UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

Alliance for Retired Americans, et al., Plaintiffs, v. Scott Bessent, in his official capacity as Secretary of the Treasury, et al., Defendants.	Civil Action No. 25-313 (CKK)

REPLY IN SUPPORT OF PLAINTIFFS' MOTION FOR A PRELIMINARY INJUNCTION

Norman L. Eisen
(DC Bar No. 435051)
State Democracy Defenders Fund
600 Pennsylvania Avenue SE
#15180
Washington, DC 20003

Nandan M. Joshi
(DC Bar No. 456750)
Nicolas Sansone
(DC Bar No. 1686810)
Allison M. Zieve
(DC Bar No. 424786)
Public Citizen Litigation Group
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

February 18, 2025

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

REGULATIONS

OTHER

INTRODUCTION

The Bureau of the Fiscal Service (the Bureau) at the Department of the Treasury (Treasury Department) holds sensitive personal information of retirees, federal workers, taxpayers, and millions of other individuals for one purpose: to ensure the seamless transfer of payments to and from federal agencies. None of these individuals has a choice. If they want to receive social security checks, receive their federal pay, or pay outstanding taxes or receive a tax refund, for example, their information is contained in the Bureau's database. Two statutes, though—the Privacy Act, 5 U.S.C. § 552a, and the Internal Revenue Code (IRC), 26 U.S.C. § 6103—assured all of us that sensitive personal information contained in the Bureau's records will not be disclosed without our consent, except as specifically authorized by law.

On its first day, the new administration began the process of upending those assurances through an executive order establishing the so-called "Department of Government Efficiency" (DOGE) to "advanc[e] the President's 18-month DOGE agenda." Exec. Order No. 14158, 90 Fed. Reg. 8441 (Jan. 29, 2025). Although the executive order did not define the "DOGE agenda," it directed agency heads "to ensure [the U.S. DOGE Service (USDS)] has full and prompt access to all unclassified agency records, software systems, and IT systems." *Id.* § 4(b). DOGE's reported actions have since made clear that the "DOGE agenda" involves accessing and sharing sensitive data stored on agency servers throughout the federal government.[1]

[1] *See, e.g.*, Jacob Bogage, *Musk's DOGE seeks access to personal taxpayer data, raising alarm at IRS*, Wash. Post, Feb. 16, 2025; Jennifer Bendery, *Elon Musk's*

At the Treasury Department, Thomas H. Krause and Marko Elez were installed to carry out DOGE work before Secretary Scott Bessent was confirmed by the Senate. Although initially denied access to the Bureau's systems, they obtained full access after Secretary Bessent took office. Defendants have submitted declarations from Mr. Krause and three others (although not from Secretary Bessent) that purport to explain what occurred behind the scenes. Critically, none deny that the DOGE team has been given access to any personal data they wish.

Plaintiffs are likely to succeed on the merits of their claim that Defendants' decision to open up the Bureau's records to DOGE is unlawful and arbitrary, and there is no jurisdictional or procedural barrier to this Court's ability to reach the merits. Defendants' decision compromises the personal information of Plaintiffs' members by depriving them of the statutory right to withhold their consent to disclosure. And once sensitive personal data is compromised, returning to the status quo ante will be difficult, if not impossible. Indeed, Mr. Elez improperly received "write" access to the Bureau's systems for only one day, and, one week later, Defendants still do not know the effect on information security. In these circumstances, a preliminary injunction is critically needed to prevent irreparable harm to Plaintiffs' members while this litigation proceeds.

DOGE Posts Classified Data On Its New Website, HuffPost, Feb. 14, 2025; David Ingram, *DOGE software approval alarms Labor Department employees*, NBC News, Feb. 13, 2025 (discussing data transfer software); Jason Leopold & Evan Weinberger, *DOGE-Backed Halt at CFPB Comes Amid Musk's Plans for 'X' Digital Wallet*, Bloomberg, Feb. 10, 2025 (discussing access to "sensitive bank examination and enforcement records"); Hannah Natanson, et al., *Elon Musk's DOGE is feeding sensitive federal data into AI to target cuts*, Wash. Post, Feb. 6, 2025.

