

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MARYLAND
SOUTHERN DIVISION

AMERICAN FEDERATION OF
TEACHERS,

555 New Jersey Ave. N.W.
Washington, DC 2000,

INTERNATIONAL ASSOCIATION OF
MACHINISTS AND AEROSPACE
WORKERS,

9000 Machinists Place
Upper Marlboro, MD 20772,

INTERNATIONAL FEDERATION OF
PROFESSIONAL AND TECHNICAL
ENGINEERS,

513 C St. NE
Washington, DC 20002,

NATIONAL ACTIVE AND RETIRED
FEDERAL EMPLOYEES ASSOCIATION,

606 N Washington St.
Alexandria, VA 22314,

NATIONAL FEDERATION OF FEDERAL
EMPLOYEES,

225 New York Ave., NW, Suite 450
Washington, DC 20005,

DONALD MARTINEZ,

c/o Murphy Anderson PLLC
1401 K St. NW
Washington, D.C. 20005,

JASON CAIN,

c/o Murphy Anderson PLLC
1401 K St. NW
Washington, D.C. 20005,

CLIFFORD GRAMBO,

c/o Murphy Anderson PLLC
1401 K St. NW
Washington, D.C. 20005,

THOMAS FANT,

c/o Murphy Anderson PLLC
1401 K St. NW
Washington, D.C. 20005,

CHRISTOPHER PURDY,

Case No. 8:25-cv-00430

c/o Murphy Anderson PLLC
1401 K St. NW
Washington, D.C. 20005, and

KRISTOFER GOLDSMITH
c/o Murphy Anderson PLLC
1401 K St. NW
Washington, D.C. 20005,

Plaintiffs,

vs.

SCOTT BESSENT, in his official capacity as
Secretary of the Treasury,
1500 Pennsylvania Ave. NW
Washington, D.C. 20220,

The UNITED STATES DEPARTMENT OF
THE TREASURY,
1500 Pennsylvania Ave. NW
Washington D.C. 20220,

CHARLES EZELL, in his official capacity as
the Acting Director of the Office of Personnel
Management,
1900 E St. NW
Washington, D.C. 20415,

The UNITED STATES OFFICE OF
PERSONNEL MANAGEMENT,
1900 E St. NW
Washington, D.C. 20415,

DENISE L. CARTER, in her official capacity
as the Acting Secretary of Education, and
400 Maryland Ave., SW
Washington, D.C. 20202,

The UNITED STATES DEPARTMENT OF
EDUCATION,
400 Maryland Ave., SW
Washington, D.C. 20202,

Defendants.

AMENDED COMPLAINT

1. Americans who interact with the U.S. Government routinely entrust federal agencies with sensitive personal information: Social Security numbers, home addresses, financial

records, and more. The government has codified its promise to treat their information with care in the requirements of the Privacy Act. Today, Defendants are permitting Elon Musk and a cadre of loyalists imported from his private companies to help themselves to the personal information of millions of Americans, in violation of those legal requirements. Plaintiffs in this case seek immediate relief to stop the Defendants from further unlawful disclosures and halt the serious harms that flow from the exposure and dissemination of sensitive personal information.

2. On January 20, 2025, President Trump issued an executive order refashioning the United States Digital Services as the “U.S. DOGE Service,” ostensibly to promote government efficiency. It has been widely reported that the DOGE effort is led by the world’s richest man, Elon Musk, and a small team of DOGE representatives that he directs, including at least one 19-year-old who had previously leaked proprietary information.

3. The White House has revealed little about the members of the DOGE and their qualifications, training, or background. It is similarly unclear whether and to what extent the members of the DOGE have been subject to the same rigorous background checks that federal employees who have access to some of the government’s most sensitive and closely guarded data systems undergo. Notwithstanding this, Defendants have provided representatives of the DOGE with access to these systems, which includes Social Security numbers, bank account numbers, dates and places of birth, and other extraordinarily sensitive records of millions of Americans.

4. Steamrolling into sensitive government record systems threatens to upend how these critical systems are maintained and compromises the safety and security of personal identifying information for Americans all across the country. It also violates federal law.

5. Collecting and securely maintaining sensitive personal information allows the federal government to provide crucial services—from managing Social Security and veterans’ disability payments, to supporting Americans pursuing higher education and helping them access health care.

6. The Privacy Act balances the government’s legitimate need for information about individual Americans with the imperative to mitigate the risks inherent in collecting personal

information at scale. “Enacted in the wake of the Watergate and the Counterintelligence Program (“COINTELPRO”) scandals involving illegal surveillance on opposition political parties and individuals deemed to be ‘subversive,’ the Privacy Act sought to restore trust in government and to address what at the time was seen as an existential threat to American democracy.” Off. of Privacy & Civ. Liberties, *Overview of the Privacy Act of 1974: 2020 Edition*, at 1. The statute carefully regulates the circumstances in which agency records about individuals can be shared. Disclosures beyond what the statute authorizes are unlawful.

7. Defendants’ mass disclosure of personal information flies in the face of that legal framework and tramples on the individual privacy rights and interests protected by the Privacy Act. It also threatens real people, including individual Plaintiffs and members of the Plaintiff Organizations (collectively, “Plaintiffs”), by exposing them to the risk of identity theft, harassment, intimidation, and embarrassment.

8. For example, Defendants Treasury Department and Secretary of Treasury Bessent have improperly disclosed to DOGE representatives the contents of the Federal Disbursement System, which is the government’s mechanism for sending payments it owes to individual Americans (as well as other payees). That system contains records relating to every American who receives (among other things) a tax refund, social security benefit, veterans pay, or a federal salary. To facilitate these payments, the system maintains highly sensitive information about millions of Americans, including Social Security numbers, dates of birth, bank account information, and home addresses.

9. Similarly, Defendants Department of Education and Acting Secretary of Education Denise L. Carter have improperly disclosed information maintained in the National Student Loan Data System. That system contains information on almost 43 million borrowers and their families necessary to manage federal student loan programs. This includes sensitive personal information such as Social Security numbers, bank records, tax returns, home addresses, employment data, documentation of marital status, mortgage statements, bank records, tax returns, child support, investments, family financial status and records, dependent-care cost,

death, divorce, job loss, immigration status, and demographic data about student-borrowers—and, often, also for their parents, spouses, or other family members.

10. Defendants U.S. Office of Personnel Management and its Acting Director Charles Ezell have improperly disclosed information in multiple sensitive record systems. Those records contain information about the 2.3 million federal employees, as well as millions of other former federal employees and job applicants. These files contain exceedingly sensitive personal information: in addition to Social Security numbers, contact information, and demographic information, they contain highly sensitive employment information.

11. All of these agencies have valid purposes for maintaining these record systems. But that does not mean that Elon Musk or other DOGE representatives may have unlimited access to them. The Privacy Act requires each of these agencies to provide access to records only as part of the agencies' routine work to advance the legitimate purposes for which the records are maintained in the first place, or with the express written consent of the individual whose data is being sought.

12. Representatives of the DOGE, however, do not believe themselves constrained by those legitimate purposes or by the individual record-holders' consent. They have accessed Defendants' data systems and the sensitive information contained within to “shut[] down” payments and in the case of the Education Department, the agency itself.¹

13. The risks to Americans whose sensitive information is improperly disclosed are very real. Failing to handle these records according to established safeguards increases the risks that external actors may access them. The personal data contained in these systems could readily facilitate identity theft and other economic crimes, with potentially devastating consequences for the victims.

14. These disclosures have directly harmed Plaintiffs. Plaintiffs include veterans who receive benefit payments as provided by law, current and former federal employees whose

¹ Elon Musk (@elonmusk), X (Feb. 2, 2025, 3:14 AM), <https://x.com/elonmusk/status/1885964969335808217>; Elon Musk (@elonmusk), X (Feb. 3, 2025, 8:30 PM), <https://x.com/elonmusk/status/1886633448078475593>.

confidential employment files reside in the Office of Personnel Management’s (“OPM”) system, and teachers, first responders, and health care workers whose pathway to careers in public service included relying on student loans to fund their own educations. As to all of them, their personal data has been improperly disclosed to DOGE representatives in a manner completely divorced from the legitimate purposes for which it was maintained and in violation of their privacy rights. Plaintiffs are anxious about the implications of this government-facilitated breach of their personal information and uncertain about how their data is being used or who it will be shared with and whether it will be weaponized against them. They are concerned that the breach may well result in serious personal, social, and economic harm, from being targeted for harassment and threats to doxxing, swatting, and identity theft.

15. The Administrative Procedure Act authorizes persons whose information has been unlawfully disclosed in violation of the Privacy Act to seek injunctive relief. *Doe v. Chao*, 435 F.3d 492, 505 n.17 (4th Cir. 2006). Accordingly, Plaintiffs ask this Court to restore the privacy they are entitled to under federal law by preventing further unauthorized and improper disclosures and ensuring that improper disclosures to DOGE representatives stop immediately.

JURISDICTION AND VENUE

16. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, because this action arises under the laws of the United States.

17. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(e)(1)(C) because Defendants are officers and agencies of the United States, no real property is at issue in this case, and one or more Plaintiffs are residents of this District.

