UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF VIRGINIA
ALEXANDRIA DIVISION

ELECTRONIC PRIVACY INFORMATION CENTER, DOE 1, *Plaintiffs*, v. U.S. OFFICE OF PERSONNEL MANAGEMENT, *et al.*, *Defendants*.	No. 1:25-cv-00255-RDA-WBP

PLAINTIFFS' MEMORANDUM
IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

The federal government collects and promises to protect vast stores of sensitive information about tens of millions of people, including Plaintiffs. This promise is buttressed by multiple federal laws requiring the government to safeguard this information, assuring the American public their personal information is safe. These laws, some of which date back to the post-Watergate era, explicitly restrict unauthorized disclosures *within* the government as well as externally. Defendants' wholesale disregard of these protections to disclose sensitive personal information about tens of millions of people to the so-called "Department of Government Efficiency" is unlawful. This Court has jurisdiction to review Defendants' new policies and ensure that Americans' data is protected as required by law.

BACKGROUND

On January 20, 2025, President Trump signed Executive Order 14,158*, Establishing and Implementing the President's "Department of Government Efficiency,"* 90 Fed. Reg. 8441 (Jan. 29, 2025) ("the EO"), reorganizing and renaming the United States Digital Service as the United States DOGE Service, and creating the U.S. DOGE Service Temporary Organization (collectively, "DOGE"), in the Executive Office of the President. Individuals working for or affiliated with DOGE rapidly obtained unprecedented and unlawful access to government systems containing troves of personally identifiable information ("PII") about tens of millions of individuals. Leadership at many agencies, including the Office of Personnel Management ("OPM") and Department of Treasury ("Treasury"), acquiesced or actively assisted in securing that access. Treasury and OPM systems to which DOGE gained access contain, among other things, Social Security numbers, taxpayer ID numbers, financial information, dates of birth, addresses, medical/health information, and information about marital status, children, mental health, and disabilities. First Am. Compl. ¶¶ 67, 110, 113 (ECF No. 51) ("FAC").

Plaintiffs Electronic Privacy Information Center, a nonprofit dedicated to focusing attention on emerging privacy and civil liberties issues, and Doe 1, a federal employee, sued, challenging DOGE's unlawful access to Treasury and OPM systems of records. Plaintiffs allege the Defendant agencies violated the Administrative Procedure Act, Privacy Act, Internal Revenue Code, and Plaintiffs' constitutional right to privacy by granting DOGE systems access, and that DOGE acted *ultra vires* and violated the separation of powers in accessing the systems.

STANDARD OF REVIEW

In considering a Rule 12(b)(1) motion, "the facts alleged in the complaint are taken as true, and the motion must be denied if the complaint alleges sufficient facts to invoke subject matter jurisdiction." *Ziegler v. Dunn*, No. 3:23-cv-00480, 2024 WL 761860, at *2 (E.D. Va. Feb. 23, 2024) (quoting *Kerns v. United States*, 585 F.3d 187, 192 (4th Cir. 2009)). Likewise, for a Rule 12(b)(6) motion, courts consider "only whether the complaint states a claim to relief that is plausible on its face," construing "facts in the light most favorable to the plaintiff" and "draw[ing] all reasonable inferences in his favor." *United States ex rel. Oberg v. Pa. Higher Educ. Assistance Agency*, 745 F.3d 131, 136 (4th Cir. 2014) (internal quotations and citations omitted).

ARGUMENT

Plaintiffs have standing to vindicate their rights against Defendants for the ongoing breach of their personal information and have adequately pled causes of action to do so. Plaintiffs have suffered injury-in-fact, and they have plausibly pled violations of the Administrative Procedure Act, Privacy Act, and the constitutional right to privacy, and that DOGE is operating in excess of its legal authority.

I. Plaintiffs have suffered an injury-in-fact.

To satisfy the "irreducible constitutional minimum of standing," *Lujan v. Defs. of Wildlife*, 504 U.S. 555, 560 (1992), Plaintiffs must show they have suffered an injury-in-fact traceable to

Defendants' actions and redressable by a favorable decision. Defendants do not contest causation and redressability, and their arguments that Plaintiffs have not pled an injury-in-fact are wrong.[1]

Defendants' invasion of Plaintiffs' privacy by wrongfully disclosing personal information to DOGE is injury-in-fact closely related "to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *Fernandez v. RentGrow, Inc.*, 116 F.4th 288, 296 (4th Cir. 2024) (internal citations and quotation marks omitted). Such injuries include "reputational harms, disclosure of private information, and *intrusion upon seclusion*." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021) (emphasis added), and "breach of confidence," *Am. Fed'n of Lab. & Cong. of Indus. Orgs. v. Dep't of Lab.*, No. 1:25-cv-00339, 2025 WL 1129227, at *9 (D.D.C. Apr. 16, 2025) ("*AFL-CIO v. DOL*") (internal citations and quotation marks omitted).

A. Improper access to sensitive records is textbook intrusion upon seclusion.

Intrusion upon seclusion is an intentional tort of intrusion "physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns . . . [which] would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B (Am. L. Inst. 1977). The tort' roots are in Samuel Warren and Louis Brandeis's article *The Right to Privacy*, which first crystallized privacy as the right "to be let alone." 4 Harv. L. Rev. 193, 193 (1890); *see also* William L. Prosser, *Privacy*, 48 Cal. L. Rev. 382, 389 (Aug. 1960) (identifying "[i]ntrusion upon the plaintiff's seclusion or solitude, or into his private affairs" as one of four invasion of privacy torts). Intrusion upon seclusion may result from "investigation or examination into [one's] private concerns, as by opening his private and personal mail, searching his safe or his wallet, examining

[1] Defendants evidently concede, as they must, that Defendants' unlawful actions caused Plaintiffs' injuries, and that a favorable decision will remedy those injuries. *See* Defs.' Mem. in Supp. of Mot to Dismiss at 6–11 (ECF No. 55) ("MTD"). Nor do Defendants contest that Plaintiffs have adequately pled standing for their constitutional claim.

his private bank account, or compelling him by a forged court order to permit an inspection of his personal documents." Restatement § 652B, cmt. b. Notably, "the intrusion itself" triggers liability, even if there is no "publication or other use of any kind" of the information discovered. *Id.*

Courts recognize wrongful access to financial, employment, and medical records is a "highly offensive" intrusion into "private affairs." *Id.*; *see, e.g.*, *Randolph v. ING Life Ins. & Annuity Co.*, 973 A.2d 702, 710 (D.C. 2009) (SSN "and other identifying information"); *Toomer v. Garrett*, 574 S.E.2d 76, 90 (N.C. App. 2002) (personnel file, "medical diagnoses and financial information"). Injuries analogous to intrusion upon seclusion may work "intangible" but "concrete" harm sufficient for standing. *TransUnion,* 594 U.S. at 425; *see Garey v. James S. Farrin, P.C.*, 35 F.4th 917, 921–22 (4th Cir. 2022) (access to personal information in violation of statute constituted injury "closely related to the invasion of privacy, which has long provided a basis for recovery at common law"); *Persinger v. S.W. Credit Systems*, *L.P.,* 20 F.4th 1184, 1192 (7th Cir. 2021) (accessing credit information without permissible purpose in violation of statute resembled "harm associated with intrusion upon seclusion" sufficiently for standing); *Nayab v. Capital One Bank, N.A.*, 942 F.3d 480, 487, 492 (9th Cir. 2019) (access to credit report in violation of statute causes "same harm" as "the basis for the tort of intrusion upon seclusion"); *Rendon v. Cherry Creek Mortg., LLC*, No. 3:22-cv-01194, 2022 WL 17824003, at *3–4 (S.D. Cal. Dec. 20, 2022) ("*Nayab* remains precedential" after *TransUnion* and injury of unauthorized credit inquiry is "sufficient 'in kind' to harm suffered by intrusion upon seclusion" to support standing).