ARGUMENT

I. Defendants have granted DOGE unprecedented access to personal information in the Bureau's records.

Plaintiffs brought this action after reports surfaced that Secretary Bessent had removed the career official in charge of the Bureau for refusing to allow DOGE to access the Bureau's systems. With the official gone, Secretary Bessent reportedly granted DOGE full access to the Bureau's files. *See* Compl. ¶¶ 34–37. Secretary Bessent has not submitted a declaration explaining his actions. But other declarations submitted by Defendants, as well as other reports, reveal that DOGE's access to personal information is expansive and unprecedented.

Mr. Krause and Mr. Elez began their DOGE work at the Treasury Department on January 23 and January 21, respectively, several days before Secretary Bessent was sworn in. Krause Decl. ¶¶ 1, 3. Mr. Krause's "role at Treasury … was created to help effectuate the mission of the President's [DOGE]," *id.* ¶ 2, "[a]n important aspect" of which was "to quickly place [Mr. Krause] into the Treasury Department," *id.* ¶ 11.

By January 26, Mr. Krause had developed a "4-6 week payment process engagement plan" whose "objective" was "to gain insight into the full, end-to-end payment process across multiple BFS payment systems." *Id.* ¶ 13. According to Mr. Krause, "this work required … the ability to review sensitive payment data." *Id.* ¶ 15. According to Mr. Krause, "[t]he Treasury Secretary, through his Chief of Staff, approved the engagement," Krause Decl. ¶ 15—presumably after Secretary Bessent was sworn in on January 28.

Defendants have not disclosed the details of the "engagement plan." In a February 4 letter to members of Congress, the Treasury Department represented that Mr. Krause was conducting an "operational efficiency assessment" of the Bureau's systems and that he was given "the kind of access that Treasury provides to individuals reviewing Treasury systems, such as auditors."[2] When providing access to auditors, however, the Bureau has "significantly limited" the "availability of production data." Gioeli Decl. ¶ 13. The declaration of the Bureau's Deputy Commissioner for Transformation and Modernization reveals that DOGE's access has been far "broader in scope than what has occurred in the past," including "multiple systems and data records." *Id.*

Because the "broad access" given to DOGE "presented risks," "[Bureau] and Treasury Departmental Office employees developed mitigation strategies." Gioeli Decl. ¶ 11. Mr. Elez was granted "read-only access" to the Bureau's systems, *id.* ¶¶ 13–14, while Mr. Krause could view "payment systems or source code while they were being accessed by another person"—what Mr. Gioeli called "over the shoulder" access, *id.* ¶ 4.

On January 28, Mr. Elez's original agency-furnished laptop, which could not access Bureau systems, was replaced with a Bureau laptop that could, and "several cybersecurity tools" were used "to monitor Mr. Elez's usage." *Id.* ¶ 12. But Defendants have not stated that any limits were placed on Mr. Elez's ability to "view and query"

[2] Treasury Department Letter to Members of Congress Regarding Payment Systems (Feb. 4, 2025) (Treasury Feb. 4 Letter), available at https://home.treasury.gov/news/press-releases/sb0009.

sensitive personal information, *id.* ¶ 17; or to copy sensitive information, including by taking "screenshots of payment systems data or records," *id.* ¶ 4.

On February 3, Treasury Department officials reportedly received a "confidential assessment that U.S. DOGE Service access to a sensitive payment network represented an 'unprecedented insider threat risk'" and that, notwithstanding the "read only" limitation, such access "should be 'immediately' suspended."[3] That same day, "Mr. Elez was provided read-only access to the Payment Automation Manager (PAM) Database, [and] Payment Automation Manager (PAM) File System," and given a "walk-through" demonstration of those systems. Gioeli Decl. ¶¶ 17–18. On February 4 and 5, Mr. Elez accessed the PAM database and the Secure Payment System (SPS) database. *Id.* ¶ 18–19.