PARTIES

18. Plaintiff **American Federation of Teachers (“AFT”)** is a national labor organization headquartered in Washington, D.C., representing 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. For over a

decade the AFT has been fighting to help teachers and nurses burdened by student debt receive Public Service Loan Forgiveness. The national union has hosted hundreds of student debt clinics for tens of thousands of its members. As part of those clinics, the AFT has helped its members apply for the Public Service Loan Forgiveness Program, which is administered by the Department of Education. AFT members have records housed within OPM and Department of Education record systems and receive payments of various kinds from the United States Treasury. AFT also advocates for the ethical use of artificial intelligence and enforcement of government regulations that protect its members' personal data.²

19. Plaintiff **National Active and Retired Federal Employees Association** (“**NARFE**”) is a nonprofit organization founded in 1921, incorporated in the District of Columbia, and headquartered in Alexandria, Virginia, with a membership of approximately 128,000 current and former federal employees as well as spousal annuitants. NARFE’s mission is to promote the general welfare of current federal civilian employees and federal retirees and their survivors, to advise and assist them with respect to their federal benefits, to represent their interests before appropriate authorities, and to support legislation and regulations beneficial to such employees and retirees and to oppose those detrimental to their interests. NARFE’s members have records housed within OPM and Department of Education record systems and receive payments of various kinds from the United States Treasury. NARFE’s advocacy efforts include calling on federal agencies to take reasonable steps to protect the privacy of NARFE members’ digital information.³

20. Plaintiff **International Association of Machinists and Aerospace Workers** (“**IAM**”) is an international labor organization and unincorporated membership organization headquartered in Upper Marlboro, Maryland. IAM is one the largest and most diverse labor unions in North America with nearly 600,000 active and retired members. Among IAM’s

² See, e.g., *The Future of Public Work: Artificial Intelligence, Algorithms & Data Protection in a Digital Age*, Am. Fed’n Tchrs. (July 17, 2022), <https://www.aft.org/resolution/future-public-work-artificial-intelligence-algorithms-and-data-protection>.

³ See, e.g., *Updates on OPM Cybersecurity Incident*, Nat’l Active & Retired Fed. Emps. Ass’n (Jan. 10, 2019), <https://www.narfe.org/blog/2019/01/10/updates-on-opm-cybersecurity-incident>.

affiliate organizations is the National Federation of Federal Employees (“NFFE”), which is a national labor organization and unincorporated membership organization headquartered in Washington, D.C. Together, IAM and NFFE represent more than 100,000 federal workers, approximately 13,000 of whom are dues-paying members, from agencies across the federal government. IAM and NFFE also represent many veterans and veterans’ groups, advocate on their behalf, and assist them in receiving their benefits, among other services. IAM and NFFE members have records housed within OPM and Department of Education record systems and receive payments of various kinds from the United States Treasury. IAM and NFFE advocacy efforts include assisting their members in seeking redress for federal agencies’ unlawful disclosures of members’ sensitive data.⁴

21. Plaintiff **International Federation of Professional and Technical Engineers (“IFPTE”)** is an international labor organization headquartered in Washington, D.C., that represents approximately 34,000 federal employees, 7,000 of which are dues-paying members. The majority of federal employees represented by IFPTE work at the Department of Defense, primarily shipyards. Other represented members include nuclear submarine engineers, scientists and researchers at NASA, Administrative Law Judges at the Social Security Administration, and nuclear engineers at the Tennessee Valley Authority, as well as employees of the Environmental Protection Agency. IFPTE comprises many members who are veterans and represents and advocates for veterans and veterans’ groups. IFPTE members have records housed within OPM and Department of Education record systems and receive payments of various kinds from the United States Treasury. IFPTE advocacy efforts include calling on federal legislators and agencies to implement policies that protect IFPTE members’ privacy interests.⁵

22. Plaintiff **Jason Cain** is a resident of North Carolina and currently works as an instructor of political science. He served for 10 years in the U.S. Army, as Sergeant First Class in

⁴ See, e.g., *Privacy Rights*, Nat’l Fed’n Fed. Emps., <https://nffe.org/members-center/privacy-rights>.

⁵ See, e.g., Letter from Paul Shearon, Pres., Int’l Fed’n Prof. Tech. Engs., to Diane Feinstein, U.S. Senator (June 14, 2021), https://www.ifpte.org/s/IFPTE_NASA_MAP_Feinstein_letter_June142021_FINAL.pdf.

the U.S. Army Special Operations Command and the 82nd Airborne and had a Top Secret security clearance. He receives financial benefits from the federal government, including VA disability benefits. He previously received GI bill benefits, student loans, and a VA home loan from the federal government. As a result of his military service, employment in the civil service, and financial benefits, federal government agencies, including Defendants OPM and the Departments of Education and Treasury, have sensitive personal information about him in their record systems. When his VA account was previously hacked, and his disability and education benefits diverted to criminal enterprises, Plaintiff Cain experienced the fear and helplessness of having his personal information compromised. He is anxious about repeating this experience based on this unauthorized access to his personal information. He is outraged that such a grave breach of his privacy took place, given the extreme caution with which he was required to handle sensitive information during his service in the military and at the VA.

23. Plaintiff **Kristofer Goldsmith** is a resident of New York and currently works as the head of a nonprofit organization combating domestic extremists. He is a military veteran of the U.S. Army, was deployed to Iraq in 2005, and left the Army as a Sergeant. He receives financial benefits from the federal government, including VA disability benefits. He has also previously received student loans from the federal government. As a result of his military service and financial benefits, federal government agencies, including Defendants Departments of Education and Treasury, have sensitive personal information about him in their record systems. Plaintiff Goldsmith is deeply concerned that his personal information is compromised, and may be exploited by domestic extremist organizations to harass, intimidate, and harm him and his family. These concerns are even more acute in light of the presidential pardons of many domestic extremists, with Musk's apparent support.

24. Plaintiff **Clifford "Buzz" Grambo** is a resident of Maryland and is currently retired. He is a military veteran who served in the U.S. Navy for 20 years, retiring as Chief Petty Officer. He receives financial benefits from the federal government, including VA disability benefits and a military pension. Because of these financial benefits from his military service,

federal government agencies, including Defendant Treasury, have sensitive personal information about him in their record systems. Plaintiff Grambo believes that the unauthorized access to his and others' personal information poses a national security risk.

25. Plaintiff **Thomas Fant** is a resident of Massachusetts and is currently retired. He is a military veteran of the U.S. Coast Guard, from which he was medically discharged. He receives financial benefits from the federal government, including VA disability benefits. Because of these financial benefits from his military service, federal government agencies, including Defendant Treasury, have sensitive personal information about him in their record systems. Plaintiff Fant is apprehensive and anxious that the unauthorized access to his and others' personal information will enable third parties affiliated with DOGE representatives to profit at the expense of him and other Americans.

26. Plaintiff **Donald Martinez** is a resident of Colorado and currently works as a rancher. He is a military veteran of the U.S. Army, and had two deployments to Iraq as a Field Artillery Officer with a Top Secret/Sensitive Compartmented Information security clearance. During his service, he sustained a traumatic brain injury and was medically retired. He receives financial benefits from the federal government, including veterans' benefits, Social Security Disability Insurance/Medicare, Combat Related Special Compensation, and a VA home loan. Apart from his military service, Plaintiff Martinez also worked for the Federal Emergency Management Agency. And he received student loans from the federal government. As a result of his military service, employment in the civil service, and financial benefits, federal government agencies, including Defendants OPM and Departments of Education and Treasury, have sensitive personal information about him in their record systems. Especially because of his previous military service in a geographically sensitive area and involvement in high-level negotiations because of which he received death threats from terrorists, Plaintiff Martinez is worried that unauthorized access and disclosure of his personal information held within the federal government will compromise his personal safety and security.

27. Plaintiff **Christopher Purdy** is a resident of Georgia and currently works as the head of a nonprofit organization. He served for eight years in the Army National Guard, where he was deployed to Iraq in 2011. He receives financial benefits from the federal government, including VA disability benefits. He previously also received a VA home loan and student loans from the federal government. As a result of his military service and financial benefits, federal government agencies, including Defendants Departments of Education and Treasury, have sensitive personal information about him in their record systems. Plaintiff Purdy is distressed that the breach of his personal information by unauthorized parties makes it more vulnerable to being released to the public, which could cause him severe economic harm. He is also very worried that Musk and DOGE may use their unauthorized access to his personal information to stop his VA disability payments, a major source of income in his household.

28. Defendant the **United States Department of the Treasury** (“Treasury”) is an agency of the United States.

29. Defendant **Scott Bessent** is sued in his official capacity as the Secretary of the Treasury.

30. Defendant the **Office of Personnel Management** is an agency of the United States.

31. Defendant **Charles Ezell** is the Acting Director of the Office of Personnel Management (“OPM”) and is sued in his official capacity.

32. Defendant **United States Department of Education** is an agency of the United States.

33. Defendant **Denise Carter** is the Acting Secretary of Education and is sued in her official capacity.

FACTUAL ALLEGATIONS

Establishment of DOGE

34. On January 20th, 2025, President Trump signed an executive order replacing the United States Digital Services with the “United States DOGE Service,” which serves as the

parent agency for the new “U.S. DOGE Service Temporary Organization.”⁶ The order called for DOGE to “implement the President’s DOGE Agenda, by modernizing Federal technology and software to maximize governmental efficiency and productivity.”⁷

35. Even before the inauguration, President Trump announced that Elon Musk would lead the DOGE effort. It has been publicly reported that Musk directly leads and supervises activities of DOGE and its team.⁸ According to the White House, Musk now serves as a Special Government Employee.⁹

36. The order establishing DOGE also provided for “DOGE teams” of at least four employees, which can include Special Government Employees, to be embedded within Federal agencies. Special Government Employee is a temporary employment status typically used for outside advisors, experts or consultants appointed to work on a short-term basis within the federal government. They are exempt from some federal ethics rules.

37. DOGE representatives within the government are a combination of friends and former employees of Musk and his companies and a cadre of young adult software engineers, including college students and at least one teenager, whose identities the White House and DOGE have sought to conceal.¹⁰

The Privacy Act’s Prohibitions on Disclosure of Records Without Express Written Consent

38. “The Privacy Act directs agencies to establish safeguards to protect individuals against the disclosure of confidential records ‘which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.’” *F.A.A. v. Cooper*, 566 U.S. 284, 294-95 (2012) (quoting 5 U.S.C. § 552a(e)(1)). It

⁶ Madeleine Ngo & Theodore Schleifer, *How Trump’s Department of Government Efficiency Will Work*, N.Y. Times (Jan. 21, 2025), <https://www.nytimes.com/2025/01/21/us/politics/doge-government-efficiency-trump-musk.html>

⁷ Executive Order, *Establishing and Implementing The President’s “Department of Government Efficiency”* The White House (Jan. 20, 2025), <https://www.whitehouse.gov/presidential-actions/2025/01/establishing-and-implementing-the-presidents-department-of-government-efficiency>.