Another court in this Circuit, after exploring extensive case law and history, recently held that injury arising from a federal agency disclosing individuals' personal information to DOGE "if unauthorized, or without adequate need, is surely sufficiently offensive so as to constitute concrete harm" and thus "sufficiently analogous to the tort of intrusion upon seclusion" to constitute injury-

in-fact. *See Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, No. 1:25-cv-00596, 2025 WL 1141737, at *42 (D. Md. Apr. 17, 2025) ("*AFSCME*"). That ruling accords with numerous others holding unlawful agency disclosures of personal information to DOGE to work harm closely analogous to intrusion upon seclusion, thus conferring standing. *See AFL-CIO v. DOL*, 2025 WL 1129227, at *7 ("As three judges facing nearly identical issues have explained, the harm that plaintiffs allege their members are suffering has a close relationship with the harm asserted in a suit for the tort of intrusion upon seclusion."); *accord Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, No. 1:25-cv-00596, 2025 WL 868953, at *35 (D. Md. Mar. 20, 2025); *All. for Ret. Ams. v. Bessent*, No. 1:25-cv-00313, 2025 WL 740401, at *15–17 (D.D.C. Mar. 7, 2025); *Am. Fed'n of Gov't Emps., AFL-CIO v. Off. of Personnel Mgmt.*, No. 1:25-cv-01237, 2025 WL 996542, at *5 (S.D.N.Y. Apr. 3, 2025) ("*AFL-CIO v. OPM"*). [2]

This case is no different. Plaintiffs have adequately alleged that Treasury and OPM Defendants' wrongful disclosure to DOGE affiliates of their sensitive financial, personnel, and other records—including health and mental health information—harms their privacy interests. FAC ¶¶ 67, 100, 139, 145. Such disclosure is closely analogous to the type of "investigation or examination into [one's] private concerns" that constitutes intrusion upon seclusion—a close correlate to "opening [one's] private and personal mail, searching his safe or his wallet, examining

[2] The *en banc* Fourth Circuit denied a stay of the *AFSCME* district court's preliminary injunction, *Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, No. 25-1411, 2025 WL 1249608 (4th Cir. Apr. 30, 2025), with a seven-judge concurrence recognizing, among other things, SSA's commitment to protecting personal information, *id.* at *2 (King, J., concurring) and the scope and volume of disclosed information, *id.* at *4 (King, J. concurring). The Supreme Court then stayed the preliminary injunction, *SSA v. Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO*, No. 24A1063, 2025 WL 1602349 (June 6, 2025), but did not provide reasoning applicable to this, or any other, case. *En banc* appeal of the preliminary injunction is pending in the Fourth Circuit. Importantly, the government articulated a clearer purported "need" for access to data in *AFSCME* than here, and no court to consider the *AFSCME* case has determined whether disclosures to DOGE constitute intra-agency disclosures for the purposes of the Privacy Act.

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 it is highly offensive to a reasonable person because "in our society, PII, such as SSNs, medical and mental health information, and certain financial records, are regarded as private, sensitive, and confidential information." *AFSCME*, 2025 WL 1141737, at *40. The Privacy Act in particular "created a new sphere" where Americans "not only *expect* privacy, but have a right to it"—"even if the sphere literally encompasses only one row of millions in a dataset." *AFL-CIO v. DOL*, 2025 WL 1129227, at *8.

Defendants' reliance on *American Federation of Teachers v. Bessent*, No. 25-1282, 2025 WL 1023638 (4th Cir., Apr. 7, 2025), is unavailing. First, Plaintiffs allege more than just the "abstract access to personal information," *id.* at *2 (Agee, J., concurring), described by Judge Agee in *Bessent*; rather, the Complaint alleges that Plaintiffs' personal information was actually disclosed and made known to DOGE and its affiliates in violation of federal law, causing fear, unease, and offense. FAC ¶¶ 3, 4, 6, 83, 116, 118, 128, 135, 139, 143, 149, 156. Second, like the plaintiffs in *AFSCME*, Plaintiffs allege that the personal data unlawfully disclosed to DOGE by the OPM and Treasury Defendants include large volumes of sensitive financial and medical information. FAC ¶¶ 67, 110, 113. The distinction, as Judge Hollander explained in *AFSCME*, is dispositive:

> If receiving a single unwanted text message or phone call is sufficiently offensive to constitute concrete harm for standing purposes, in the context of intrusion upon seclusion . . . providing the DOGE Team with access to the medical records and sensitive financial information of millions of people, if unauthorized, or without adequate need, is surely sufficiently offensive so as to constitute concrete harm.

AFSCME, 2025 WL 1141737, at *81. So too here.

Defendants argue that *Bessent* is more applicable here than *AFSCME* because *AFSCME* concerned Social Security records of "millions upon millions of American citizens." MTD at 10 (citing *Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, 2025 WL 1249608, at *4 (King,

J., concurring)). But that only reveals that *AFSCME* is on all fours with this case. *AFSCME* concerned "a wide swath of confidential and sensitive PII, such as medical and mental health records, financial and bank information, tax records, work histories, birth certificates, and personal records concerning children." *Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, No. 1:25-cv-00596, 2025 WL 1206246, at *31 (D. Md. Apr. 17, 2025). That is exactly what is at stake here: BFS holds SSNs, personal financial information, tax returns, addresses, marital statuses, information on children, medical and health information, mental health information, disability information, and other records of up to 100 million American taxpayers, FAC ¶ 67; EHRI and other OPM systems contain similar records of the millions of Americans who have applied to work for the federal government, FAC ¶¶ 110, 113. By contrast, the *Bessent* plaintiffs only alleged disclosure of certain identifying information of "two million or so plaintiffs." *Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, 2025 WL 1249608, at *4 (King, J., concurring) (citing *Am. Fed'n of Tchrs. v. Bessent*, No. 8:25-cv-00430, 2025 WL 895326 (D. Md. Mar. 24, 2025)).

B. Plaintiffs have suffered unease caused by unwarranted access

Plaintiffs have suffered "the feeling of unease when and where one should ideally be at peace" from disclosure of their personal information—the precise ill the *Bessent* court identified at the core of intrusion upon seclusion. *Bessent*, 2025 WL 1023638, at *4. They have "significant fear" about both "misuse of [their] information by those who have accessed it," and increased "vulnerability . . . to further theft" and "risk of identity theft." Declaration of Doe 1 ¶ 10 (ECF No. 20-1) ("Doe Decl."). Defendants argue that "not just any 'feeling of unease will do.'" MTD at 9 (citing *Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, 2025 WL 1249608, at *7 (Richardson, J., dissenting). But like the *AFSCME* plaintiffs, Plaintiffs have "described the kind of 'unease' that Judge Richardson regards as integral to an intrusion upon seclusion claim" by

alleging "anxiety" and "distress" from "DOGE personnel having access to PII." *Am. Fed'n of State, Cnty. & Mun. Emps., AFL-CIO v. SSA*, 2025 WL 1206246, at *31; *see* Doe Decl. ¶ 10; *accord* Declaration of Alan Butler ¶ 11 (ECF No. 7-2) ("Butler Decl."); Declaration of Leonard J. Kennedy ¶ 14 (ECF No. 7-3) ("Kennedy Decl."); Declaration of David Brody ¶¶ 14, 15 (ECF No. 7-4) ("Brody Decl."). That is eminently reasonable: the ongoing Treasury and OPM breaches put Plaintiffs' private information at severe and continuous risk of further disclosure, violate their constitutional right against disclosure of personal matters, and harm their privacy interests. FAC ¶¶ 67, 100, 139, 141, 145.