In addition to these "walk-through" demonstrations, the DOGE team was actively engaged in reconfiguring the Bureau's processes to identify foreign assistance payments that the administration did not want made. One such effort began on January 26, Robinson Decl. ¶ 8, and the other on January 31, *id.* ¶ 10; Krause Decl. ¶¶ 17–20. On February 3, Mr. Elez also "copied two USAID files directly from the PAM database to his [Bureau] laptop" for reasons that are not explained. Gioeli Decl. ¶ 18.

---

[3] Joseph Menn et al., *Treasury was warned DOGE access to payments marked an 'insider threat'*, Wash. Post, Feb. 7, 2025; *see also* Vittoria Elliott & Leah Feiger, *A US Treasury Threat Intelligence Analysis Designates DOGE Staff as 'Insider Threat'*, Wired, Feb. 7, 2025 ("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.").

According to Mr. Gioeli, on February 6, "it was discovered" that Mr. Elez's database access to SPS had "mistakenly" been set to "read/write permissions instead of read-only." *Id.* ¶ 20. A forensic analysis of Mr. Elez's activities "is still ongoing," but "preliminary reviews" have "found no indication" that he "used his [Bureau] laptop to share payment systems data outside of the U.S. Government." *Id.* ¶ 21. Mr. Gioeli does not state whether personal information has been shared outside of the Treasury Department.

Mr. Elez resigned on February 6,[4] and his credentials and equipment have been returned to the agency. Defendants do not state whether he has provided an "attestation statement" that "any copies of Treasury information made would be properly destroyed" and that "no suspicious or unauthorized access to Bureau information or data had occurred during the engagement," as required by the Bureau's risk-mitigation measures. Gioeli Decl. ¶ 14.

On February 14, counsel for Defendants advised the U.S. District Court for the Southern District of New York that the "forensic analysis thus far" shows that "there were emails sent outside Treasury," but Defendants did not yet "know [the] content."[5]

Defendants' own evidence thus confirms that the DOGE team has been given essentially unbounded access to the personal data on the Bureau's systems, and that

[4] Gioeli Decl. ¶ 22; Katherine Long, *DOGE Staffer Resigns over Racist Posts*, Wall St. J., Feb. 6, 2025.

[5] Victoria Benkiempis, *US Judge Extends Order to Block DOGE From Treasury Department Data*, Wired, Feb. 14, 2025.

measures implemented to "mitigate" the associated risks of that unprecedented access failed to keep the Bureau's data secure for even one week.

II. This Court has the authority to protect people's personal information pending a decision on the merits.

A. Plaintiffs have standing.

To pursue a case in federal court, a plaintiff must have experienced a "concrete" harm, which can either be tangible or intangible. *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021). In determining whether a harm is concrete, "[c]ourts must afford due respect to Congress's decision to impose a statutory prohibition or obligation on a defendant" and "should assess whether the alleged injury to the plaintiff has a 'close relationship' to a harm 'traditionally' recognized as providing a basis for a lawsuit in American courts." *Id.* at 424–25 (quoting *Spokeo v. Robins*, 578 U.S. 330, 340–41 (2016). Here, both considerations support Plaintiffs' standing.

1. Starting with tradition, the tort of intrusion upon seclusion consists of "an intentional interference with [one's] interest in solitude or seclusion, either as to [one's] person or as to [one's] private affairs or concerns, of a kind that would be highly offensive to a reasonable [person]." Restatement (Second) of Torts § 652B, cmt. a (1977). As the Supreme Court has recognized, the privacy harm that arises from an "intrusion upon seclusion" is among the historically recognized intangible injuries that are sufficiently "concrete" to satisfy Article III. *TransUnion*, 594 U.S. at 425.