⁸ Bobby Allyn & Shannon Bond, *Elon Musk Is Barreling into Government With DOGE, Raising Unusual Legal Questions*, NPR (Feb. 3, 2025), <https://www.npr.org/2025/02/03/nx-s1-5285539/doge-musk-usaid-trump>.

⁹ Kaitlan Collins & Tierney Sneed, *Elon Musk Is Serving as a ‘Special Government Employee,’ White House Says*, CNN (Feb. 3, 2025), <https://www.cnn.com/2025/02/03/politics/musk-government-employee/index.html>.

¹⁰ Theodore Schleifer et al., *Young Aides Emerge as Enforcers in Musk’s Broadside Against Government*, N.Y. Times (Feb. 7, 2025), <https://www.nytimes.com/2025/02/07/us/politics/musk-doge-aides.html>.

does that by providing a legal framework for how the government handles sensitive records about Americans in a manner that protects their significant privacy rights.

39. The Privacy Act states, “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” without consent of the individual whose information is in the record, subject to twelve statutory exceptions.¹¹

40. Under the Privacy Act, a system of records is “a group of any records under the control of an agency from which information is retrieved by the name of the individual or ... other identifying particular assigned to the individual.”¹²

41. A record is “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.”¹³

42. Office of Management and Budget (“OMB”) guidelines state that disclosure under the Privacy Act “may be either the transfer of a record or the granting of access to a record.”¹⁴ Disclosure can be written, oral, electronic, or a mechanical transfer between computers of record content.¹⁵

43. The Privacy Act specifies when individual information maintained in an agency record system may be disclosed. It does not prohibit disclosures to employees of the maintaining agency “who have a need for the record in the performance of their duties.”¹⁶

44. Similarly, the Privacy Act does not prohibit disclosures made for a “routine use,” defined as “the use of such record for a purpose which is compatible with the purpose for which

¹¹ 5 U.S.C. § 552a(b).

¹² 5 U.S.C. § 552a(5).

¹³ 5 U.S.C. § 552a(a)(4).

¹⁴ OMB Guidelines, 40 Fed. Reg. 28,948, 28,953 (July 9, 1975).

¹⁵ *Id.*

¹⁶ 5 U.S.C. § 552a(b)(1).

it was collected.”¹⁷ Agencies must publish a Statement of Record Notice (“SORN”) identifying all possible routine uses of a system of records.¹⁸

45. Additionally, the Privacy Act mandates that “Each agency that maintains a system of rec-ords shall . . . establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained[.]”¹⁹

The Treasury Department’s Federal Disbursement Services

46. The Federal Disbursement Services (“FDS”), which is housed within the Treasury Department’s Bureau of the Fiscal Service (the “Fiscal Service”), provides critical payment services for hundreds of federal agencies, allowing them to disburse payments such as Social Security benefits, federal income tax refunds, and veterans’ pay, on which more than 70 million Americans rely.²⁰

47. In fiscal year 2024, FDS disbursed more than 1.27 billion payments, valued at more than \$5.45 trillion.²¹

48. The payment systems that make up FDS contain extensive amounts of sensitive, personally identifiable information (“PII”). This includes name, Social Security number, date and location of birth, physical address, telephone number, and financial institution information, among many other pieces of PII.²² Within the payment systems, there is PII for tens of millions of individuals, if not more.²³

¹⁷ 5 U.S.C. § 552a(a)(7).

¹⁸ *Id.*

¹⁹ 5 U.S.C. § 552a(e)(10).

²⁰ See U.S. Dep’t Treasury, *Federal Disbursement Services (FDS)*, (last modified Oct. 15, 2024), <https://fiscal.treasury.gov/fds/>; *Monthly Statistical Snapshot, December 2024*, Social Security Administration (Jan. 2025), https://www.ssa.gov/policy/docs/quickfacts/stat_snapshot/.

²¹ *Id.*

²² U.S. Dep’t Treasury, Notice of a Modified System of Records. 85 Fed. Reg. 11,776, 11,778 (Feb. 27, 2020).

²³ U.S. Dep’t Treasury, *Privacy and Civil Liberties Impact Assessment: Payment Automation Manager* (Jul. 11, 2019), <https://www.fiscal.treasury.gov/files/pia/pampclia.pdf>.

49. Historically, “only a small group of career employees” has operated the payment systems.²⁴ It is “extremely unusual” for “anyone connected to political appointees” to request or gain access to the payment systems.²⁵ Payment system access is strictly limited to “[o]nly employees whose official duties require access.”²⁶

50. The Fiscal Service does not play a discretionary role in providing payment services. Rather, when federal agencies provide the Fiscal Service with a payment voucher to disburse money to a recipient and the Fiscal Service verifies that the voucher has been completed properly, payment systems within Fiscal Service issue the disbursement without exercising independent judgment.²⁷ Stated differently, the Fiscal Service’s routine use of the FDS is limited to issuing disbursements requested by various federal agencies.

DOGE’s Repeated Efforts to Improperly Access the Federal Disbursement Services

51. For months, individuals affiliated with the initiative that would later become DOGE have worked to gain access to the Federal Disbursement System.²⁸ Indeed, soon after the November 2024 election, they asked for access to the system in an effort to have the Treasury Department serve as a “chokepoint” on payments.²⁹

52. David A. Lebryk, a senior career civil servant at Treasury, denied all of DOGE’s requests for access to the sensitive personal data stored on the FDS. On January 24, 2025, DOGE-related officials asked Lebryk, at the time Acting Secretary of the Treasury, to “immediately shut off all USAID payments using [Treasury’s] ultra-sensitive payment processing system.”³⁰ Lebryk refused to do so on the grounds that stopping payments other

²⁴ Jacqueline Alemany et al., *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, WASH. POST (Jan. 31, 2025), <https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems>.

²⁵ *Id.*

²⁶ 85 Fed. Reg. 11,776, 11,778.

²⁷ See 31 U.S.C. § 3325(a).

²⁸ Jacqueline Alemany et al., *Senior U.S. Official Exits After Rift with Musk Allies over Payment System*, WASH. POST (Jan. 31, 2025), <https://www.washingtonpost.com/business/2025/01/31/elon-musk-treasury-department-payment-systems>.

²⁹ Katelyn Polantz, Phil Mattingly & Tierney Sneed, *How an Arcane Treasury Department Office Became Ground Zero In The War Over Federal Spending*, CNN (Feb. 1, 2025), <https://www.cnn.com/2025/01/31/politics/doge-treasury-department-federal-spending>.

³⁰ *Id.*

federal agencies have requested is not within the Treasury's purview or part of its practice.³¹

Lebryk was subsequently placed on administrative leave and later announced his retirement.³²

53. On or before January 31, 2025, and following Lebryk's placement on administrative leave, at least two people affiliated with DOGE gained access to the Federal Disbursement System.³³ They included Tom Krause, the CEO of Cloud Software Group, and Marko Elez, a 25-year-old DOGE staffer and Elon Musk deputy.³⁴ The government has claimed that both Krause and Elez were appointed as Special Government Employees in the Treasury Department.

54. The day after Krause and Elez gained access to the payment systems, Musk posted on X that DOGE representatives "discovered" that "payment approval officers at Treasury were instructed always to approve payments, even to known fraudulent or terrorist groups."³⁵

55. On February 2, 2025, Musk posted on X that "[c]areer Treasury officials are breaking the law every hour ... by approving payments that are fraudulent" and this had to "stop NOW!"³⁶ The same day, Musk replied to a post on X criticizing funding to specific religiously affiliated non-profit organizations and stated that "[t]he @DOGE team is rapidly shutting down these illegal payments."³⁷

56. On February 3, 2025, White House Press Secretary Karoline Leavitt said DOGE staff had been granted read-only access to the Treasury payments system.³⁸ A letter from the Treasury Department to members of Congress on February 4, 2025 reiterated that Treasury staff

³¹ *Id.*

³² Andrew Duehren et al., *Treasury Official Quits After Resisting Musk's Requests on Payments*, N.Y. TIMES (Jan. 31, 2025), <https://www.nytimes.com/2025/01/31/us/politics/david-lebryk-treasury-resigns-musk.html>.

³³ Andrew Duehren et al., *Elon Musk's Team Now Has Access to Treasury's Payments System*, N.Y. TIMES (Feb. 1, 2025), <https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html>.

³⁴ Tobias Burns, *DOGE Staffer Who Accessed Treasury Department Payment Systems Resigns after Racist Posts Exposed*, THE HILL (Feb. 6, 2025), <https://thehill.com/business/5131442-elon-musk-deputy-resign>.

³⁵ Elon Musk (@elonmusk), X (Feb. 1, 2025, 1:52 AM), <https://x.com/elonmusk/status/1885582076247712229>.

³⁶ Elon Musk (@elonmusk), X (Feb. 2, 2025, 2:27 PM), <https://x.com/elonmusk/status/1886134485822922785>.

³⁷ Elon Musk (@elonmusk), X (Feb. 2, 2025, 3:14 AM), <https://x.com/elonmusk/status/1885964969335808217>.

³⁸ Jonathan Swan et al., *Inside Musk's Aggressive Incursion Into the Federal Government*, N.Y. TIMES (Feb. 3, 2025), <https://www.nytimes.com/2025/02/03/us/politics/musk-federal-government.html>.

working with Krause would have read-only access to the coded data of the payment systems.³⁹ The letter further stated that this was the type of access provided to individuals reviewing Treasury systems, such as auditors.

