payments, one looks at the data to see if any such payments are made."); *id.* at 23 ("[If] one is looking for fraudulent or improper payments that may or may not be going out by the Social Security Administration, one would need to look at the records, the beneficiary data, the payment data in order to do an assessment of that and to recommend potential changes."); *id.* at 24 ("I can tell you that they are looking for instances of improper or fraudulent payments and that it is natural that one would look at the data in that system to see if they've been substantiated . . . ."); *id.* at 39 ("These particular people are working at the agency in order to carry out the sort of broad policy prescription contained in the Executive Order. They are also looking at improper payments and potential waste or improper or fraudulent payments. . . ."); *id.* at 85 ("[I]f you wanted to decide whether or not [a claim for benefits] was improper or not, you would need to look at the records to see if the payment was properly made or if it was fraudulent.").

Defendants have not submitted declarations from the hired experts on the DOGE Team explaining why such unrestricted and unfettered access is necessary. They have not provided a

particularized explanation of how or why virtually the entire data base of SSA is needed to conduct the investigation, or why redacted or anonymized records, at least initially, would be inadequate. The silence on this issue is deafening.

In my view, plaintiffs have shown a likelihood of success on the merits as to their claim that the access to records provided by SSA to the DOGE Team does not fall within the need-to-know exception to the Privacy Act. Therefore, the access violates both the Privacy Act and the APA.

f. Routine Use

Defendants maintain that, to the extent employees of the DOGE Team cannot be considered employees of the SSA, the access they have obtained is not improper under the Privacy Act because it "fits within the routine use exception." ECF 36 at 25 (citing 5 U.S.C. § 552a(b)(3)). The defendants' attempt to plug the events here into the routine use exception of the Privacy Act, 5 U.S.C. § 552a(b)(3), is unavailing. It amounts to the proverbial effort to fit a square peg into a round hole.

In 5 U.S.C. § 552a(b)(3) it states:

> **(b) Conditions of disclosure.—**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, unless disclosure of the record would be—
>
> * * *
>
> **(3)** for a routine use as defined in subsection (a)(7) of this section and described under subsection (e)(4)(D) of this section; . . . .

In turn, 5 U.S.C. § 552a(a)(7) states:

> **(7)** the term "routine use" means, with respect to the disclosure of a record, the use of such record for a purpose which is compatible with the purpose for which it was collected; . . . .

Relevant here, the statute also requires the agency to "publish in the Federal Register . . . a notice . . . which notice shall include . . . (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use." 5 U.S.C. § 552a(e)(4)(D). To justify the information shared with the DOGE Team, defendants point to SSA Privacy Act systems of records notices "("SORN"), corresponding to each data system to which access has been granted. ECF 36 at 25. These SORNs contain the following "routine use," which defendants argue applies to the facts here: "'To student volunteers, individuals working under a personal services contract, and other workers who technically do not have the status of Federal employees, when they are performing work for us, as authorized by law, and they need access to personally identifiable information (PII) in our records in order to perform their assigned agency functions.'" *Id*. But, defendants do not explain how this routine use applies here.

Members of the DOGE Team with access to these systems are not "student volunteers," nor are they "individuals working under a personal services contract." As employees of DOGE, these individuals would be considered federal employees or contractors, even if they are not employees of SSA. Thus, they are not "other workers who technically do not have the status of Federal employees."

Even assuming these individuals fit into one of the categories outlined in the SORN, and there is no evidence to demonstrate that they do, the SORN still requires that these individuals "*need access* to personally identifiable information (PII) . . . in order to perform their assigned agency functions" (emphasis added). As discussed earlier, no such need has been proffered to justify the wholesale access of a vast quantity of PII belonging to millions of people.

For these reasons, plaintiffs are likely to succeed on their claim that SSA's provision to the DOGE Team of access to SSA systems is "not in accordance with" the Privacy Act, and therefore in violation of the APA. *See* 5 U.S.C. § 706(2).