Numerous cases hold that an intrusion upon seclusion, or an analogous injury, can occur when private information is shared with unauthorized individuals. *See, e.g.*, *In re Nickelodeon Consumer Privacy Litig.*, 827 F.3d 262, 274 (3d Cir. 2016) (browsing

and video-viewing history); *Patel v. Facebook, Inc.*, 932 F.3d 1264, 1273 (9th Cir. 2019) (biometric information); *Feldman v. Star Trib. Media Co.*, 659 F. Supp. 3d 1006, 1015 (D. Minn. 2023) (video-viewing history); *Hall v. Harleysville Ins. Co.*, 896 F. Supp. 478, 484 (E.D. Pa. 1995) (credit reports); *McKenzie v. Allconnect, Inc.*, 369 F. Supp. 3d 810, 819 (E.D. Ky. 2019) (employee information); *see also Pileggi v. Washington Newspaper Publ'g Co.*, No. 23-cv-345, 2024 WL 324121, at *5 & n.2 (D.D.C. Jan. 29, 2024), *appeal docketed*, No. 24-7022 (D.C. Cir. Feb. 22, 2024) (collecting cases). And applying *TransUnion*, courts regularly hold that a plaintiff has experienced an Article III injury when such an intrusion has occurred. *See, e.g.*, *Feldman*, 659 F. Supp. 3d at 1015; *Pileggi*, 2024 WL 324121, at *5 & n.2. Especially as concerns about data privacy have grown, some courts have recognized that individuals "have a property interest in their personal information." *Calhoun v. Google LLC*, 526 F. Supp. 3d 605, 635 (N.D. Cal. 2021) (collecting cases).

Defendants' conduct here constitutes an intrusion upon seclusion or, at a minimum, a closely analogous harm. *See TransUnion*, 594 U.S. at 433 (noting that an "exact duplicate" of a traditional harm is not required for standing); *See, e.g., Persinger v. Sw. Credit Sys., L.P.*, 20 F.4th 1184, 1192 (7th Cir. 2021) (holding that "whether [plaintiff] would prevail in a lawsuit for common law invasion of privacy is irrelevant," so long as "the harm alleged in her complaint resembles the harm associated with intrusion upon seclusion"). Defendants' actions permitted private information to be disseminated to individuals even if Plaintiffs' members have not consented to the disclosure. The information at issue is personal and sensitive—

including the names, Social Security numbers, birth dates, home addresses, phone numbers, email addresses, and bank account details of Plaintiffs' members. That the information was stored in the Bureau's systems, rather than on the personal devices of Plaintiffs' members, does not lessen the privacy interests at stake when that information is improperly accessed.

According to Defendants, Plaintiffs are injured in a concrete way only in the event of a "public disclosure." Opp. 11. But the common-law tort of intrusion upon seclusion "does not depend upon any publicity given to the person whose interest is invaded or to his affairs," but rather concerns "his interest in solitude or seclusion … as to his private affairs or concerns." Restatement (Second) of Torts § 652B, cmt. a; *see Feldman*, 659 F. Supp. 3d at 1015 ("[U]nder the common law tradition associated with invasion-of-privacy and intrusion-upon-seclusion claims, 'publication' of a private matter is not an essential element."). In contrast, the cases that Defendants cite invoke common-law torts that *do* include publication as an element. *See TransUnion*, 594 U.S. at 434 n.6 (defamation); *Hunstein v. Preferred Collection & Mgmt. Servs*, 48 F.4th 1236, 1245–50 (11th Cir. 2022) (public disclosure); *Farst v. AutoZone, Inc.*, 700 F. Supp. 3d 222, 231–32 (M.D. Pa. 2023) (same); *Barclift v. Keystone Credit Servs., LLC*, 585 F. Supp. 3d 748, 758–59 (E.D. Pa. 2022) (same). Intrusion on seclusion, however, is a distinct tort with distinct elements, and it is a concrete harm that is independently sufficient to establish standing. *See TransUnion*, 594 U.S. at 425 (listing "reputational harms, disclosure of private information, and intrusion upon seclusion" as discrete categories of concrete harm); *cf. Gadelhak v.*

AT&T Servs., Inc., 950 F.3d 458, 462 (7th Cir. 2020) (Barrett, J.) (finding standing based solely on injuries analogous to an intrusion upon seclusion).