C. Intrusion upon seclusion does not require publication or secondary disclosure.

Defendants resist analogizing Plaintiffs' injuries to intrusion upon seclusion on two other grounds, neither credible. First, Defendants suggest disclosure of personal information in violation of federal law can only work a concrete harm if the recipient of that information is "outside the government." MTD at 8. This is incorrect. "Intrusion upon seclusion 'does not depend upon any publicity given to the person whose interest is invaded or to his affairs.'" *AFSCME*, 2025 WL 1141737, at *38 (quoting Restatement § 652B, cmt. a); *Martin v. Mooney*, 448 F. Supp. 3d 72, 82 (D.N.H. 2020) (intrusion upon seclusion "does not require publicity."). To hold otherwise would upend Congress's decision to prohibit (and make actionable) wrongful intra-governmental disclosures of personal information, including through the Privacy Act and section 6103 of the Internal Revenue Code. Finally, Defendants—relying on *O'Leary v. TrustedID, Inc.*, 60 F.4th 240 (4th Cir. 2023)—imply that "unwanted intrusion into the home" or other physical space is necessary for intrusion upon seclusion. MTD at 9 (quoting *O'Leary*, 60 F.4th at 246). Yet the Fourth Circuit just rejected this narrow reading in *Bessent*: "intrusion upon seclusion can occur

beyond the confines of the home. And the government overreaches when arguing for such a limited understanding of the tort." *Bessent*, 2025 WL 1023638, at *5.

D. Congress has made clear that improper access to information is Article III injury.

Congressional judgment and intent also support Plaintiffs' Article III standing by analogy to intrusion upon seclusion. Because it is "well positioned to identify intangible harms that meet minimum Article III requirements," Congress has the authority to "elevat[e] to the status of legally cognizable injuries concrete, *de facto* injuries that were previously inadequate in law," *Spokeo, Inc. v. Robins*, 578 U.S. 330, 341 (2016) (quoting *Lujan*, 504 U.S. at 578). And "[b]y enacting the Privacy Act, the Social Security Act, FISMA, and the Internal Revenue Code, Congress recognized, in general, that improper access to or disclosure of personally identifiable information—even to government employees—poses a harm to legitimate privacy interests." *AFSCME*, 2025 WL 1141737, at *41.

The legislative history of the Privacy Act shows that the Act was intended to extend to government systems of records the same privacy protections that had long existed at common law. As Congress understood, "[t]he privacy of an individual is directly affected by the collection, maintenance, use, and dissemination of personal information by federal agencies[.]" Privacy Act of 1974, Pub. L. No. 93-579, § 2(a)(1), 88 Stat. 1896 (Dec. 31, 1974). "[T]o provide certain safeguards for an individual against an invasion of personal privacy," Congress found it necessary "to regulate the collection, maintenance, use, and dissemination of information by such agencies." *Id.* §§ 2(a)(1), (5)(B). The 93rd Congress viewed these safeguards as an extension of the common law—or in the words of Rep. Robert Drinan, "another important step in protecting the 'sacred precincts of private and domestic life.'" S. Comm. on Gov't Operations & H. Comm. on Gov't Operations, 94th Cong., 2d Sess., *Legislative History of the Privacy Act of 1974*, at 776 (Comm.

Print. 1976) (statement of Rep. Robert Drinan) (quoting Warren & Brandeis, 4 Harv. L. Rev. at 195); *see also id.* at 776 (statement of Sen. Charles Percy) ("[W]e have computers, the type of devices Brandeis probably never even conceived of. I hope that we are prepared to take that next step by passing legislation to safeguard privacy."); *id.* at 803 (statement of Sen. Barry Goldwater) ("By privacy, . . . I mean the right 'to be let alone'—from intrusions by Big Brother in all his guises. . . . We must act now while there is still privacy to cherish."). Congress's judgment to extend common law protections to government-held personal records reinforces the close analogy between intrusion upon seclusion and Plaintiffs' harms.

E. <u>Breach of confidence provides an independent basis for standing.</u>

Finally, Plaintiffs' claims are also closely analogous to the common law tort of breach of confidence, which establishes their Article III standing on independent grounds. *See AFL-CIO v. DOL*, 2025 WL 1129227, at *9. As Judge Bates recently explained in *AFL-CIO v. DOL*:

> [Breach of confidence] "lies where a person offers private information to a third party in confidence and the third party reveals that information to another." Nothing beyond the "plaintiff's trust in the breaching party [being] violated" must occur for the harm to be actionable. The trusted party's disclosure to a third party is sufficient.

Id. at *9 (internal citations omitted) (quoting *Jeffries v. Volume Servs. Am.*, 928 F.3d 1059, 1064–65 (D.C. Cir. 2019)). Here, as in *AFL-CIO v. DOL*, Plaintiffs provided much of the personal information at the heart of this case to OPM and Treasury on the assurance and reasonable assumption that it would be protected pursuant to the Privacy Act, FISMA, 6103 of the Internal Revenue Code, and the Taxpayer Bill of Rights. Plaintiffs allege that such protections were breached when the OPM and Treasury Defendants made "unconsented, unprivileged disclosure[s] to a third party"—namely, DOGE personnel. *Jeffries*, 928 F.3d at 1065 (quoting *Kamal v. J. Crew Grp.*, 918 F.3d 102, 114 (3d Cir. 2019)).

Plaintiffs' asserted harms thus bear a sufficiently close relationship to those recognized at common law to support Article III standing. Indeed, "[t]his common-law analogue is more like a common-law twin." *AFL-CIO v. DOL*, 2025 WL 1129227, at *9.

II. Plaintiffs have pled a cognizable APA claim.

Plaintiffs challenge Defendant agencies' adoption of new access policies giving DOGE unfettered access to agency systems. Adoption of those policies was final agency action subject to APA review, and must be set aside as contrary to law, arbitrary and capricious, and promulgated without notice and comment.

A. Defendants' DOGE Access Policies are final agency action.

Defendants have "abandoned [the] safeguards" of law and agency policies, "relinquishing control of" sensitive systems and "disclosing vast stores of personal information to individuals unauthorized by law to access them." FAC ¶ 64. Defendants' rapid, wholesale shift in handling sensitive data is a consequential new policy susceptible to judicial review under the APA.

The Administrative Procedure Act provides for judicial review for a "final agency action for which there is no adequate remedy in a court." 5 U.S.C. § 704. An agency action is final if it (1) "mark[s] the consummation of the agency's decisionmaking process" and (2) is an action "by which rights or obligations have been determined, or from which legal consequences will flow." *Bennett v. Spear*, 520 U.S. 154, 177–78 (1997). But courts take a "'pragmatic' approach . . . to finality." *U.S. Army Corps of Eng'rs v. Hawkes Co.*, 578 U.S. 590, 599 (2016) (quoting *Abbott Labs. v. Gardner,* 387 U.S. 136, 149 (1967)). Plaintiffs have pled final agency action here.

Defendants do not contest the first *Bennett* prong, nor could they—the decision to rewrite data access policies to accommodate DOGE is final, not tentative or interlocutory. *See* MTD at 22 (arguing only that Defendants' policy changes created no "rights, obligations, or legal consequences for Plaintiffs"). And Defendants' actions resulted in the kind of "'direct and

appreciable legal consequences'" required under the second *Bennett* prong's "'pragmatic' inquiry" *Sierra Club v. EPA*, 955 F.3d 56, 63 (D.C. Cir. 2020) (quoting *Hawkes Co.*, 578 U.S. at 598–99).

As soon as Defendants changed access standards, Plaintiffs' rights and obligations changed with respect to their sensitive data. Regulations permitting information disclosure "certainly affect individual . . . confidentiality rights of those who submit [that] information." *Chrysler Corp. v. Brown*, 441 U.S. 281, 303 (1979). Defendants' actions also changed the *agencies'* position as to requirements for those seeking access to PII in Defendants' data systems, altering their "own rights or obligations," which is independently sufficient to constitute final action. *Doe v. Tenenbaum*, 127 F. Supp. 3d 426, 461 (D. Md. 2012) (relevant inquiry under *Bennett* is whether agency action "determined its own rights or obligations" *or* "determine[d] Plaintiffs' rights or obligations"). And the changes determined DOGE's rights to access the agencies' information.