2. Arbitrary and Capricious

The APA requires courts to "hold unlawful and set aside agency action, findings, and conclusions" that are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). "The scope of review under the 'arbitrary and capricious' standard is narrow and a court is not to substitute its judgment for that of the agency." *Motor Vehicle Mfrs. Ass'n of the U.S., Inc. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983).

But, the agency must "articulate a satisfactory explanation for its action including a 'rational connection between the facts found and the choice made.'" *Id.* (quoting *Burlington Truck Lines v. United States,* 371 U.S. 156, 168 (1962)). Agency action is generally considered arbitrary or capricious 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." *Motor Vehicle Mfrs. Ass'n of the U.S., Inc.*, 463 U.S. at 43.

As discussed, defendants have not provided the Court with a reasonable explanation for why the DOGE Team needs access to the wide swath of data maintained in SSA systems in order to root out fraud and abuse. And, as detailed by Flick, SSA has practices in place for audits or other searches for alleged fraud or abuse. Instead, defendants disregarded protocols for proper hiring, onboarding, training, and access limitations, and, in a rushed fashion, provided access to a

massive amount of sensitive, confidential data to members of the DOGE Team, without any articulated explanation for the need to do so.

Defendants clearly understand why guarding privacy, rather than waiting for harm to occur, is important. After all, that is precisely the reason why they have withheld even the names of the members of the SSA DOGE Team. But, defendants have not shown the same level of care with the far more sensitive, confidential data of millions of Americans who entrusted their government with their personal and private information. The trust appears to have been violated, without any articulated need. Plaintiffs are likely to succeed on a claim that the conduct at issue was unreasonable and capricious. Plaintiffs have therefore shown a likelihood of success on their arbitrary and capricious claim.

B. Irreparable Harm

Plaintiffs contend that their members "are irreparably harmed by DOGE's ongoing, illegal access to their sensitive information." ECF 21-1 at 29 (emphasis omitted). In their view, that "harm will continue until DOGE is blocked from SSA systems, forced to destroy any data it or its associates retain, and prohibited from re-entering SSA systems moving forward." *Id.*

For example, plaintiffs contend that some of their members receive disability benefits. ECF 21-1 at 30 (citing ECF 22-1, Widger Declaration, ¶ 10); ECF 22-4, Imperiale Declaration, ¶ 4); ECF 22-6, Fiesta Declaration, ¶ 18)). According to plaintiffs, to receive these benefits, "members must submit extensive medical information, including details about the prescription and non-prescription medicines the applicant takes; lists of their healthcare providers and the medical conditions for which they were evaluated and treated, including mental health conditions; and other sensitive medical information." ECF 21-1 at 30 (citing ECF 22-1, ¶ 11). Plaintiffs argue, ECF 21-1 at 30 (quoting ECF 22-1, ¶ 12): "Some of this information, including concerning 'health

conditions like HIV or other STDs, can result in stigma, social isolation, job loss, housing loss, and other harms.'"

"The disclosure of this information to DOGE," plaintiffs say, "is an actual, ongoing harm to Plaintiffs' members, who did not consent to DOGE accessing their sensitive information and who face injury in the form of a privacy violation each day the department retains that access." ECF 21-1 at 30. According to plaintiffs, their members "are irreparably harmed by DOGE's ongoing, illegal access to their sensitive information." *Id.* at 29 (emphasis omitted). In their view, that "harm will continue until DOGE is blocked from SSA systems, forced to destroy any data it or its associates retain, and prohibited from re-entering SSA systems moving forward." *Id.* And, citing Judge Boardman's decision in *American Federation of Teachers et al.*, 2025 WL 582063, at *14, plaintiffs assert: "[T]hat harm cannot be rectified by money damages down the road." ECF 21-1 at 30.