In any event, the Privacy Act and IRC reflect that "an exchange internal to the federal government," Opp. 12, is a "public disclosure." The Privacy Act and the IRC apply to the nonconsensual disclosure of information *within* the government, as well as outside the government. The congressional judgment" reflected in these laws is "instructive and important," given Congress's unique advantage in "identify[ing] intangible harms" that warrant judicial redress. *Spokeo, Inc.*, 578 U.S. at 341. And the exposure of "personally identifiable information … to an unauthorized third party" is "sufficiently concrete" for standing, even if the third party were an otherwise "legitimate" operation. *Salazar v. Nat'l Basketball Ass'n*, 118 F.4th 533, 542–43 (2d Cir. 2024).

2. Beyond the basic harm caused by Defendants' decision to relax or remove the guardrails that Congress established to protect personal information, Defendants' actions create a nonspeculative risk of dissemination of private information to additional unauthorized parties. "A person exposed to a risk of future harm may pursue forward-looking, injunctive relief to prevent the harm from occurring, at least so long as the risk of harm is sufficiently imminent and substantial." *TransUnion*, 594 U.S. at 435.

Defendants claim that the risk of unauthorized disclosure is "speculative" in light of "extensive security measures Treasury has employed." Opp. 13. But those security measures did not prevent Mr. Elez from obtaining "write" access to the

Bureau's SPS system or prevent emails potentially containing personal information from being sent out of the Treasury Department. *See supra* p.6 Indeed, the Treasury Department's internal threat watchdog warned officials about the risk, *see supra* n.3, and the measures that have been taken depend on compliance by the DOGE team. *See* Gioeli Decl. ¶¶ 11, 14; *see also* Br. of Former Treasury Dep't Officials, ECF 20-1, at 19 ("Read-only access would still threaten individuals' privacy, compromise national security, and provide information that could support a broad and inappropriate use of the improper payments law to initiate illegal impoundment.").

Moreover, Plaintiffs' members have attested to experiencing the additional concrete injury of emotional distress as a result of Defendants' actions. *See, e.g.*, Rosenblatt Decl. ¶ 10 (attesting to being "disturbed, anxious, and frustrated" due to the exposure of personal data); McElhaney Decl. ¶ 10 (same); Casey Decl. ¶ 10 (same). Defendants are incorrect that such distress is insufficient to constitute concrete harm. Opp. 13 n.3. In *Doe v. Chao*, 540 U.S. 614 (2004), the Supreme Court addressed a Privacy Act claim brought by an individual whose sole claim of injury rested on his testimony that he was concerned and worried by the disclosure of his Social Security number. *See id.* at 617–18. The Court held that this "adverse consequence" was insufficient to allow him to recover a statutory damages award because the court interpreted the relevant statutory provision to permit recovery only upon a showing of "actual damages." *Id.* at 620. Critically, though, the Court expressly recognized the plaintiff's emotional distress was sufficient to avoid "dismissal for want of standing" and was "injury enough to open the courthouse door." *Id.* at 624–25; *see Mulhern v.*

Gates, 525 F. Supp. 2d 174, 184 n.13 (D.D.C. 2007) (holding that allegations that a disclosure caused an individual to "experience emotional distress" were "sufficient to establish an 'adverse effect' of the sort required to confer standing").

Defendants rely on *In re Science Applications International Corp. (SAIC) Backup Tape Data Theft Litigation*, 45 F. Supp. 3d 14 (D.D.C. 2014), for the proposition that emotional distress is "not sufficient to constitute a concrete harm." Opp. 13 n.3. In that case, though, "it was highly unlikely" that an unauthorized third party "understood what the [exposed records] were, let alone had the wherewithal to access them." 45 F. Supp. 3d at 29. In other words, the distress occasioned by the exposure in that case was not "objectively reasonable." Opp. 13 n.3. Here, it is clear that DOGE knows what it is doing with the personal information it has been collecting from the Bureau (and other federal databases). *See supra* n.1. Under such circumstances, the distress voiced by Plaintiffs' members is reasonable, genuine, and sufficiently concrete to establish this Court's jurisdiction over their challenge to Defendants' practices.