57. On February 4, 2025, WIRED reported that, contrary to Leavitt’s and Treasury’s representations, Elez possessed read *and* write access to Treasury Department payment systems.⁴⁰ Elez’s administrative-level privileges reportedly included the ability to write code on the Payment Automation Manager (PAM) and Secure Payment System (SPS) at the Bureau of the Fiscal Service (BFS). WIRED reported that “[t]ypically, those admin privileges could give someone the power to . . . change user permissions, and delete or modify critical files.”

Defendants’ Disclosure of Information in the FDS to DOGE Officials Violates the Privacy Act

Payment Systems Within the FDS Are a System of Records

58. Multiple payment systems within FDS are systems of records, as certified by the Chief Privacy Officer of the Fiscal Service.⁴¹ The Fiscal Service has published a Systems of Records Notice (SORN) for these payment systems.⁴²

59. The information in specific payment systems within FDS, including the Secure Payment System, the Invoice Processing Platform, and the Automated Standard Application for Payments, among others, is retrieved by an “identifying particular” assigned to an individual.⁴³

60. The payment systems maintained within FDS contain extensive personally identifiable information about individuals, including but not limited to Social Security numbers, sensitive financial information, and addresses.⁴⁴

³⁹ U.S. Dep’t Treasury, *Treasury Department Letter to Members of Congress Regarding Payment Systems* (Feb. 4, 2025), <https://home.treasury.gov/news/press-releases/sb0009>.

⁴⁰ Vittoria Elliott et al., *A 25-Year-Old With Elon Musk Ties Has Direct Access to the Federal Payment System*, WIRED (Feb. 4, 2025), <https://www.wired.com/story/elon-musk-associate-bfs-federal-payment-system/>

⁴¹ See, e.g., *Privacy and Civil Liberties Impact Assessment: Secure Payment System*, U.S. Dep’t Treasury (Mar. 22, 2021), <https://www.fiscal.treasury.gov/files/pia/spsplcia.pdf>.

⁴² 85 Fed. Reg. 11,776.

⁴³ See, e.g., *Privacy and Civil Liberties Impact Assessment: Secure Payment System*, U.S. Dep’t Treasury (Mar. 22, 2021), <https://www.fiscal.treasury.gov/files/pia/spsplcia.pdf>.

⁴⁴ 85 Fed. Reg. 11,776.

*Providing DOGE Representatives with Direct Access to the FDS is a “Disclosure”
Under the Privacy Act*

61. Representatives of DOGE were granted access to payment systems within FDS and the records and data therein on January 31, 2025.⁴⁵ That access qualifies as a disclosure under the Privacy Act.

62. None of the individual Plaintiffs, and on information and belief, none of the members of the Plaintiff Organizations requested disclosure or provided express written consent to the disclosure of their records and information to DOGE representatives.

*DOGE Representatives Do Not Require Access to the FDS in the Performance of Their
Duties*

63. The New York Times recently reported that “Musk allies who have been granted access to the payment system were made Treasury employees.”⁴⁶

64. The Privacy Act’s exception for disclosures to employees who need the record “in the performance of their duties” does not apply. Even if Krause and Elez were Treasury employees at the time Defendants provided them with access to the FDS, Musk’s stated purpose for that access, which is to stop “approving” all payments,⁴⁷ is incompatible with any legitimate duties of the Department of the Treasury with respect to the FDS.

65. The Treasury Department maintains the relevant record systems so that it may, in a non-discretionary manner, send out payments approved by other federal agencies.⁴⁸ Consistent with the Treasury Department’s limited role in the payment disbursement process, FDS’s payment systems are designed to “facilitate” payments from federal government entities to their recipients.⁴⁹ Stated differently, the payment systems contained within the FDS serve as

⁴⁵ Andrew Duehren et al., *Elon Musk’s Team Now Has Access to Treasury’s Payments System*, N.Y. Times, (Feb. 1, 2025), <https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html>.

⁴⁶ *Id.*

⁴⁷ Elon Musk (@elonmusk), X (Feb. 2, 2025, 2:27 PM), <https://x.com/elonmusk/status/1886134485822922785>.

⁴⁸ See 31 U.S.C. § 3325(a); U.S. Dep’t Treasury, *Treasury Department Letter to Members of Congress Regarding Payment Systems* (Feb. 4, 2025), <https://home.treasury.gov/news/press-releases/sb0009> (“To be clear, the agency responsible for making the payment always drives the payment process.”).

⁴⁹ 85 Fed. Reg. 11,776, 11,778.

processing centers that enact disbursement requests received from agencies; they are not independent centers of review.⁵⁰

Defendants' Disclosures of FDS Information to DOGE Representatives is Not a "Routine Use" of the Protected Information

66. The Privacy Act's "routine use" exception also does not apply. The SORN for payments systems within FDS lists 19 possible routine uses, none of which apply to DOGE staffers' access to FDS.⁵¹

67. For example, representatives of DOGE are not accessing FDS records on behalf of the banking industry, an investigative agency, an agency responsible for law enforcement, a court, a foreign government, a congressional office, a union, a third party during the course of an investigation, a federal creditor agency, a state, debt collectors, or representatives of the National Archives and Records Administration.⁵²

68. Representatives of DOGE also are not responding to a suspected or confirmed "breach of the system of records,"⁵³ or "ensuring the efficient administration" of "payment processing services."⁵⁴

69. Rather, representatives of DOGE intend to change the purpose of payment systems within FDS to "scrutinize[]" payments and "pause" those they deem "improper," rather than disburse payments in a non-discretionary manner.⁵⁵ Consistent with this, Musk has indicated that DOGE officials are looking to control, and potentially cut off, disbursements from the Bureau of the Fiscal Service.⁵⁶ This is not a routine use listed in the SORN that would authorize Defendants' disclosure of sensitive personal and financial data to DOGE

⁵⁰ U.S. Dep't Treasury, *Privacy and Civil Liberties Impact Assessment: Secure Payment System* (Mar. 22, 2021), <https://www.fiscal.treasury.gov/files/pia/spsplia.pdf>.

⁵¹ 85 Fed. Reg. 11,776, 11,778.

⁵² *See id.*

⁵³ *Id.*

⁵⁴ *Id.*

⁵⁵ Andrew Duehren et al., *Elon Musk's Team Now Has Access to Treasury's Payments System*, N.Y. TIMES (Feb. 1, 2025), <https://www.nytimes.com/2025/02/01/us/politics/elon-musk-doge-federal-payments-system.html>. ; Elon Musk (@elonmusk), X (Feb. 3, 2025, 11:43 AM), <https://x.com/elonmusk/status/1886455404713943058>.

⁵⁶ Elon Musk (@elonmusk), X (Feb. 2, 2025, 3:14 AM), <https://x.com/elonmusk/status/1885964969335808217>.

Representatives.⁵⁷ Nor could it be, given the Treasury’s practice and policies regarding use of the FDS to fulfill its duty to disburse payments approved by other agencies.

70. None of the other statutory exceptions for disclosure of personal information set forth in the Privacy Act applies or would have applied to authorize Defendants Bessell’s and the Treasury’s decision to disclose the sensitive information and data contained within the FDS to DOGE representatives.

U.S. Office of Personnel Management Federal Work Force Files

71. OPM serves as the “chief human resources agency and personnel policy manager for the Federal Government.”⁵⁸

72. As part of its workforce management responsibilities, OPM maintains systems that are responsible for “government-wide personnel management activities,” such as tracking human resource and payroll data, operating centralized application and hiring systems for federal government jobs, and managing health benefits for more than 8 million federal civilian employees and other eligible individuals.⁵⁹

73. The systems that OPM operates and maintains contain extensive amounts of sensitive PII. This includes name, Social Security number, employment history, address, telephone number, demographic information, and disability status, among many other pieces of PII.⁶⁰ Within the OPM systems, there is PII for tens of millions of individuals, if not more,

⁵⁷ 85 Fed. Reg. 11,776.

⁵⁸ *About Us*, U.S. Off. Personnel Mgmt., <https://www.opm.gov/about-us>.

⁵⁹ *Privacy Impact Statement for Health Insurance Data Warehouse*, U.S. Off. Personnel Mgmt. (July 2, 2021), <https://www.opm.gov/information-management/privacy-policy/privacy-policy/hidw-pia.pdf> [hereinafter *HIDW PIA*]; *Privacy Impact Assessment for USAJOBS*, U.S. Off. Personnel Mgmt. (July 8, 2020), <https://web.archive.org/web/20241228071153/https://www.opm.gov/information-management/privacy-policy/privacy-policy/usajobs-pia.pdf>; *Privacy Impact Statement for Enterprise Human Resources Integration Data Warehouse*, U.S. Off. Personnel Mgmt. (July 11, 2019), <https://www.opm.gov/information-management/privacy-policy/privacy-policy/ehridw.pdf>.

⁶⁰ *Privacy Impact Assessment Summaries*, U.S. Off. Personnel Mgmt., <https://www.opm.gov/information-management/privacy-policy/#url=PIAs>.

including current and former federal employees and applicants to jobs at more than 500 federal agencies.⁶¹

74. It has been reported that access to these OPM systems is generally held only by “senior career employees” at OPM.⁶² Some subsets of records in OPM systems are subject to even stricter access restrictions, such as those in the Health Insurance Data Warehouse, which are generally confined to “a limited number of well-trained [health insurance] analysts.”⁶³

DOGE’s Efforts to Improperly Access OPM Systems

75. Shortly after the inauguration of President Trump, civil servants within OPM received instructions to provide access to the sensitive OPM systems to DOGE representatives.⁶⁴

76. On information and belief, DOGE representatives have gained sweeping access to highly sensitive record systems within the last few weeks. The *Washington Post* reported on February 6:

At least six DOGE agents were given broad access to all personnel systems at the OPM on the afternoon of Jan. 20, the day of Trump’s inauguration, according to two agency officials. Three more gained access about a week later, they said.