Defendants argue that plaintiffs have not established that they will suffer irreparable harm for the same reasons defendants argue that plaintiffs do not have standing—their claimed injury "is not concrete". *See* ECF 36 at 31. Defendants also allege that plaintiffs' argument fails because they "have an adequate alternative remedy to the emergency relief they seek: a private right of action under the Privacy Act." *Id*. at 32 (citing 5 U.S.C. § 552a(g)(4)).

The government cites two recent cases from the D.C. District Court denying a TRO or a preliminary injunction because the plaintiffs in each case did not establish irreparable harm. ECF 36 at 31 (citing *Carter*, 2025 WL 542586, at *5; *Alliance for Retired Americans*, 2025 WL 740401, at *20–24). But, defendants do not explain that the D.C. Circuit appears to maintain a higher bar for injunctive relief in these types of cases, as explained by Judge Kollar-Kotelly in *Alliance for Retired Americans*, 2025 WL 740401. She stated that in the D.C. Circuit, plaintiffs' asserted injury

"'must be both certain and great'" to support a preliminary injunction. *Id.* (quoting *Wis. Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985)).

And, in the context of disclosure of private information, courts in the D.C. Circuit "have consistently 'declined to find irreparable injury . . . where the challenged disclosure is not public' but instead is to a small number of 'individuals obligated to keep [the information] confidential.'" *Alliance for Retired Americans*, 2025 WL 740401, at *21 (quoting *Carter*, 2025 WL 542586, at *5) (alteration in *Alliance*) (cleaned up). This is because, she noted, the court could order adequate corrective relief after the fact. *See Alliance for Retired Americans*, 2025 WL 74040, at *21. For example, she explained that the court "could order the small number of individuals who received the information to return or destroy it," and the possibility that adequate relief would later be available weighed against a finding of irreparable harm. *See id.*

Defendants also cite *Electronic Privacy Information Center v. U.S. Office of Personnel Management.*, No. 1:25-CV-255 (RDA/WBP), 2025 WL 580596 (E.D. Va. Feb. 21, 2025), in support of their argument. That case involved the accessing of data systems containing "Social Security numbers, dates of birth, salaries, home addresses, and job descriptions of all civil government workers, along with any disciplinary actions they have faced." However, the extensive data housed within the SSA's systems is not limited to government workers. *See id.* at *2. Moreover, Judge Alston emphasized that plaintiffs' arguments about "heightened risk of exposure or exfiltration by hostile actors"; future "misuse" of private data "by arbitrarily stopping payments through access to [the Treasury Department's] system"; and risk of "future identity theft because OPM's network is regularly subject to hacking attempts," which plaintiffs claimed were "more likely to be successful as a result of Defendants' actions," were "unpersuasive" and "too speculative." *Id.* at *6–7. But, what is critical here is the irreparable harm associated with

defendants' ongoing, unprecedented, unfettered access to the income history, tax return data, and medical information of millions of Americans.

In a case involving the disclosure of records by the Departments of Education, Treasury, and OPM, Judge Boardman determined that plaintiffs had "made a clear showing that they are likely to suffer irreparable harm without injunctive relief." *American Federation of Teachers et al.*, 2025 WL 582063, at *13. She explained, *id.*: "DOGE affiliates have been granted access to systems of record that contain some of the plaintiffs' most sensitive data—Social Security numbers, dates of birth, home addresses, income and assets, citizenship status, and disability status—and their access to this trove of personal information is ongoing. There is no reason to believe their access to this information will end anytime soon because the government believes their access is appropriate." Here, several individuals affiliated with DOGE have been granted access to additional, arguably even more sensitive data, including medical information. And, because defendants believe this access is necessary for these employees, there is no reason to think it will end anytime soon. *See* ECF 36 at 20.

Plaintiffs' members do not know if their information has been viewed or documented by any of these employees, nor how many times it has been viewed or will continue to be viewed in the coming hours, days, weeks, or months. But, plaintiffs know their sensitive, personally identifiable information is accessible to the DOGE Team on a daily basis, with no proper justification.