3. Plaintiffs' members have attested that they "trusted the government to maintain the privacy of [that] information and to only use [it] for lawful purposes." *See, e.g.*, Rosenblatt Decl. ¶ 10. And despite Defendants' claim that this trust was based on nothing more than "subjective expectations," Opp. 13, *Congress* created and guaranteed those expectations in the Privacy Act by "requiring federal agencies, except as otherwise provided by law, to … permit an individual to prevent records pertaining to him obtained by such agencies for a particular purpose from being used

or made available for another purpose without his consent." Pub. L. No. 93-579, § 2(b), 88 Stat. 1896, 1896 (1974); *cf. Eichenberger v. ESPN, Inc.*, 876 F.3d 979, 983 (9th Cir. 2017) (describing another statute in which Congress protected individuals' right to "retain control over their personal information"). Contrary to Defendants' suggestion, Opp. 13, it is eminently "reasonable" for Plaintiffs' members to expect the government to comply with laws enacted to protect individual privacy. Opp. 13.

B. Plaintiffs' APA claims challenge final agency action.

The APA authorizes judicial review of "final agency action." 5 U.S.C. § 704. Courts have held that an agency's decision to disclose information to others is final agency action subject to judicial review. *Chrysler Corp. v. Brown*, 441 U.S. 281, 318–19 (1979) (holding that a "decision to disclose [reports under the Freedom of Information Act] is reviewable agency action" under the APA); *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 final agency action). "Agency action generally need not be committed to writing to be final and judicially reviewable." *Bhd. of Locomotive Eng'rs & Trainmen v. Fed. R.R. Admin.*, 972 F.3d 83, 100 (D.C. Cir. 2020). Agency action is final when it "mark[s] the 'consummation' of the agency's decisionmaking process," that is, it is not "of a merely tentative or interlocutory nature," and the action is one "by which 'rights or obligations have been determined,' or from which 'legal consequences will flow.'" *Bennett v. Spear*, 520 U.S. 154, 178 (1997) (quoting *Port of Boston Marine Terminal Assn. v. Rederiaktiebolaget Transatlantic*, 400 U.S. 62, 71 (1970)). Courts take a "pragmatic" approach in applying these factors. *U.S. Army Corps of Eng'rs v. Hawkes*

Co., 578 U.S. 590, 599 (2016) (quoting *Abbott Laboratories v. Gardner,* 387 U.S. 136, 149 (1967)).

Here, Defendants correctly do not dispute that the first prong is satisfied: The decision to grant access to DOGE has been made and implemented. *See U.S. Army Corps of Eng'rs v. Hawkes Co.*, 578 U.S. 590, 598 (2016) (holding that the first finality prong is met when the agency "has ruled definitively"). Defendants contend, however, that the action has no legal consequences. Opp. 14. But an agency's decision has legal consequences when it "alter[s] the legal regime to which the agency action is subject." *Bennett*, 520 U.S. at 178. Until Secretary Bessent took office, the Bureau enforced the legal requirements against unauthorized disclosure of personal or tax information without the consent of the individual concerned. *See* 5 U.S.C. § 552a(b); 26 U.S.C. § 6103(c); *see also* 31 C.F.R. § 1.28(b)(vii) (Privacy Act regulations prohibiting dissemination of information outside the Treasury Department). Defendants' new policy grants DOGE access to Bureau records without obtaining the required consent. The legal effect is just as final as if Defendants had decided to post personal information contained in the Bureau's records on its website.