The *AFSCME* district court concluded that another agency's similar DOGE access policy changes constitute "a sea change that falls within the ambit of a final agency action." 2025 WL 1141737, at *52. The same conclusion should follow here. *See also* Order on Prelim. Inj. at 88, *AFL-CIO v. OPM,* No. 1:25-cv-01237 (June 9, 2025), ECF No. 121 ("PI Order, *AFL-CIO v. OPM*") ("The decision to give access to DOGE agents was the 'consummation' of OPM's decision-making process; it was neither tentative nor interlocutory . . . The decisions here were not discrete decisions as to individual employees."); *AFL-CIO v. DOL*, 2025 WL 1129227 at *12–13 (at motion to dismiss, claims that "agency defendants' across the board policies . . . to grant USDS personnel access to sensitive record systems" allege final agency action); *Venetian Casino Resort, LLC v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008) ("Adopting a policy of permitting employees to disclose confidential information without notice is surely" final agency action).

B. Defendants' violations of the Privacy Act may be challenged under the APA.

Contrary to Defendants' arguments, the Court may act to halt the ongoing unlawful disclosures now. People harmed by these systematic unlawful disclosures need not wait to be alerted to a data breach and then be confined to only limited relief.

Courts "begin with the strong presumption that Congress intends judicial review of administrative action." *Bowen v. Mich. Academy of Fam. Physicians*, 476 U.S. 667, 670 (1986); *see DHS v. Regents of the Univ. of Calif.*, 591 U.S. 1, 16–17 (2020). Thus, courts may review agency action under the APA unless other laws provide an "adequate remedy in court." 5 U.S.C. § 704. The APA "requires federal courts to set aside federal agency action that is 'not in accordance with law'—which means, of course, *any* law." *FCC v. NextWave Pers. Commc'ns, Inc.*, 537 U.S. 293, 300 (2003) (quoting 5 U.S.C. § 706(2)(A)) (emphasis in original).

While the Privacy Act provides some remedies by its own terms—injunctive relief to force the release or modification of records, and monetary damages for unlawful disclosures, 5 U.S.C. §§ 552a(g)(3)–(4)—these are not an adequate substitute for (nor do they displace) judicial review under the APA in certain circumstances. For instance, where, as here, unlawful disclosures are ongoing, and where the government will not act to stop them, only injunctive relief can remedy the situation—monetary damages cannot stop the unlawful conduct. That is especially true when the government's position that it is acting lawfully frustrates Plaintiffs' ability to access the Privacy Act's enumerated remedies. *Cf. Sackett v. EPA*, 566 U.S. 120, 127 (2012) (APA review available when plaintiff "cannot initiate" a statutory remedy and must await further injury). And the government will not provide notice to Plaintiffs or others that their information has been breached, frustrating their ability even to *initiate* claims under the Privacy Act's statutory remedies.

Contemporaneous implementing guidance and subsequent caselaw confirm the availability of APA review. The Office of Management and Budget's ("OMB") 1975 guidelines for Privacy

Act implementation, 5 U.S.C. § 552a(v)(1), explained that "an individual may have grounds for action under other provisions of the law in addition to those provided" by the Privacy Act, including by "seek[ing] judicial review under other provisions of the Administrative Procedure Act." 40 Fed. Reg. 28,948, 28,968 (July 9, 1975) ("OMB Guidelines").

The Supreme Court has expressly contemplated the likelihood that the APA's provisions for equitable relief may explain the omission of standards for it in the Privacy Act. *See Doe v. Chao*, 540 U.S. 614, 619 n.1 (2004) (Privacy Act's silence on equitable relief in some circumstances may "be explained by the general provisions for equitable relief within the" APA). Similarly, the D.C. Circuit has expressly concluded that APA review is available for claims like these. In *Doe v. Stephens*, 851 F.2d 1457, 1463 (D.C. Cir. 1988), the court found that the Privacy Act did not "authorize the injunctive relief sought by" the Plaintiff, but the APA *did* because the agency had violated the Veterans' Records Statute, as amended by the Privacy Act, by disclosing the Plaintiffs' records. *Id.* at 1463, 1466. *See also Radack v. DOJ*, 402 F. Supp. 2d 99, 104 (D.D.C. 2005) (the Privacy Act does not provide an adequate remedy for plaintiffs who seek declaratory and injunctive relief; the APA is the source for equitable relief to such plaintiffs). More recently, multiple courts, including one in this Circuit, have determined that the APA may provide injunctive relief to plaintiffs harmed specifically by DOGE's data access in violation of the Privacy Act. *See*, *e.g.*, *AFL-CIO v. DOL*, 2025 WL 1129227, at *13–18; *AFSCME*, 2025 WL 1141737, at *52–53; *AFL-CIO v. OPM*, 2025 WL 996542, at *18–19.

C. Defendants' grant of system access to DOGE is contrary to law.

Courts must set aside agency action that violates the law. 5 U.S.C. § 706(2)(A). Defendants claim no exception to Section 706—their only defense is that they have not violated any law. But Plaintiffs have adequately pled that Defendants' changes to their access policies violate FISMA, the Privacy Act, Internal Revenue Code, the Fifth Amendment, and separation of powers. *See* Parts

III, IV, V, VI, and VII, *infra*; FAC ¶¶ 127–41, 160–71. A similar contrary to law claim based on the Privacy Act and concerning the same data breach has already withstood another motion to dismiss. *See AFL-CIO v. OPM*, 2025 WL 996542, at *16. Each of these violations is sufficient to demonstrate that Defendants' actions were contrary to law and should be set aside under the APA.

D. Defendants' system access policies are arbitrary and capricious.

Courts must set aside "arbitrary and capricious" agency action. 5 U.S.C. § 706(2)(A). An agency "must examine the relevant data and articulate a satisfactory explanation for its action including a 'rational connection between the facts found and the choice made.'" *Motor Vehicle Mfrs. Ass'n of U.S. v. State Farm Mut. Auto. Ins. Co.*, 463 U.S. 29, 43 (1983) (quoting *Burlington Truck Lines v. U.S.*, 371 U.S. 156, 168 (1962)). "An agency may not . . . depart from a prior policy *sub silentio* or simply disregard rules that are still on the books," and must "show that there are good reasons for the new policy." *FCC v. Fox Television Stations, Inc.*, 556 U.S. 502, 515 (2009). An agency need not "demonstrate . . . that the reasons for the new policy are better than the reasons for the old one" or "provide a more detailed justification than what would suffice for a new policy," but must at least "display awareness that it *is* changing position." *Id.*

Defendants provide no substantive response to the argument that their new system access policies were "hasty, ill-considered, unsupported, and destructive to the interests that government privacy laws are intended to advance," bearing all the hallmarks of arbitrary and capricious action. FAC ¶ 152. They simply assert that agencies' implementation of an executive order should be insulated from APA review, effectively conceding the merits of Plaintiffs' arbitrary and capricious claim. *See* MTD at 25. But an executive order cannot release an agency from its APA obligations; Defendants cite no case to support this extreme argument. Indeed, "courts regularly apply APA review to agency actions taken in direct response to a presidential directive, such as an Executive Order." *Int'l Refugee Assistance Project v. Trump*, 373 F. Supp. 3d 650, 662 (D. Md. 2019), *rev'd*

on other grounds 961 F.3d 635 (4th Cir. 2020); *see also Chamber of Com. of the U.S. v. Reich*, 74 F.3d 1322, 1327 (D.C. Cir. 1996) (an agency's action to implement a Presidential order is not "insulate[d] . . . from judicial review under the APA, even if the validity of the Order were thereby drawn into question."); *E. Bay Sanctuary Covenant v. Trump*, 932 F.3d 742, 770–71 (9th Cir. 2018) (a court "may consider the validity of the agency's proposed action" under the APA even though the action incorporates a Presidential order by reference); *AFL-CIO v. DOL*, 2025 WL 1129227, at *5 n. 4 (finding that there is "no basis" for the government's position that APA review is not available concerning an agency's implementation of the EO.). If the Court concludes that APA review is available in this matter, there is no question that Plaintiffs should prevail on their arbitrary and capricious claim, given Defendants' concession of its merits.