Money damages cannot rectify this invasion of privacy of plaintiffs' members. *See, e.g.*, *Norman-Bloodsaw v. Lawrence Berkeley Lab'y*, 135 F.3d 1260, 1275 (9th Cir. 1998) (finding "the retention of [the plaintiff's] undisputedly intimate medical information [without consent] . . . would constitute a continuing 'irreparable injury' for purposes of equitable relief"); *In re Meta Pixel*

Healthcare Litig., 647 F. Supp. 3d 778, 802 (N.D. Cal. 2022) ("The invasion of privacy triggered by the Pixel's allegedly ongoing disclosure of plaintiffs' medical information is precisely the kind of intangible injury that cannot be remedied by damages."); *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000) (Disclosure of data including psychiatric and medical treatment and diagnoses "is the quintessential type of irreparable harm that cannot be compensated or undone by money damages."); *Haw. Psychiatric Soc. v. Ariyoshi*, 481 F. Supp. 1028, 1038 (D. Haw. 1979) (finding irreparable injury because "[t]he disclosure of the highly personal information contained in a psychiatrist's files to government personnel is itself a harm that is both substantial and irreversible").

C. Balance of the Equities and the Public Interest

As noted, the third and fourth elements, which address whether the balance of the equities tip in the movant's favor and whether the injunction is in the public interest, merge "when the Government is the opposing party." *Nken*, 556 U.S. at 435.

Plaintiffs posit, ECF 21-1 at 33: "The government cannot suffer harm from an injunction that merely ends an unlawful action because '[the government] is in no way harmed by issuance of a preliminary injunction which prevents the [government] from enforcing restrictions likely to be found unconstitutional' or which 'merely ends an unlawful practice.'" (Quoting *Leaders of a Beautiful Struggle v. Balt. Police Dep't*, 2 F.4th 330, 346 (4th Cir. 2021)). In other words, plaintiffs argue that "'there is a substantial public interest in having governmental agencies abide by federal laws'" and, "'[i]f anything, the system is improved by such an injunction.'" ECF 21-1 (quoting *HIAS, Inc. v. Trump*, 415 F. Supp. 3d 669, 686 (D. Md. 2020) and then *Centro Tepeyac v. Montgomery Cnty.*, 722 F.3d 184, 191 (4th Cir. 2013)).

In sum, plaintiffs contend, ECF 21-1 at 33: "Defendants' actions violate numerous federal laws and will cause increasing harm to Plaintiffs' 7.7 million members as long as they are allowed to continue. Those members, along with countless similarly situated Americans, would benefit from the Court's grant of the relief requested herein."

According to defendants, ECF 36 at 32: "Plaintiffs' argument for why the equities and the public interest fall in their favor largely collapse into the merits." In defendants' view, even if plaintiffs are correct that defendants' practices are unlawful, "considering only likelihood of success is insufficient to justify injunctive relief." *Id.* at 33 (citing *Winter*, 555 U.S. at 22). In any event, defendants argue that the proposed TRO would "harm" the public interest "by limiting the President's ability to effectuate the policy choices the American people elected him to pursue by limiting his advisors and other employees' ability to access information necessary to inform that policy." ECF 36 at 33. Defendants add that the proposed TRO "would also frustrate the President's ability to identify fraud, waste, and abuse throughout the federal government." *Id.*

Logically, "[t]here is generally no public interest in the perpetuation of unlawful agency action." *League of Women Voters of United States*, 838 F.3d at 12. On the other hand, there is a substantial public interest "in having governmental agencies abide by the federal laws that govern their existence and operations." *Washington v. Reno*, 35 F.3d 1093, 1103 (6th Cir. 1994); *see Roe*, 947 F.3d at 230–31. Nonetheless, the Fourth Circuit has recently stated that it is improper to collapse "the first *Winter* factor—likelihood of success on the merits—with the merged balance of equities and public interest factor." *USA Farm Lab., Inc.*, 2025 WL 586339, at *4. Likelihood of success on the merits alone does not suffice. *Id.*