Defendants respond that the challenged action cannot have legal consequences because it arose from the Treasury Department's "day-to-day operations." Opp. 15 (citing *Norton v. S. Utah Wilderness All.*, 542 U.S. 55, 61–62 (2004)). The cited case, however, holds that agency action is subject to judicial review if it is a "discrete" action. 542 U.S. at 64. It does not suggest an agency's "day-to-day" operations cannot give rise to discrete actions that have legal consequences. Moreover, permitting

DOGE to access sensitive data on the Bureau's systems is hardly a "day-to-day" event. DOGE did not even exist one month ago.

Public Citizen v. U.S. Trade Representative, 5 F.3d 549 (D.C. Cir. 1993), on which Defendants rely (Opp. 15), does not require a different result. There, the challenged agency action was not final because the ultimate decision rested with the President. *Id.* at 300. Here, Defendants made the decision, and no additional actions stand in the way of DOGE obtaining access to the Bureau's records. Indeed, Defendants have already provided access.

C. Damages actions under the Privacy Act and the IRC do not provide an adequate remedy for Plaintiffs' injuries.

Defendants maintain that Plaintiffs are unlikely to establish their entitlement to injunctive relief under the APA because the Privacy Act and the IRC provide adequate remedies for Defendants' disclosure of the personal and financial information of Plaintiffs' members. Opp. 15–20. The "exception" to the APA's "general authorization for review of agency action" that applies when adequate relief is available through other avenues, however, "should not be construed to defeat the central purpose providing a broad spectrum of review of agency action." *Bowen v. Massachusetts*, 487 U.S. 879, 903 (1988). Here, the remedies available under the Privacy Act and IRC are inadequate substitutes for the injunctive relief that Plaintiffs seek under the APA.

To determine "whether an alternative remedy is 'adequate' and therefore preclusive of APA review, [courts] look for 'clear and convincing evidence' of 'legislative intent' to create a special, alternative remedy and thereby bar APA

review." *Citizens for Responsibility & Ethics in Washington v. U.S. Dep't of Justice*, 846 F.3d 1235, 1244 (D.C. Cir. 2017) (*CREW*) (quoting *Garcia v. Vilsack*, 563 F.3d 519, 523 (D.C. Cir. 2009)). While "[a]n alternative that provides for *de novo* district-court review of the challenged agency action offers … evidence of Congress' will" to displace an APA remedy, *id.* at 1245, the potency of this evidence is fatally diminished where there is a significant "gap between the *relief* [the alternative] provides and the relief … [sought] under the APA," *id.* at 1246 (emphasis added). For example, the availability of "a naked money judgment against the United States" under an alternative statutory scheme is not necessarily "an adequate substitute for prospective relief" under the APA where a plaintiff seeks "entry of declaratory or injunctive relief that requires the [government] to modify future practices." *Bowen*, 487 U.S. at 905; *cf. Garcia*, 563 F.3d at 525 (holding that an alternative remedial scheme was adequate where a successful plaintiff could "obtain declaratory and injunctive relief against [an] agency itself, in addition to money damages, and such remedies would presumably deter [the agency] to the same extent as a successful APA claim").

Here, the primary relief that Plaintiffs seek under the APA is an injunction barring Defendants from giving unauthorized individuals access to private personal and financial information and requiring Defendants to ensure that no further unlawful disclosure occurs. *See* Compl. ¶ 18. Neither the Privacy Act nor the IRC provides comparable relief. *Cf. Bowen*, 487 U.S. at 903 (noting that Congress withheld

APA remedies when an adequate alternative remedy already existed so as not to "duplicate existing procedures for review of agency action").

The Privacy Act authorizes individuals to seek monetary relief under certain circumstances and provides for injunctive relief directing an agency to amend the individual's records or to produce those records to the individual. 5 U.S.C. §§ 552a(g)(2)–(4). These forms of relief are entirely distinct from the relief that Plaintiffs seek in this case. As the Supreme Court has recognized, money damages against the government are not an adequate substitute for "the general equitable powers of a district court" to craft injunctive relief that preemptively averts the harmful effects of unlawful official conduct before they come to pass. *Bowen*, 487 U.S. at 905. And as for the injunctive relief available under the Act, the difference between an injunction to have one's records corrected or produced on request and an injunction to prevent one's records from being unlawfully disseminated to unauthorized and unaccountable third parties is not merely "some mismatch." *CREW*, 846 F.3d at 1246. The two genres of injunction are entirely different in kind. *Cf. id.* (holding that equitable relief under the Freedom of Information Act was an adequate substitute for an APA remedy because it would permit the plaintiff to "gain access to all the records" sought despite not requiring the agency to make the records available for public inspection).