E. Defendants were required to undertake notice and comment rulemaking.

Neither Treasury nor OPM engaged in notice-and-comment rulemaking prior to granting DOGE sweeping access to their protected information. Their failure to do so violated the APA.

Confidential information held by both Treasury and OPM is subject to agency-specific regulations promulgated pursuant to notice-and-comment rulemaking. *See* 31 C.F.R. §§ 1.8, *et seq.* (Treasury regulations); 5 C.F.R. §§ 297.101, *et seq*. (OPM regulations). The new DOGE access policies—which are final agency actions—represent substantial changes to these regulations: as currently written, neither OPM nor Treasury regulations, *see* 5 C.F.R. § 297.401; 31 C.F.R. § 1.9, authorize or even contemplate these categorical disclosures. The "Administrative Procedure Act requires agencies to afford notice of a proposed rulemaking and an opportunity to comment prior to . . . the promulgation, *amendment, modification*, or repeal" of a rule. *Liquid Energy Pipeline Ass'n. v. Fed. Energy Regul. Comm'n*, 109 F.4th 543, 547 (D.C. Cir. 2024) (citations omitted) (emphasis added). Defendants do not dispute that OPM and Treasury can only lawfully amend their policies (or adopt new disclosure policies which conflict with previously promulgated ones)

through notice and comment. Instead, they characterize the new DOGE access policies as workaday matters of agency operation and imply that they therefore are not subject to notice-and-comment. But Plaintiffs allege that they are new access policies, and, at this stage, the Court must treat that allegation as true. Defendants' argument runs contrary to the APA, established law, and Defendants' prior promulgation of the access policies through notice-and-comment.

III. Plaintiffs have pled cognizable Privacy Act violations.

Under the Privacy Act, agency Defendants may not "disclose" records except in certain circumstances, none of which exist here. 5 U.S.C. § 552a(b). Faced by this clear violation, Defendants argue that their sweeping grant of access to DOGE personnel is not a "disclosure" within the meaning of the Privacy Act, that any disclosure which may exist is covered by the Privacy Act's "need to know" exception, and that the disclosure is permitted under a routine use of agency Defendants' systems of records. These arguments are unavailing.

A. Defendants have made a massive disclosure of records under the Privacy Act.

Defendants have "disclosed" records within the meaning of the Privacy Act. "[D]isclosure may be either the transfer of a record or the granting of access to" it. OMB Guidelines, 40 Fed. Reg. at 28,953.[3] Plaintiffs allege, and Defendants have not meaningfully disputed, that Defendant agencies have granted DOGE affiliates sweeping access to systems of records.

[3] Defendants argue Plaintiffs have not adequately alleged DOGE Affiliates' access to PII at OPM. *See* MTD at 13–14 n.4 (arguing that as of March 6, certain DOGE Affiliates had not yet *logged in* to certain systems). This argument misses the mark. DOGE Affiliates have been granted *access*—the "right, opportunity, or ability to enter"— OPM systems, even if they have not yet logged in. *Access*, Black's Law Dictionary (12th ed.). This case challenges OPM's "adopt[ion of] a *policy* of granting" DOGE "access to any system to which they request access." FAC ¶ 107 (emphasis added). Defendants' argument about the sufficiency of Plaintiffs' allegations about DOGE's actual *use* of particular systems does not bear on Plaintiffs' allegations about existence of an access *policy*. In a recent decision granting a preliminary injunction against DOGE access to OPM systems, a court rejected the arguments Defendants make here, concluding that (1) the actual access by DOGE staff that had occurred was sufficient to violate the Privacy Act; (2) the March 6

Providing ongoing access to records or modifying policies to allow that access far exceeds conduct held to constitute Privacy Act disclosures. For instance, "plac[ing] records . . . on a server accessible by other federal employees and members of the public" constitutes disclosure under the Privacy Act. *Tolbert-Smith v. Chu*, 714 F. Supp. 2d 37, 43 (D.D.C. 2010). And another court in this Circuit has already concluded that "OPM[] and Treasury disclosed records with the plaintiffs' PII to DOGE affiliates," *Am. Fed. of Tchrs. v. Bessent*, 2025 WL 895326, at *28, by granting and continuing the ongoing access at issue here.[4] That is true whether or not the unauthorized individual "actually reviewed, much less used those records"—"providing access" is enough. *AFL-CIO v. OPM*, 2025 WL 996542, at *12. Even Defendants acknowledge that Plaintiffs have alleged exactly that: "USDS employees have . . . been granted access to large databases that contain [Plaintiffs'] information somewhere." MTD at 12.[5]

B. <u>Disclosure to DOGE is not permitted by the need-to-know exception.</u>

Defendants' Privacy Act theory primarily relies on the "need to know" exception, 5 U.S.C. § 552a(b)(1), which would allow either Defendant agency to disclose records to "employees of the agency . . . who have a need for the record in the performance of their duties." But DOGE affiliates do not need the unprecedented and sweeping access that Defendant agencies have granted them, nor are they properly considered employees of the agency.

---

audit of DOGE access was not reliable; (3) DOGE staff had directed OPM career staff to extract data for their use; and (4) it was the *ability* to access the data, rather than the actual use or review of the data, that constituted a "disclosure" and an intrusion upon seclusion. *See* PI Order, *AFL-CIO v. OPM* at 61–64, 74. This court should similarly reject Defendants' arguments on this score; at best, they suggest the need for more developed factfinding at a later stage of this case.

[4] The Fourth Circuit recently stayed the District of Maryland's preliminary injunction in *Bessent*, but did not call into question or otherwise address the district court's conclusion on disclosure.

[5] If this Court concludes that it is dispositive whether Defendants viewed Plaintiffs' records *specifically*, limited discovery on that question would be appropriate.

First, Defendants have not meaningfully suggested that DOGE affiliates have a need to access Defendant agencies' systems of records. Their only purported basis for such a need relies entirely on Executive Order 14,158, which instructs agency heads "to ensure USDS has full and prompt access to all unclassified records," EO § 4(b), in order to "maximize governmental efficiency and productivity," *id.* § 1. This sparse language does not demonstrate a particularized need for access to each system, much less unfettered access. Even if the EO were more specific, an executive order cannot, by itself, "license the defendants to violate the Privacy Act." *Parks v. IRS*, 618 F.2d 677, 681 (10th Cir. 1980). To avail themselves of the "need to know" exception, Appellants must show that *each* disclosure was supported by a need: each time a DOGE affiliate was given access to PII, he "must have examined the record in connection with the performance of duties assigned to him and [must have] had to do so in order to perform those duties properly." *Bigelow v. DOD*, 217 F.3d 875, 877 (D.C. Cir. 2000). Defendants have never identified such a need, and their effort to do so in their Motion to Dismiss is unpersuasive.

Even assuming the EO's instruction to "improve agency data systems," MTD at 13, *could* constitute a need to know for Privacy Act purposes (which it cannot), it does not articulate a need for anyone to access PII specifically. Defendants may be correct that modernizing data systems would require access to those systems' structure, *see id.*, but they have not even attempted to explain why it would require access to the PII contained in the records *within* those systems rather than relying on anonymized data to improve structure or functions.

Defendants' reliance on the Executive Order frustrates the purposes of the Privacy Act, which 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." S. Rep. No. 1183, 93d Cong.,

2d Sess. (1974). If a highly general Executive Order can be read to provide an adequate "need" for access to records, the President could simply unilaterally evade the protections of the Privacy Act.

Second, DOGE affiliates are not employees of Defendant agencies for purposes of the Privacy Act. This independently closes off the "need to know" exception, which only allows *intra-agency* disclosures. To determine which agency, "as a practical matter," *Jud. Watch, Inc. v. Dep't of Energy*, 412 F.3d 125, 132 (D.C. Cir. 2005) employs a federal employee, it is appropriate to consider "all the circumstances," *id.* at 131 (quoting *Spirides v. Reinhardt*, 613 F.2d 826, 831 (D.C. Cir. 1979)), including matters on which he works and who supervises him. *Id.* at 131–32.