The data that the DOGE team can access includes a massive trove of personal information for millions of federal employees, included in systems called Enterprise Human Resources Integration and Electronic Official Personnel Folder. It also includes personal information for anyone who applied to a federal job through the site USAJobs, the people said. Last year alone, the people said, there were 24.5 million such applicants.

⁶¹ U.S. Gov. Accountability Off., USAJOBS Website: OPM Has Taken Actions to Assess & Enhance the User Experience (Oct. 2020), <https://www.gao.gov/assets/gao-21-31.pdf#:~:text=approximately%2017.5%20million%20job%20applications%20were%20started,applicants%20are%20deemed%20qualified%20and%20which%20are;HIDWPIA,supra%20note%2059>.

⁶² Tim Reid, *Exclusive: Musk Aides Lock Workers Out of OPM Computer Systems*, Reuters (Feb. 2, 2025), [https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31; see, e.g., HIDW PIA, supra note 59, at 9 \(noting that “only a limited number of well-trained \[health-insurance\] analysts have access to the information in the \[Health Insurance Data Warehouse system\].”\); *Privacy Impact Assessment for the Payment Processing Automation Initiative*, U.S. Off. Personnel Mgmt. at 8 \(June 3, 2020\), <https://www.opm.gov/information-management/privacy-policy/privacy-policy/ppai-olbp.pdf> \(noting “access controls that limit access to only those with a need to know and only with access appropriate to their roles and responsibilities”\).](https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31;see,e.g.,HIDWPIA,supra%20note%2059,at%209(noting%20that%20%22only%20a%20limited%20number%20of%20well-trained%20[health-insurance]%20analysts%20have%20access%20to%20the%20information%20in%20the%20[Health%20Insurance%20Data%20Warehouse%20system].%22);PrivacyImpactAssessmentforthePaymentProcessingAutomationInitiative,U.S.Off.PersonnelMgmt.at8(June3,2020),https://www.opm.gov/information-management/privacy-policy/privacy-policy/ppai-olbp.pdf(noting%20%22access%20controls%20that%20limit%20access%20to%20only%20those%20with%20a%20need%20to%20know%20and%20only%20with%20access%20appropriate%20to%20their%20roles%20and%20responsibilities%22))

⁶³ HIDW PIA, supra note 59.

⁶⁴ Caleb Ecarma & Judd Legum, *Musk Associates Given Unfettered Access to Private Data of Government Employees*, Popular Info. (Feb. 3, 2025), <https://popular.info/p/musk-associates-given-unfettered>.

The two OPM officials said the level of access granted to DOGE agents means they could copy the Social Security number, phone numbers and personnel files for millions of federal employees.⁶⁵

77. The access instructions specified that DOGE representatives should have “admin user” access that allowed them to “code read and write permissions,” in essence allowing these officials to “make updates to anything that they want.”⁶⁶

78. Defendants OPM and Acting Director Ezell provided DOGE representatives, including a recent high school graduate, with access to these sensitive systems and databases, including USAJOBS, the Enterprise Human Resources Integration Data Warehouse (“EHRI DW”), USA Staffing, USA Performance, and the Health Insurance Data Warehouse (“HIDW”), and the personally identifiable information contained within.⁶⁷

79. In late January, career officials who have long had access to these systems had their permissions “revoked.”⁶⁸

80. DOGE representatives at OPM have since used their access to examine job description data and “remove” specific government employees.⁶⁹ On February 8, 2025, the Washington Post reported that access to EHRI DW and the Electronic Official Personnel Folder was revoked for “some” DOGE agents.⁷⁰

Defendants’ Disclosure of Information in OPM Systems to DOGE Representatives Violates the Privacy Act

OPM Systems Contain Systems of Records

⁶⁵ Isaac Stanley-Becker et al., *Musk’s DOGE Agents Access Sensitive Personnel Data, Alarming Security Officials*, Wash. Post (Feb. 6, 2025), <https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security>.

⁶⁶ Ecarma & Legum, *supra* note 64.

⁶⁷ *Id.*

⁶⁸ Tim Reid, *Exclusive: Musk Aides Lock Workers Out of OPM Computer Systems*, Reuters (Feb. 2, 2025), <https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31>.

⁶⁹ Ecarma & Legum, *supra* note 64.

⁷⁰ Isaac Stanley-Becker and Hannah Natanson, *Some DOGE agents removed from sensitive personnel systems after security fears*, Washington Post (Feb. 8, 2025), <https://www.washingtonpost.com/nation/2025/02/08/doge-opm-musk/>.

81. The systems to which DOGE-related officials have access within OPM, including USAJOBS, EHRI DW, USA Staffing, USA Performance, and HI DW (collectively, “OPM Systems”), are systems of records, as certified by the Chief Privacy Officer of OPM.⁷¹ OPM has published a SORN for these record systems.⁷²

82. The information in the OPM Systems is retrieved by “an identifying particular” assigned to an individual.⁷³

83. The systems within OPM contain extensive personally identifiable information about individuals, including but not limited to Social Security number, employment history, and addresses.⁷⁴

Providing DOGE Representatives with Direct Access to Specific OPM Systems is a Disclosure Under the Privacy Act

84. Representatives of DOGE were granted access to personnel- and benefit-related systems within OPM and the records therein on or before January 31, 2025.⁷⁵ That access qualifies as a disclosure under the Privacy Act.

85. DOGE representatives within OPM have ““review[ed] position description level data,”” an act that would involve information retrieval from systems within OPM.⁷⁶

86. Disclosure can be written, oral, electronic, or a mechanical transfer between computers of record content.⁷⁷

87. None of the individual Plaintiffs, and on information and belief, none of the members of the Plaintiff Organizations requested disclosure or provided express written consent

⁷¹ *Privacy Policy*, U.S. Off. Personnel Mgmt., <https://www.opm.gov/information-management/privacy-policy/#url=PIAs>

⁷² *System of Records Notices (SORN)*, U.S. Off. Personnel Mgmt., <https://www.opm.gov/information-management/privacy-policy/#url=SORNs>.

⁷³ *OPM SORN GOVT-2 Employee Performance File System Records*, U.S. Off. Personnel Mgmt., <https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf>.

⁷⁴ See, e.g., *HIDW PIA*, *supra* note 59.

⁷⁵ See Tim Reid, *Exclusive: Musk Aides Lock Workers Out of OPM Computer Systems*, REUTERS (Feb. 2, 2025), <https://www.reuters.com/world/us/musk-aides-lock-government-workers-out-computer-systems-us-agency-sources-say-2025-01-31>.

⁷⁶ Ecarma & Legum, *supra* note 64.

⁷⁷ OMB Guidelines, 40 Fed. Reg. 28,948, 28,953 (July 9, 1975).

to the disclosure of their records and information to DOGE representatives. As such, Defendants' continued and ongoing disclosure of their records to DOGE representatives constitutes a violation of the Privacy Act, for which no exception applies.

DOGE Representatives Do Not Require Access to the FDS in the Performance of Their Duties

88. It has been reported that the DOGE representatives who have been provided by Defendants with access to the OPM systems are “political appointees” at OPM.⁷⁸ However, it has also been reported that DOGE representatives “have received official government credentials, including official email addresses, at multiple agencies.”⁷⁹ For example, some DOGE representatives in the Department of Education’s internal address book “also have GSA or OPM email addresses,” seemingly holding themselves out as employees of multiple agencies at the same time, while ultimately serving DOGE’s mission.

89. The Privacy Act’s exception for disclosures to employees who need the record “in the performance of their duties” does not apply to the disclosures here. On information and belief, DOGE’s purpose for accessing that data is to significantly “restructur[e]” the government by “push[ing]” out employees.⁸⁰

Defendants’ Disclosures of Specific OPM Systems to DOGE Officials is Not a “Routine Use” of the Protected Information

90. The Privacy Act’s “routine use” exception also does not apply. The SORNs for specific systems within OPM, namely USAJOBS, EHRI DW, USA Staffing, USA Performance, and HI DW, list 114 overlapping possible routine uses, none of which apply here.⁸¹

⁷⁸ Ecarma & Legum, *supra* note 64.

⁷⁹ Washington Post Staff, *Elon Musk’s DOGE Has Swept into 15 Federal Agencies. Here’s What to Know.*, WASH. POST (Feb. 8, 2025), <https://www.washingtonpost.com/business/2025/02/04/elon-musk-government-legal-doge>.

⁸⁰ *Id.*; Reuters, *Musk’s DOGE agents access sensitive government personnel data, Washington Post reports* (Feb. 6, 2025), available at <https://www.reuters.com/world/us/musks-doge-agents-access-sensitive-opm-personnel-data-washington-post-reports-2025-02-06/>.

⁸¹ See Privacy Act of 1974: Update and Amend System of Records, 79 Fed. Reg. 16834 (March 26, 2014); *OPM GOVT-2 Applicant Race, Sex National Origin, & Disability Status Records*, U.S. Off. Personnel Mgmt., <https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-7-applicant-race-sex-national-origin-and-disability-status-records.pdf>; Privacy Act of 1974: Update Existing System of Records, 77 Fed. Reg.

91. For example, representatives of DOGE are not accessing OPM records on behalf of a training facility, educational institution, foreign government official, agency adjudicating benefit claims, agency choosing to honor employees, labor organization official, the Merit Systems Protection Board, or the Equal Employment Opportunity Commission, among others.⁸²

92. Rather, on information and belief, representatives of DOGE intend to misuse OPM's systems to indiscriminately remove individuals from their positions en masse.⁸³ This is not a routine use listed in the SORNs.⁸⁴

93. None of the other statutory exceptions for disclosure of personal information set forth in the Privacy Act applies or would have applied to authorize Defendants' decision to disclose the sensitive information and data contained within the FDS to DOGE representatives.