Nevertheless, as addressed earlier, there is a strong public interest in maintaining the confidentiality of PII, such as medical records and financial information. Indeed, society expects

as much. Defendants admit that the SSA granted DOGE personnel broad access to millions of Americans' sensitive PII. This intrusion into the personal affairs of millions of Americans—absent an adequate explanation for the need to do so—is not in the public interest. To be sure, rooting out possible fraud, waste, and mismanagement in the SSA is in the public interest. But, that does not mean that the government can flout the law to do so. The President's advisors and employees are not exempt from the statutes Congress enacted to protect American citizens from overbroad and unnecessary access to their PII.

VIII. Conclusion

The American public may well applaud and support the Trump Administration's mission to root out fraud, waste, and bloat from federal agencies, including SSA, to the extent it exists. But, by what means and methods?

The DOGE Team is essentially engaged in a fishing expedition at SSA, in search of a fraud epidemic, based on little more than suspicion. It has launched a search for the proverbial needle in the haystack, without any concrete knowledge that the needle is actually in the haystack.

To facilitate the expedition, SSA provided members of the SSA DOGE Team with unbridled access to the personal and private data of millions of Americans, including but not limited to Social Security numbers, medical records, mental health records, hospitalization records, drivers' license numbers, bank and credit card information, tax information, income history, work history, birth and marriage certificates, and home and work addresses.

Yet, defendants, with so called experts on the DOGE Team, never identified or articulated even a single reason for which the DOGE Team needs unlimited access to SSA's entire record systems, thereby exposing personal, confidential, sensitive, and private information that millions of Americans entrusted to their government. Indeed, the government has not even attempted to

explain why a more tailored, measured, titrated approach is not suitable to the task. Instead, the government simply repeats its incantation of a need to modernize the system and uncover fraud. Its method of doing so is tantamount to hitting a fly with a sledgehammer.

In my view, plaintiffs are likely to succeed on their claim that such action is arbitrary and capricious, and in violation of the Privacy Act and the APA. Plaintiffs have also demonstrated that their members will suffer irreparable harm in the absence of a TRO, the equities tip in their favor, and the TRO serves the public interest.

For the foregoing reasons, plaintiffs' Motion (ECF 21) is granted. A Temporary Restraining Order shall issue.

IX. Bond

Fed. R. Civ. P. 65(c) states, in relevant part: "The court may issue a . . . temporary restraining order only if the movant gives security in an amount that the court considers proper to pay the costs and damages sustained by any party found to have been wrongfully enjoined or restrained." The purpose of this Rule is "to provide a mechanism for reimbursing an enjoined party for harm it suffers as a result of an improvidently issued injunction or restraining order." *Hoechst Diafoil Co.*, 174 F.3d at 421. A district court has discretion in setting the bond amount. *See id.* at 421 n.3; *Maryland Dep't of Hum. Res. v. U.S. Dep't of Agric.*, 976 F.2d 1462, 1483 (4th Cir. 1992); *Maryland, et al. v. United States Dep't of Agriculture, et al.*, 2025 WL 800216, at *26. The amount "ordinarily depends on the gravity of the potential harm to the enjoined party . . . ." *Hoechst Diafoil Co.*, 174 F.3d at 421 n.3.

Plaintiffs ask the Court to "exercise its discretion to waive or set at $0 the security requirement . . . because Defendants will face no monetary injury from any relief ordered by the Court." ECF 21-1 at 35 n.39. Defendants' Opposition is silent on the security requirement.

I conclude that a nominal bond is appropriate. Accordingly, I shall require each plaintiff to pay a bond of $250, for a total of $750.

Date: March 20, 2025

/s/
Ellen Lipton Hollander
United States District Judge