As Plaintiffs allege, DOGE affiliates are functionally supervised by DOGE. Defendants' own characterization of the DOGE affiliates' work relies entirely on the EO and its instructions to DOGE teams. MTD at 12–14. But the EO requires DOGE affiliates to "coordinate their work with" DOGE while requiring only that the affiliates "advise" Defendants Bessent and Ezell. EO § 3(c). To "coordinate" with DOGE means that DOGE affiliates working at Defendant agencies must "harmonize" their work with DOGE. *Coordinate*, Webster's Third New International Dictionary at 501 (1971). DOGE Teams cannot plausibly both be independently supervised by each agency *and* harmonized in their work across the government. Coordination therefore must mean that DOGE affiliates must "harmonize" with DOGE's instructions and expectations. In contrast, DOGE affiliates need only "advise" agency heads, which requires neither agency head supervision, nor any form of alignment. In practice, to comply with the EO, DOGE affiliates must report not to Defendants Ezell and Bessent, but to DOGE.[6] *See also* PI Order, *AFL-CIO v. OPM*

[6] Further, the EO instructs that USDS—not individual DOGE affiliates—be granted system access at agencies. EO § 4(b). If DOGE affiliates are in fact employees of Defendant agencies, the instruction to grant access to *USDS* cannot serve as the basis to grant them access. By Defendants' own characterization of the EO as the basis for DOGE affiliates' purported "need" for access, the affiliates *must* be part of DOGE, and the exception for intra-agency disclosures cannot apply.

at 76 (finding that multiple DOGE affiliates at OPM likely took direction from DOGE and should not be functionally considered OPM employees). At a minimum, limited discovery would be appropriate to evaluate the degree and nature of DOGE's control of agency DOGE teams.

C. Defendants' disclosures are not permissible as a routine use.

As a last-ditch effort, Defendants argue that DOGE affiliates' access to Treasury systems is permitted as a "routine use" under the Privacy Act. Defendants are wrong.

The routine use on which Defendants rely applies to only three BFS systems: Payment Records, Debt Collection Operations System, and Do Not Pay Payment Verification Records. 85 Fed. Reg. 11,776 at 11,779, 11,793, 11,803 (Feb. 27, 2020). But Plaintiffs allege Privacy Act violations arising from access to other systems, FAC ¶¶ 67, 69. At most, a routine use may authorize access to the system to which it applies; it cannot authorize access to *other* systems.[7]

Nor do these routine uses justify the breadth of access Defendants have granted to DOGE—even where they apply. "[I]dentifying, preventing, or recouping improper payments," 85 Fed Reg. at 11,779, may require access to *some* PII, such as to confirm a given recipient received or sought improper payments, or to identify recipients of improper payments and actively recover funds. But it strains credulity that these purposes require unbridled access to extensive PII about tens of millions of Americans before identifying particularized indicia of impropriety. To allow the routine use exception to empower government officials to conduct sweeping fishing expeditions through the PII of hundreds of millions of Americans would grant Defendants "virtually unlimited power to rewrite the [Privacy] Act." *See Biden v. Nebraska*, 600 U.S. 477, 502 (2023).

[7] The routine use on which Defendants rely for DOGE access at OPM allows only "contractors, grantees, or volunteers" to access OPM information. 77 Fed. Reg. 73,694, 73,697 (Dec. 11, 2012). It cannot be read to provide unfettered access to federal *employees* to all OPM information systems.

D. Injunctive relief is available under the Privacy Act for Plaintiffs' claims.

APA Injunctive relief is available to halt an agency disclosure policy which violates the Privacy Act. *See* Section II.B, *supra*. Alternatively, the Privacy Act permits review of claims that the government has "fail[ed] to comply" with certain provisions, including the relevant § 552(b) provisions in a way which has "an adverse effect on an individual." 5 U.S.C. § 552a(g)(1)(D). When Congress vests jurisdiction in courts, "inherent equitable powers . . . are available for [its] proper and complete exercise," and cannot "be denied or limited in the absence of a clear and valid legislative command." *Porter v. Warner Holding Co.*, 328 U.S. 395, 398 (1946). Courts have understood the Privacy Act to permit equitable relief beyond § 552a(g)(1) and § (g)(2). *See Haase v. Sessions*, 893 F.2d 370, 374 n.6 (D.C. Cir. 1990) ("It is not at all clear . . . Congress intended to preclude broad equitable relief (injunctions) to prevent" violations of 552a(e)(7)"); *Smith v. Nixon*, 807 F.2d 197, 204 (D.C. Cir. 1986) (courts may order equitable relief for § 552a(e)(7) violations). If such relief is not appropriate here, the Privacy Act cannot provide Plaintiffs an "adequate remedy in a court," 5 U.S.C. § 704, and APA relief must be available.

IV. Plaintiffs have adequately pled a violation of the Internal Revenue Code.

The Internal Revenue Code provides that "[r]eturns and return information shall be confidential" and that "no officer or employee of the United States . . . shall disclose any return or return information," where "'disclosure' means the making known to any person in any manner whatever." 26 U.S.C. § 6103(a). That prohibition has only limited exceptions, "guarantee[ing] . . . personal information in a return will be guarded from persons not directly engaged in processing or inspecting the return for tax administration purposes." *Gardner v. United States*, 213 F.3d 735, 738 (D.C. Cir. 2000) (quotation omitted). When an individual taxpayer's data is disclosed in violation of that prohibition, she may sue for relief. 26 U.S.C. § 6103. Such a claim "must specifically allege who made the alleged disclosures, to whom they were made, the nature of the

disclosures, the circumstances surrounding them, and the dates on which they were made." *Bancroft Global Dev. v. United States*, 330 F. Supp. 3d 82, 101 (D.D.C. 2018) (quotation omitted).

Plaintiff Doe 1's allegations make this claim plausible. On January 27, Defendant Bessent granted unauthorized DOGE personnel, including Marko Elez, access to BFS databases containing Doe's confidential tax information. FAC ¶¶ 79–88, 132–137. Defendants say that is no disclosure at all unless "Treasury has wrongfully inspected or disclosed *her* tax return or return information." MTD at 17. But disclosing a database containing her information *is* disclosing her information—and Doe has alleged the details of the disclosure more than adequately "to put the government on notice of which exact actions" she is challenging. *Bancroft*, 330 F. Supp. 3d at 101.

Defendants also argue this disclosure falls under an exception for Treasury "officers and employees." 26 U.S.C. § 6103(h); MTD at 17. This is incorrect. Marko Elez was not a Treasury employee—he was a DOGE employee, FAC ¶¶ 58, 60, and other DOGE affiliates at Treasury should also be considered DOGE employees. *See supra*, Section III.B. And Defendants have shown neither that DOGE affiliates satisfy the exception's requirement that their "official duties require such inspection or disclosure for tax administration purposes," 26 U.S.C. § 6103(h), nor that they could not perform such duties with access solely to the system structure and not to PII.

V. Plaintiffs have adequately pled a violation of their constitutional right to privacy.

Under the Fifth Amendment, Plaintiffs have "the right to shield information from disclosure." *Dobbs v. Jackson Women's Health Org.*, 597 U.S. 215, 273 (2022).[8] And in the Fourth Circuit, "the constitutional right to privacy extends to . . . individual interest in avoiding disclosure of personal matters." *Walls v. City of Petersburg*, 895 F.2d 188, 192 (4th Cir. 1990) (quoting

[8] There are "two very different meanings of the [right to personal privacy]: the right to shield information from disclosure and the right to make and implement important personal decisions without governmental interference." *Dobbs*, 597 U.S. at 273. This case only involves the former.