Department of Education Student Loan Systems

94. The Department of Education (ED) is responsible for managing the federal student loan system through its Federal Student Aid (FSA) office. ED maintains several systems of record that support operation of the federal student loan system.

National Student Loan Data System

95. The National Student Loan Data System (NSLDS) is a comprehensive national database for the Federal financial aid program. "As the central database for Title IV student financial aid, NSLDS stores information about loans, grants, students, borrowers, lenders, guaranty agencies . . . , schools, and servicers. It provides detailed information on individuals

73694 (Dec. 11, 2012); *OPM GOVT-6 Personnel Research & Test Validation Records*, U.S. Off. Personnel Mgmt., <https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-6-personnel-research-and-test-validation-records.pdf>; *OPM SORN GOVT-2 Employee Performance File System Records*, U.S. Off. Personnel Mgmt., <https://www.opm.gov/information-management/privacy-policy/sorn/opm-sorn-govt-2-employee-performance-file-system-records.pdf>; Privacy Act of 1974; System of Records, 89 Fed. Reg. 72902 (Sep. 6, 2024).⁸² 77 Fed. Reg. 73694.

⁸³Ecarma & Legum, *supra* note 64.

⁸⁴ U.S. Off. Personnel Mgmt., *System of Records Notices (SORN)*, <https://www.opm.gov/information-management/privacy-policy/#url=SORNs>.

pertaining to their Title IV loans and grants during all stages of their aid life cycle, from approval through disbursement, repayment, default, and closure.”⁸⁵

96. The NSLDS contains sensitive PII about the tens of millions of Americans who apply for or receive Federal student aid, including Social Security Number, name, date of birth, address, phone number, email address, and driver’s license information, as well as demographic data about the borrower.⁸⁶

97. Personal data about a borrower’s parents or co-signers is also contained in the NSLDS. Among other things, it contains “information on the parent(s) of a dependent recipient, including name, date of birth, SSN, marital status, email address, highest level of schooling completed, and income and asset information.”⁸⁷

Common Origination and Disbursement System

98. The Common Origination and Disbursement System (CODS) processes information relating to determining eligibility for federal student aid.⁸⁸

99. The CODS includes records about aid applicants and recipients and their parents and spouses, including Social Security number, name, date of birth, mailing address, email address, driver’s license, and telephone number, and demographic information.⁸⁹

FUTURE Act System

100. The FUTURE Act System (FAS) is used to determine eligibility for, or repayment obligations under, various income-driven repayment plans for federal student loans.⁹⁰

101. FAS contains information about aid applicants, including last name, date of birth, Social Security number and/or Tax Identification Number. It also includes similar information

⁸⁵ See U.S. Dep’t of Educ., *Privacy Impact Assessment for the National Student Loan Data System (NSLDS-New)* at 4-5 (May 19, 2022), <https://www.ed.gov/sites/ed/files/notices/pia/pia-nslds-new.pdf>. The records on the NSLDS “legacy” system were transferred to a revamped NSLDS-New system in October 2022. *Id.*

⁸⁶ U.S. Dep’t of Educ., Notice of a Modified System of Records (“NSLDS SORN”), 87 Fed. Reg. 57,873, 57,878. ⁸⁷ *Id.* at 57,879.

⁸⁸ U.S. Dep’t of Educ., *Privacy Impact Assessment for the Common Origination & Disbursement System* (Sept. 29, 2023), <https://www.ed.gov/sites/ed/files/notices/pia/fsa-pia-cod.pdf>.

⁸⁹ U.S. Dep’t of Educ., Notice of a Modified System of Records (“CODS SORN”), 88 Fed. Reg. 41,942, 41,947 (June 28, 2023).

⁹⁰ U.S. Dep’t of Educ., *Privacy Impact Assessment for the Federal Tax Information Module* (June 4, 2024), <https://www.ed.gov/sites/ed/files/notices/pia/pia-ftim.pdf>.

about parents of dependent applicants and spouses of independent applicants, plus spousal income and asset information and parental income and asset information.⁹¹

Financial Management System

102. The Financial Management System (“FMS”) interfaces with other Federal Student Aid systems and consolidates and centralizes all Federal Student Aid accounting and financial data into one system. FMS contains personally identifying information about individual borrowers who are entitled to a refund of an overpayment or discharge, or both. The system includes a borrower’s Social Security number, name and address, amount of overpayment to be refunded and name of the loan holder.⁹²

DOGE’s Efforts to Improperly Access ED’s Systems

103. According to a report in the Washington Post, “roughly 20 people with Elon Musk’s ‘Department of Government Efficiency,’ known as DOGE, have begun working inside the Education Department, looking to cut spending and staff.”⁹³ The Washington Post has also written, “DOGE staffers have gained access to multiple sensitive internal systems, including a financial aid dataset that contains the personal information for millions of students enrolled in the federal student aid program.”⁹⁴ The access has “deeply alarmed” career staff.⁹⁵ On information and belief, the systems accessed include NSLDS, COGS, FAS and/or FMS.

104. It has been publicly reported that DOGE representatives “fed sensitive data from across the Education Department into artificial intelligence software to probe the agency’s programs and spending.”⁹⁶ The Washington Post has reported that “[t]he DOGE team plans to

⁹¹ U.S. Dep’t of Educ., Notice of a New System of Records (“FAS SORN”), 88 Fed. Reg. 42,220, 42,222 (June 29, 2023).

⁹² U.S. Dep’t of Educ., Notice of a New System of Records (“FMS SORN”), 73 Fed. Reg. 177, 177 (Jan. 2, 2008).

⁹³ Laura Meckler et al., *Trump Preps Order to Dismantle Education Dept. as DOGE Probes Data*, WASH. POST (Feb. 3, 2025), <https://www.washingtonpost.com/education/2025/02/03/trump-education-department-dismantling-executive-order-draft>.

⁹⁴ *Id.*

⁹⁵ Jeff Stein et al., *U.S. Government Officials Privately Warn Musk’s Blitz Appears Illegal*, WASH. POST (Feb. 4, 2025), <https://www.washingtonpost.com/business/2025/02/04/elon-musk-government-legal-doge>.

⁹⁶ Hannah Natanson et al., *Elon Musk’s DOGE Is Feeding Sensitive Federal Data into AI to Target Cuts*, WASH. POST (Feb. 6, 2025), <https://www.washingtonpost.com/nation/2025/02/06/elon-musk-doge-ai-department-education>.

replicate this process across many departments and agencies, accessing the back-end software at different parts of the government and then using AI technology to extract and sift through information about spending on employees and programs.”

Defendants’ Disclosure of Information in ED’s Systems to DOGE Officials Violates the Privacy Act

The ED Systems are Systems of Record

105. NLSDS, COGS, FAS, and FMS (collectively, the “ED Systems”) are each a system of records, and ED has published a SORN describing each system’s purposes and uses.⁹⁷

106. The information in each of the ED Systems is retrieved by the name of the individual or other “identifying particular” assigned to an individual.⁹⁸

107. ED’s systems contain extensive personally identifiable information about individuals, including but not limited to Social Security number, sensitive financial information, and address.

Providing DOGE Representatives with Direct Access to ED Systems is a “Disclosure” Under the Privacy Act

108. On information and belief, Defendants Acting Secretary of Education Denise Carter and the Department of Education granted representatives of DOGE access to ED Systems on or before February 3, 2025. That access qualifies as a disclosure under the Privacy Act.

109. None of the individual Plaintiffs, and on information and belief, none of the members of the Plaintiff Organizations requested disclosure or provided express written consent to the disclosure of their records and information to DOGE representatives.

“Feeding” ED Systems Data to Unvetted AI Tools Is Likewise a “Disclosure” Under the Privacy Act

110. Public reporting has revealed that DOGE has begun “feeding” ED data into artificial intelligence tools, including “data with personally identifiable information for people

⁹⁷ See NLSDS SORN, CODS SORN, FAS SORN, FMS SORN.

⁹⁸ NLDS SORN, 87 Fed. Reg. 57,873, 57,881; CODS SORN, 88 Fed. Reg. 41,942, 41,950; FAS SORN, 88 Fed. Reg. 42,220, 42,225; FMS SORN, 73 Fed. Reg. 177, 179.

who manage grants, as well as sensitive internal financial data.”⁹⁹ Reporting also indicates that DOGE plans to use artificial intelligence programs to analyze data retrieved from additional agency systems.¹⁰⁰ The AI tools DOGE is using to analyze agency data are reportedly hosted on cloud-based computers that are located outside of federal-government facilities.¹⁰¹

111. Feeding ED Systems data into DOGE’s AI tools constitutes additional unauthorized disclosures of data to the pur-based computers and operators of those systems.¹⁰²

DOGE Representatives Do Not Require Access to ED Systems in the Performance of their Duties

112. The Privacy Act carves out an exception for disclosures without prior written consent to “officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties.”

113. The Privacy Act’s exception for disclosures to employees who need the record “in the performance of their duties” does not apply.

114. Disclosure of data housed in any of the ED Systems to DOGE representatives is not necessary for the performance of the duties of ED employees or officials.

115. The data stored on ED Systems is collected and maintained to enable administration of the student loan system under Title IV of the Higher Education Act.¹⁰³

116. DOGE and its representatives’ access to ED Systems has a very different purpose: Musk has boasted online that DOGE is advancing President Trump’s aim to “end[] the federal Department of Education.”¹⁰⁴ Musk’s claim comes after President Trump “repeatedly vowed to shutter the federal agency” on the campaign trail and announced after taking office that he

⁹⁹ See Natanson, *supra* n.102.

¹⁰⁰ *Id.*

¹⁰¹ *Id.*

¹⁰² *Id.*

¹⁰³ NLDS SORN, 87 Fed. Reg. 57,873, 57,877-78; CODS SORN, 88 Fed. Reg. 41,942, 41,945-46; FMS SORN, 73 Fed. Reg. 177, 178; FAS SORN, 88 Fed. Reg. 42,220, 42,221-22.