Whalen v. Roe, 429 U.S. 589, 599–600 (1997)). In determining whether an individual's right to informational privacy has been violated, courts in this Circuit consider: (1) whether a person has a "reasonable expectation of privacy" in the relevant information and (2) whether there is "a compelling governmental interest in disclosure [that] outweighs the individual's privacy interest." *Payne v. Taslimi*, 998 F.3d 648, 655–56 (4th Cir. 2021). Both factors weigh against dismissal.

The government has repeatedly promised to protect the information of federal employees and individual American taxpayers. *See, e.g.*, 26 U.S.C. § 6103; 5 U.S.C. § 552a. When individuals provide their personal information to the government, they expect the government to abide by those obligations, protecting and keeping that information confidential. That expectation is particularly strong with regard to financial information. *See Walls*, 895 F.2d at 194 (recognizing Constitutional privacy right regarding "outstanding debts and judgments"). Defendants have no compelling interest that would justify DOGE's unauthorized access to Plaintiffs' information, nor have Defendants attempted to assert any. *See* MTD at 18–20. Defendants have not even established that their interest in disclosure is "legitimate," *see NASA v. Nelson*, 562 U.S. 134, 143 (2011).

Faced by their violation of Plaintiffs' constitutional rights, Defendants: (1) question the validity of a right expressly recognized by the Fourth Circuit; (2) contend that the mere existence of the Privacy Act immunizes their disclosure from constitutional infirmity; and (3) assert that the disclosure at issue here does not sufficiently "shock the conscience." None of these is persuasive.

First, the Fourth Circuit has made clear the existence of a right to informational privacy applicable to sensitive financial information;[9] *Walls*, 895 F.2d at 194 ("[f]inancial information . . . is protected by a right to privacy."). In *Walls*, the court identified a reasonable expectation of

[9] The Supreme Court has not held otherwise. Defendants' characterization of the Supreme Court's "nonchalance," MTD at 18, does not call the Fourth Circuit's holdings into question.

privacy in financial information, though ultimately held that a municipal government's interest as an employer against corruption among its employees was adequately compelling to permit its collection. *Id.* Noting that the city would keep the information "in a private filing cabinet that is locked at night, and only four persons would be authorized to have access," *id.*, the Fourth Circuit cautioned that its "conclusions might have been different" if the information "had been more widely distributed"—for instance, stored in a "database" along with "vast amounts of information about individuals in sophisticated computer files." *Id.*

The Fourth Circuit "follow[ed] *Walls*" in *Payne*, 998 F.3d at 657, even while holding "a prisoner's reasonable expectations of privacy are limited," and that therefore, "an inmate in a prison medical center . . . lacked a reasonable expectation of privacy in his HIV status." *Id.* at 658. But Plaintiffs are not inmates. Rather, like the *Walls* plaintiff, they have a reasonable expectation of privacy in their confidential financial information. And unlike the city in *Walls*, Defendants have offered no justification for DOGE's access and are in fact storing Plaintiffs' data precisely as the *Walls* court feared—in a massive database to which multiple people now have unlawful access.

Second, Defendants' argument that their legal duty to avoid disclosures should allay Plaintiffs' concerns, MTD at 19–20, hurts Defendants more than it helps. True, both the Privacy Act and Internal Revenue code apply here. And true, they evince a desire to "give 'forceful recognition' to" the "interest in maintaining the 'confidentiality of sensitive information.'" *Nelson*, 562 U.S. at 156 (quoting *Detroit Edison Co. v. NLRB*, 440 U.S. 301, 318 n.16 (1979)). But this is not a case, like *Nelson*, where the existence of these safeguards—and the government's presumptive compliance with them—can allay concerns about "the Government's *collection* of information." *Id*. As discussed above, in Parts III and IV, Plaintiffs allege Defendants are *actively violating* the Privacy Act and the Internal Revenue Code. Defendants' invocation of privacy laws

they are violating cannot warrant dismissing Plaintiffs' claims, especially when Defendants claim that those alleged violations cannot be reviewed by a court. If anything, the existence of these statutes only underscores Plaintiffs' reasonable expectation of privacy in their information.

Finally, Plaintiffs need not allege that Defendants' actions shock the conscience. "[T]here are 'two strands of the substantive due process doctrine.'" *D.B. v. Cardall*, 826 F.3d 721, 740 (4th Cir. 2016) (quoting *Seegmiller v. LaVerkin City*, 528 F.3d 762, 767 (10th Cir. 2008)). One "protects an individual's fundamental liberty interests, while the other protects against the exercise of government power that shocks the conscience." *Seegmiller*, 528 F.3d at 767. The right to privacy falls within the first of these and does not require a "shocks the conscience" test. *See, e.g.*, *Walls*, 895 F.2d at 191–93 (analyzing informational privacy claim without considering whether government's actions shocked the conscience); *Payne*, 998 F.3d at 655–660 (same); *see also Reno v. Flores*, 507 U.S. 292, 302 (1993) (infringing fundamental liberty interest prohibited unless "narrowly tailored to serve a compelling state interest," without "shocks the conscience" test).

Even if infringements on the right to privacy were subject to a "shocks the conscience" test, Plaintiffs' allegations satisfy it. Plaintiffs allege purposeful, unjustified, and unlawful disclosure of millions of individuals' most sensitive personal information to an unknown number of unauthorized DOGE affiliates. And this Court should decline Defendants' invitation to mechanistically require intent on the part of the government as a prerequisite to satisfying the "shocks the conscience" test. MTD at 20. "[T]he measure of what is conscience shocking is no calibrated yard stick," *Cnty. of Sacramento v. Lewis*, 523 U.S. 833, 847 (1998), and when "extended opportunities to do better are teamed with protracted failure even to care, indifference" to substantive due process violations "is truly shocking." *Id.* at 853. Defendants faced no split-second decisions. To the contrary, they chose to grant unlawful systems access after deliberation

and despite contrary advice. *See* FAC ¶¶ 72–81, 104–16. Such purposeful disclosure, contrary to express guarantees made by the government, "interferes with rights 'implicit in the concept of ordered liberty,'" *United States v. Salerno*, 481 U.S. 739, 746 (1987) (quoting *Palko v. Connecticut*, 302 U.S. 319, 325–26 (1937), and fails to "comport with traditional ideas of fair play and decency," *Breithaupt v. Abram*, 352 U.S. 432, 435 (1957)—Plaintiffs' constitutional claim does not seek to enforce a constitutional "guarantee [of] due care." *Lewis*, 523 U.S. at 849.

VI. Defendants' violations of FISMA are judicially reviewable.

Under FISMA, the "head of each agency shall be responsible for providing information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of" information or systems maintained by the agency. 44 U.S.C. § 3554(a)(1)(A). By failing even to assess necessary protections with respect to DOGE access, Defendants have failed to meet FISMA's mandate.

Compliance with FISMA is judicially reviewable, despite Defendants' arguments to the contrary. Courts may conduct "barebones review" for compliance with basic obligations even when a statute "smacks of flexibility." *Mach Mining, LLC v. EEOC*, 575 U.S. 480, 492, 494 (2015). Where a statute directs an official to consider certain factors, "narrow" review is available to ensure the official "addressed the terms" of the statute while "allowing the exercise of broad discretion" by not "reach[ing] the correctness of the assessment of the factors considered or of the ultimate decision." *Sluss v. DOJ, Int'l Prisoner Transfer Unit*, 898 F.3d 1242, 1252 (D.C. Cir. 2018). Defendants' decision-making must evince *some* consideration of "risk and magnitude of the harm resulting from" the DOGE access policies. 44 U.S.C. § 3554(a)(1)(A). Plaintiffs allege it does not; instead, DOGE directed Treasury and OPM to "flagrantly violate" the "safeguards" of FISMA and other laws to grant sweeping access to "high risk information system[s]." FAC ¶¶ 64, 72, 101, 104. These facts are entirely distinct from cases declining substantive FISMA review, like

Cobell v. Kempthorne, where the court was asked to study a robust years-long record of agency IT decisions and changes to make its own judgments about FISMA compliance. *See* 455 F.3d 301, 307–11 (D.C. Cir. 2006). The facts here suggest *no* meaningful attempt by Defendants to consider or comply with FISMA requirements, a failure that is susceptible to narrow judicial review.