¹⁰⁴ Elon Musk (@elonmusk), X (Feb. 3, 2025, 8:30 PM), <https://x.com/elonmusk/status/1886633448078475593>; see also Meckler et al., *supra* note 92 (noting that DOGE access “is a prelude to a more dramatic effort to make good on one of Trump’s campaign promises: eliminating the Education Department altogether”).

expects his nominee for Secretary of Education to “put herself out of a job.”¹⁰⁵ On February 7, 2025, after DOGE officials had gained access to ED systems, Musk claimed that the department “doesn’t exist.”¹⁰⁶

Defendants’ Disclosures of ED Systems Information to DOGE Officials is Not a “Routine Use” of the Protected Information

117. The Privacy Act’s “routine use” exception also does not apply.

118. The SORN for NSLDS lists 14 routine uses, none of which apply here.

119. The routine uses for NSLDS generally fall into several broad categories: uses related to administration of the loan program; disclosures to enable enforcement by agencies “charged with the responsibility of investigating or prosecuting” specific violations; litigation or alternative disputes resolution procedures; disclosures required under the Freedom of Information Act or Privacy Act; contract-related disclosures; employment- or benefit-related matters; employee grievance proceedings; labor organization disclosure; disclosures to the Justice Department or OMB; disclosures in the course of responding to a data breach; disclosures in assisting another agency responding to a data breach; and disclosures to the National Archives and Records Administration.¹⁰⁷

120. None of the routine uses listed by the NSLDS SORN contemplate data access for the purpose of dismantling the Department of Education.

121. None of the routine uses listed by the NSLDS SORN contemplate “feeding” data into artificial intelligence systems, and certainly not for the purpose of dismantling the Department of Education.

122. As alleged above, DOGE officials are accessing the ED Systems for purposes of destroying ED, not for any of the purposes identified in the NSLDS SORN.

¹⁰⁵ Zachary Schermele, *President Trump Says He Wants His Education Secretary to ‘Put Herself out of a Job’*, USA TODAY (Feb. 4, 2025), <https://www.usatoday.com/story/news/education/2025/02/04/trump-education-department-mcmahon/78220522007>.

¹⁰⁶ Elon Musk (@elonmusk), X (Feb. 7, 2025, 5:34 PM), <https://x.com/elonmusk/status/1888038615780909178>.

¹⁰⁷ NLDS SORN, 87 Fed. Reg. 57,873, 57,879-81.

123. The SORN for CODS lists 15 routine uses, none of which apply here. The routine uses for CODS are similar to those for NSLDS.¹⁰⁸

124. As alleged above, DOGE officials are accessing the ED Systems for purposes of destroying ED, not for any of the purposes identified in the CODS SORN.

125. The SORN for FAS lists 15 routine uses, none of which apply here. The routine uses for FAS are similar to those for NSLDS and CODS.¹⁰⁹

126. As alleged above, DOGE officials are accessing the ED Systems for purposes of destroying ED, not for any of the purposes identified in the FAS SORN.

127. The SORN for FMS lists 10 routine uses, none of which apply here. The routine uses for FAS are similar to those for NSLDS, CODS, and FAS.¹¹⁰

128. As alleged above, DOGE officials are accessing the ED Systems for purposes of destroying ED, not for any of the purposes identified in the FMS SORN.

129. The use of the records contained in ED Systems to dismantle ED is incompatible with any legitimate duties of the Department and with the purpose for which the records were collected and maintained.

130. None of the other statutory exceptions for disclosure of personal information set forth in the Privacy Act applies or would have applied to authorize Defendants' decision to disclose the sensitive information and data contained within the ED to DOGE representatives.

Defendants' Disclosure of Protected Data to DOGE Employees Is Unprecedented

131. Defendants and DOGE have turned the data systems that enable the government to function into a weapon to dismantle the government from the inside. Indeed, Mr. Musk exults the non-routine nature of DOGE. In response to a post on X that said "DOGE is speedrunning government reform--\$4B/day cuts could start THIS weekend. Bureaucracy never saw it

¹⁰⁸ CODS SORN, 88 Fed. Reg. 41,942, 41,948-50.

¹⁰⁹ FAS SORN, 88 Fed. Reg. 42,220, 42,223-25.

¹¹⁰ FMS SORN, 93 Fed. Reg. 177, 178-79.

coming[,]” Musk seemed to agree, explaining: “Very few in the bureaucracy actually work the weekend, so it’s like the opposing team just leaves the field for 2 days!”¹¹¹

132. As DOGE’s intrusion into Plaintiffs’ sensitive data is unprecedented, Defendants’ disclosures cannot constitute “routine use” authorized by the Privacy Act.¹¹² When these systems are used for routine purposes, access is usually very restricted.¹¹³ For instance, “the aggregate information contained in the OPM databases is so sensitive, said a U.S. official, that even White House requests for certain types of data were rebuffed under previous administrations.”¹¹⁴

133. Defendants are disclosing protected data to DOGE representatives not to advance their agencies’ respective agendas, but to advance the DOGE agendas. Destroying Congressionally-established federal agencies is not a “routine use” of these systems. Identifying entire programs to eliminate is not a “routine use” of these systems. And feeding Americans’ PII into private artificial intelligence systems is not a “routine use” of these systems.

Defendants’ Disclosure of Protected Data Has Harmed and Will Continue to Harm Plaintiffs

134. President Gerald Ford, who signed the Privacy Act into law, described the Act as codifying this country’s long-held commitment to “safeguard personal privacy.” Indeed, the Act mandates that the government “protect the right of privacy for every American.” Defendants’ unauthorized access and disclosure of that information to DOGE representatives violates Plaintiffs’ rights under the Privacy Act. It has also exposed Plaintiffs’ sensitive information to serious risk.

¹¹¹ Elon Musk (@elonmusk), X (Feb. 1, 2025 3:37 PM), <https://x.com/elonmusk/status/1885789468713476492>.

¹¹² Charlie Warzel & Ian Bogost, *The Government’s Computing Experts Say They are Terrified*, *The Atlantic* (Feb. 7, 2025), <https://www.theatlantic.com/technology/archive/2025/02/elon-musk-doge-security/681600/>.

¹¹³ *Id.*

¹¹⁴ Isaac Stanley-Becker et al., *Musk’s DOGE Agents Access Sensitive Personnel Data, Alarming Security Officials*, *Wash. Post* (Feb. 6, 2025), https://www.washingtonpost.com/national-security/2025/02/06/elon-musk-doge-access-personnel-data-opm-security/?utm_campaign=wp_post_most&utm_medium=email&utm_source=newsletter&carta-url=https%3A%2F%2Fs2.washingtonpost.com%2Fcar-ln-tr%2F40f0f54%2F67a4ea66cd86f13ee737dd6e%2F5972aa5bade4e21a84818a4e%2F14%2F60%2F67a4ea66cd86f13ee737dd6e.

135. Plaintiffs, like many millions of Americans since the Act’s passage, rely on the protections enshrined in the Privacy Act to safeguard their sensitive information housed in the systems described in this Complaint. Defendants’ actions have run roughshod over those protections. Cyber security experts warn that Defendants’ actions pose several extreme risks. “As one administrator for a federal agency with deep knowledge about the government’s IT operations told [the *Atlantic*], “I don’t think the public quite understands the level of danger.”¹¹⁵

136. According to public reporting, a Treasury Department internal threat analysis has designated DOGE to be an “insider threat.”¹¹⁶ The Bureau of Fiscal Service’s threat intelligence team recommended “suspending [DOGE’s] access immediately and conducting a comprehensive review of all actions they may have taken on these systems.”¹¹⁷ The internal Treasury report went on, “Continued access to any payment systems by DOGE members, even ‘read only,’ likely poses the single greatest insider threat risk the Bureau of the Fiscal Service has ever faced.”¹¹⁸

137. The chaotic¹¹⁹ and secretive¹²⁰ process by which DOGE representatives have gained access to protected data—sometimes without proper vetting or security clearances¹²¹—increases Plaintiffs’ concern about additional risks of unauthorized disclosure. Even “read only” access allows users to copy and transfer Plaintiffs’ protected data into other systems—without limitation.¹²²

¹¹⁵ Charlie Warzel & Ian Bogost, *The Government’s Computing Experts Say They are Terrified*, *The Atlantic* (Feb. 7, 2025), <https://www.theatlantic.com/technology/archive/2025/02/elon-musk-doge-security/681600/>.

¹¹⁶ Vittoria Elliott & Leah Feiger, *A US Treasury Intelligence Analysis Designates DOGE Staff as ‘Insider Threat’*, *Wired* (Feb. 7, 2025), <https://www.wired.com/story/treasury-bfs-doge-insider-threat/>.

¹¹⁷ *Id.*

¹¹⁸ *Id.*

¹¹⁹ Makena Kelly, *DOGE Staff Had Questions About the ‘Resign’ Email. Their New HR Chief Dodged Them*, *Wired* (Feb. 1, 2025), <https://www.wired.com/story/doge-hr-elon-musk-resignation-fork-road-leaked-staff-meeting/>.

¹²⁰ Vittoria Elliott et al., *The US Treasury Claimed DOGE Technologist Didn’t Have “Write Access” When He Actually Did*, *Wired* (Feb. 6, 2025), <https://www.wired.com/story/treasury-department-doge-marko-elez-access/>.

¹²¹ Nick Schwellenbach, *Elon Musk’s DOGE Teams Raise Vetting, Ethic Concerns*, *Project on Government Oversight* (Feb. 6, 2025), <https://www.pogo.org/investigations/elon-musks-doge-teams-raise-vetting-ethics-concerns>.

¹²² Charlie Warzel & Ian Bogost, *The Government’s Computing Experts Say They are Terrified*, *The Atlantic* (Feb. 7, 2025), <https://www.theatlantic.com/technology/archive/2025/02/elon-musk-doge-security/681600/>.

138. At least one DOGE representative has been publicly reported to have been a member of cybercrime communities¹²³ and was reported to have been previously fired from a cybersecurity firm for leaking company secrets.¹²⁴ It has also been widely reported that DOGE representatives are using non-government issued devices to connect to government servers, which significantly increases the risk of hacking.¹²⁵

139. Exacerbating the risk of additional unauthorized access to Plaintiffs' private records is the planned introduction of the at-issue data into artificial intelligence systems. The security risks associated with AI are well-documented. President Biden issued an Executive Order on October 30, 2023—which President Trump has since rescinded—identifying the “extraordinary potential” for “peril” associated with use of AI, including but not limited to “fraud, discrimination, bias, and disinformation” and creating risks “to national security.”¹²⁶ Notwithstanding this, Defendants and DOGE representatives have adopted a “move fast and break things” “AI-first strategy” that has already resulted in the sharing of sensitive Education Department information with AI software with additional AI uses likely to follow.¹²⁷

140. Defendants' unlawful disclosures of Plaintiffs' data to DOGE representatives has caused Plaintiffs major distress and anxiety, as they do not know who their data has been or will be shared with, whether these disclosures have made them vulnerable to further privacy breaches, and how it may be weaponized against them. They are concerned that as a result of the

¹²³ Brian Krebs, *Teen on Musk's DOGE Team Graduated from 'The Com'*, Krebs on Security (Feb. 7, 2025), <https://krebsonsecurity.com/2025/02/teen-on-musks-doge-team-graduated-from-the-com/>.

¹²⁴ Jason Leopold et al., *Musk's DOGE Teen Was Fired By Cybersecurity Firm for Leaking Company Secrets*, Bloomberg (Feb. 7, 2025), <https://www.bloomberg.com/news/articles/2025-02-07/musk-s-doge-teen-was-fired-by-cybersecurity-firm-for-leaking-company-secrets?accessToken=eyJhbGciOiJIUzI1NiIsInR5cCI6IkpXVCJ9.eyJzbnVzIjY2UiOiJTdWJzY3JpYmVzR2lmdGVkQXJ0aWNsZSIsImVudCI6MTczODk1NzQyNCwiZXhwIjoxNzU5NTYyMjI0LCJhcnRpY2xlSWQiOiJTUkxMTlUMVVNMfFwMCI6ImJjb25uZW50SWQiOiIyQjE3NzFFOTIEODc0QzRDOTY1Njg1RTZBQkJKGM0QwRRCJ9.vxGv4ncXEbIUGmUYpTUdxLmCVDwzmEWp-VRWV9otME&leadSource=uverify%20wall>.

¹²⁵ Cynthia Brumfield, *Musk's DOGE effort could spread malware, expose US systems to threat actors*, CSO (Feb. 4, 2025), <https://www.csoonline.com/article/3815925/musks-doge-effort-could-spread-malware-expose-us-systems-to-threat-actors.html>.

¹²⁶ Exec. Order No. 14,110, 88 Fed.Reg. 75,191 (Nov. 1, 2023).

¹²⁷ Victor Tangermann, *Elon Musk's DOGE Training an AI to Analyze Government Spending*, Futurism (Feb. 7, 2025), <https://futurism.com/elon-musk-doge-ai-government>; Natanson, *supra* n. 103.

unlawful disclosures, they will be subject to harassment, intimidation, and economic and reputational harm. These harms are ongoing and will continue absent judicial intervention.

Ongoing Litigation

141. On February 3, several unions and membership associations sued Defendants Bessent and Department of the Treasury in Federal District Court of the District of Columbia asserting Privacy Act violations based on DOGE access to FDS systems. On February 6, the judge in that case deferred ruling on the plaintiffs' motion for a temporary restraining order on the basis of an agreement among the parties limiting access to FDS records to specific Treasury Department officials, as well as Krause and Elez, "until such time as the Court rules on the Plaintiffs' forthcoming Preliminary Injunction Motion."

142. On February 7, 2025, the attorneys general of 19 states filed a lawsuit against President Trump and Defendants Bessent and Department of the Treasury in the Southern District of New York challenging the defendants' policy to expand the Bureau of Fiscal Services' access to political appointees and Special Government Employees. The States allege that the policy violates the Privacy Act, APA, separation of powers doctrine, and the Take Care Clause of the United States Constitution.

143. On February 8, 2025, the judge in that case granted the plaintiffs' motion for a temporary restraining order, restraining the defendants from granting access to any Treasury Department data system containing PII to any political appointee, Special Government Employee, or detailee from another agency, and ordering them to direct any person who has already received such access to immediately destroy any and all copies of material downloaded from Treasury Department systems.

144. Despite the existence of these other lawsuits, Plaintiffs anticipate additional disclosures of their protected data as DOGE continues its plans to expand its reach within the agencies.

COUNT I – Violation of APA

(Not in accordance with law)

145. The APA directs courts to hold unlawful and set aside agency actions that are found to be arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law. 5 U.S.C. § 706(2)(A).

146. The Privacy Act prohibits Defendants from disclosing records on individuals to any person without the individual's consent except in specified circumstances, none of which are present here. 5 U.S.C. § 552a(b).

147. Defendants have granted DOGE representatives ongoing access to their systems of records containing sensitive and personal data.

148. Defendants have disclosed Plaintiffs' records and the records of Plaintiffs' members to DOGE representatives without obtaining their consent.

149. Defendants have disclosed Plaintiffs' records and the records of Plaintiffs' members to DOGE representatives for uses other than the routine uses specified in the applicable SORNs.

150. Defendants' actions violate the prohibitions in the Privacy Act and are therefore not in accordance with law.

151. An individual action against Defendants for damages under the Privacy Act would not cause Defendants to end the unlawful disclosure of Plaintiffs' and their members' records to DOGE Representatives, including future DOGE Representatives. Defendants' action is "final agency action for which there is no other adequate remedy in a court" and is therefore subject to judicial review. 5 U.S.C. §§ 702, 704.

COUNT II – Violation of APA

(Arbitrary and capricious)

152. The APA directs courts to hold unlawful and set aside agency actions that are found to be arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law. 5 U.S.C. § 706(2)(A).

153. Defendants have failed to consider the consent requirements of the Privacy Act, 5 U.S.C. § 552a(b), and their duty to protect the sensitive data on their systems, 5 U.S.C. §

552a(e)(1); the risks that their disclosures would result in corrupted data; and the security threats that are likely to result from their action.

154. Defendants failed to engage in reasoned decision-making to grant DOGE representatives sweeping access to their systems of records containing sensitive and personal data for the purposes of advancing the DOGE agenda.

155. Because Defendants have failed to consider an important aspect of the problem, failed to engage in reasoned decision-making, and offer explanations that run counter to the evidence before them, Defendants' actions are arbitrary and capricious.

156. An individual action against Defendants for damages under the Privacy Act would not cause Defendants to end the unlawful disclosure of Plaintiffs' and their members' records. Defendants' action is "final agency action for which there is no other adequate remedy in a court" and is therefore subject to judicial review. 5 U.S.C. §§ 702, 704.

COUNT III – Violation of APA

(Excess of statutory authority)

157. The APA directs courts to hold unlawful and set aside agency actions in excess of statutory authority. 5 U.S.C. § 706(2)(C).

158. Defendants have a non-discretionary duty to protect records on individuals from unauthorized disclosure.

159. Defendants' action to grant DOGE representatives access to their systems of records containing sensitive and personal data violates that duty.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs pray that this Court:

- a. Declare that Defendants acted unlawfully in disclosing records protected by the Privacy Act to DOGE representatives.
- b. Enjoin Defendants from continuing to permit such access or otherwise obtain such information.

- c. Enjoin Defendants to ensure that there is no further unauthorized use or dissemination resulting from the unauthorized disclosures.
- d. Enjoin Defendants to retrieve or ensure the destruction of any copies of any records that were unlawfully disclosed.
- e. Enjoin Defendants to ensure that future disclosure of individual records will occur only in accordance with the Privacy Act and the SORNs applicable to the system of records at issue.
- f. Grant any temporary, preliminary, or permanent injunctive relief necessary to protect the privacy of individuals whose information is contained within the system of records.
- g. Award Plaintiffs their costs and attorneys' fees for this action; and
- h. Grant any other relief as this Court deems appropriate.

DATED: February 12, 2025

By: /s/ Mark Hanna

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

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

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

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

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

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

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

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

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

Attorneys for Plaintiffs

CERTIFICATE OF SERVICE

I hereby certify that on this 12th day of February, 2024, copies of the Amended Complaint and Redlined Amended Complaint were filed via CM/ECF, emailed to Department of Justice attorneys involved in other litigation, and sent via overnight delivery to the following:

Attorney General of the United States
U.S. Department of Justice
950 Pennsylvania Avenue, NW
Washington, DC 20530-0001

Civil Process Clerk
U.S. Attorney's Office for D.C.
601 D Street, NW
Washington, DC 20530

Erek Barron
United States Attorney for the District of Maryland
36 S. Charles Street, 4th Fl.
Baltimore, MD 21201

Scott Bessent
Secretary of the Treasury
1500 Pennsylvania Ave. NW
Washington, DC 20220

Department of the Treasury
1500 Pennsylvania Ave. NW
Washington, DC 20220

Charles Ezell
Acting Director of the Office of Personnel Management
1900 E St. NW
Washington, D.C. 20415

U.S. Office of Personnel Management
1900 E St. NW
Washington, D.C. 20415

Denise Carter
Acting Secretary of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

U.S. Department of Education
400 Maryland Avenue, SW
Washington, D.C. 20202

Dated: February 12, 2025

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

Xiaonan April Hu