VII. DOGE's unauthorized access to is *ultra vires* and violates separation of powers.

Finally, Plaintiffs sufficiently allege *ultra vires* and separation of powers claims against the agency DOGE Teams and those Defendants who control or direct their work.[10]

An *ultra vires* claim is a non-statutory claim for judicial review of lawless government actions. All "officers of the government from the highest to the lowest, are creatures of the law, and are bound to obey it." *Butz v. Economou*, 438 U.S. 478, 506 (1978). "Government action is *ultra vires* if the agency or other government entity 'is not doing the business which the sovereign has empowered him to do or he is doing it in a way which the sovereign has forbidden.'" *Ancient Coin Collectors Guild v. Customs & Border Prot.*, 698 F.3d 171, 179 (4th Cir. 2012) (quoting *Larson v. Domestic & Foreign Com. Corp.*, 337 U.S. 682, 689 (1949)); *see also Fed. Express Corp. v. Dep't of Com.*, 39 F.4th 756, 764 (D.C. Cir. 2022) (action is *ultra vires* when "plainly beyond the bounds" of lawful authority). Unlawful action which goes further and seizes another branch of government's lawful authority violates separation of powers. *See Seila Law LLC v. CFPB*, 591 U.S. 197, 227 (2020); *Trump v. United States*, 603 U.S. 593, 637–38 (2024).

[10] Plaintiffs allege USDSTO (FAC ¶ 51), USDS (which houses USDSTO), OPM and its director (FAC ¶¶ 52–54), GSA and its administrator (*id.*), Musk (FAC ¶ 56), and Davis (FAC ¶ 57) direct, control, and/or house DOGE or its components. Defendants do not dispute that those who direct DOGE are liable if it violates separation of powers or acts *ultra vires*. Instead, Defendants suggest in passing that Plaintiffs have not stated a claim against GSA and its administrator. MTD at 30. But their argument boils down to an implication that GSA "may not" control DOGE. *Id*. Plaintiffs have alleged, to the contrary, that DOGE is partly housed at GSA, and that GSA formally employs some DOGE affiliates, including DOGE's day-to-day leader, FAC ¶¶ 46, 52–54, 57. Those allegations, which must be accepted as true at this stage, sufficiently state claims against GSA.

Plaintiffs allege that DOGE acted without authority and infringed on Congressional authority by "directing and controlling the use and administration" of OPM's and Treasury's systems and unlawfully accessing "personal data of tens of millions of people." FAC ¶ 161; *id.* ¶¶ 160–71. Defendants respond only that Plaintiffs' claims duplicate "their Privacy Act, IRC, Fifth Amendment, and APA claims," MTD at 28. Not so. Plaintiffs' APA, Privacy Act, IRC, and Fifth Amendment claims concern Treasury and OPM Defendants' *disclosure*s of Plaintiffs' information. *See* FAC ¶¶ 127–59. Plaintiffs' *ultra vires* and separation of powers claims run against DOGE and those who direct it,[11] and contend that DOGE has no lawful authority to *access* Plaintiffs' sensitive information or to *direct* Treasury or OPM to permit such access. *See* FAC ¶¶ 160–71.

The core of an *ultra vires* claim is whether government action is within the bounds of an official's or entity's lawful authority. *See Ancient Coin Collectors Guild*, 698 F.3d at 179. Plaintiffs are not aware of, nor do Defendants invoke, *any* statute that conceivably authorizes DOGE to exercise the authority that it has in this case. Just as in *AFL-CIO v. DOL* and *AFL-CIO v. OPM*, where DOGE failed to point to a plausible source of authority for its actions, its motion to dismiss must fail. *See AFL-CIO v. DOL*, 2025 WL 1129227, at *22 ("motion to dismiss points to no legal source that grants USDS the authority to take these actions" so "'the Court will permit' the ultra vires claim 'to proceed.'") (quoting *Ctr. for Biological Diversity v. Trump*, 453 F. Supp. 3d 11, 48 (D.D.C. 2020)); *AFL-CIO v. OPM*, 2025 WL 996542, at *20 (denying motion to dismiss claims that the "disclosure of the OPM records of tens of millions of Americans to unvetted and untrained individuals who had no legal right to access those records . . . was directed and controlled by the DOGE Defendants" who "have no statutory authority with respect to OPM records").

[11] Plaintiffs bring both sets of claims against OPM; the first concerns OPM's conduct in granting DOGE access to systems, while the second concerns OPM's role overseeing and housing DOGE.

Because Defendants acted outside of the agency structure established by Congress to undertake agency functions, they violated separation of powers. Power to establish agencies and determine their "functions and jurisdiction" rests with Congress. *Myers v. United States*, 272 U.S. 52, 129 (1926). Congress designed Treasury and OPM to perform certain work and keep sensitive personal data safe while doing it. "Except where such authority is expressly given by [the Internal Revenue Code] to any person other than an officer or employee of the Treasury Department, the Secretary shall prescribe all needful rules and regulations," 26 U.S.C. § 7805(a); nothing in Title 26 grants DOGE authority to set or alter Treasury access policy. Congress similarly provided that the Director of OPM alone be responsible for all OPM systems and regulations. 5 U.S.C. § 1103. Again, Congress has not authorized DOGE to set or alter OPM's access policies.

Defendants invoke the EO as the lone authority for DOGE's actions. *See* MTD at 25. But an executive order cannot grant statutory or constitutional authority. "Fundamentally, '[a]dministrative agencies are creatures of statute,' and 'possess only the authority that Congress has provided.'" *PFLAG, Inc. v. Trump*, No. 8:25-cv-00337, 2025 WL 685124, at *16 (D. Md. Mar. 4, 2025) (quoting *Nat'l Fed'n of Indep. Bus. v. OSHA*, 595 U.S. 109, 117, 142 (2022)). An agency "literally has no power to act . . . unless and until Congress confers power upon it,'" *New York v. Trump*, 764 F. Supp. 3d 46, 50 (D.R.I. 2025) (*citing La. Pub. Serv. Comm'n v. FCC*, 476 U.S. 355, 374 (1986)), and "[a]ny action that an agency takes outside the bounds of its statutory authority is ultra vires." *City of Providence v. Barr*, 954 F.3d 23, 31 (1st Cir. 2020) (*citing City of Arlington v. FCC*, 569 U.S. 290, 297 (2013)). Plaintiffs' allegations that DOGE has acted without authority conferred by Congress meets these standards, making their *ultra vires* claim plausible.

CONCLUSION

The Court should deny Defendants' motion to dismiss.

Dated: June 17, 2025

Respectfully submitted,

/s/ Matthew B. Kaplan

Matthew B. Kaplan, VSB # 51027
THE KAPLAN LAW FIRM
1100 N. Glebe Rd., Suite 1010
Arlington, VA 22201
Telephone: (703) 665-9529
mbkaplan@thekaplanlawfirm.com

Mark B. Samburg*
Orlando Economos*
Aman T. George*
Robin F. Thurston*
Skye Perryman**
DEMOCRACY FORWARD FOUNDATION
P.O. Box 34553
Washington, D.C. 20043
Telephone: (202) 448-9090
Fax: (202) 796-4426
msamburg@democracyforward.org
oeconomos@democracyforward.org
ageorge@democracyforward.org
rthurston@democracyforward.org
sperryman@democracyforward.org

Alan Butler*
EPIC Executive Director
John L. Davisson*
EPIC Director of Litigation
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave, N.W.
Washington, D.C. 20036
(202) 483-1140 (telephone)
(202) 483-1248 (fax)

* *admitted* pro hac vice
**pro hac vice *application forthcoming*

Counsel for Plaintiffs