Defendants do not explain why Privacy Act remedies resemble the remedies sought here or why they would "deter [Defendants]" from granting unauthorized third-party access to confidential records "to the same extent [that] a successful APA

claim" would. *Garcia*, 563 F.3d at 525. Instead, they rely on three district court decisions that, they say, stand for the blanket proposition that "a plaintiff cannot bring an APA claim to obtain relief for a Privacy Act violation." Opp. 18 (quoting *Westcott v. McHugh*, 39 F. Supp. 3d 21, 33 (D.D.C. 2014)). The cases on which Defendants rely, however, rejected APA claims seeking "relief … [that] *is* available under the Privacy Act," such that they could not "rely on the APA for duplicative relief." *Poss v. Kern*, No. 23-cv-2199, 2024 WL 4286088, at *6 (D.D.C. Sept. 25, 2024) (emphasis added). In two cases, a plaintiff sought the removal or amendment of their own governmental records, *see id.* (seeking "removal and deletion of [an] allegedly defamatory report" from official files); *Westcott*, 39 F. Supp. 3d at 23 (seeking "removal or revision" of a memorandum "contained in [plaintiff's] official military records"), where such removal or revision is available under the Privacy Act, 5 U.S.C. § 552a(g)(2)(A) (expressly providing for amendment); *Abdelfattah v. DHS*, 787 F.3d 524, 534 (D.C. Cir. 2015) (recognizing "expungement of agency records" as a Privacy Act remedy). The third case, meanwhile, did not discuss remedy at all, holding only that the plaintiff could not "duplicate" her Privacy Act claims by bringing identical APA claims. *Tripp v. Dep't of Def.*, 193 F. Supp. 2d 229, 238 (D.D.C. 2002).

Although Defendants also rely extensively on *Cell Associates, Inc. v. NIH*, 579 F.2d 1155 (9th Cir. 1978), *cited at* Opp. 17–18, that case supports Plaintiffs' position. *Cell Associates* involved a claim brought directly under the Privacy Act—not the APA—seeking to "enjoin the government from releasing" certain records. 579 F.2d at 1156. In rejecting the claim, the court held that "the Act makes no provision for [such

relief] as part of the remedies that it … provide[s]." *Id.* at 1160. Critically, though, the APA *does* authorize a court to use its "general equitable powers" to enjoin unlawful agency action. *Bowen*, 487 U.S. at 905. In explaining that such relief is unavailable under the Privacy Act, *Cell Associates* underscores that the Act's remedial provisions supply no alternate adequate remedy for unlawful disclosures of the sort that Plaintiffs challenge.

As for the IRC, Defendants acknowledge that "[c]ivil damages … are the sole remedy" available under the statute for a violation of section 6103, and that the relevant remedial provision "does not authorize injunctive relief." Opp. 19. The lone case that Defendants cite for the proposition that damages under the IRC are an adequate substitute for injunctive relief under the APA is a 1988 case from the District of Arizona that did not so much as mention the APA, let alone address an APA claim. *See Agbanc Ltd. v. Berry*, 678 F. Supp. 804, 806–08 (D. Ariz. 1988). The case also predates the Supreme Court's recognition in *Bowen* that the availability of an alternative damages remedy does *not* preclude an APA claim for injunctive relief. *See* 487 U.S. at 905. The prospect of retrospective compensation for the irreparable injury that Defendants' ongoing unlawful practices inflict on Plaintiffs' members' privacy rights is not an adequate substitute for an equitable judicial order that puts an end to the preventable continuation of those injuries here and now.

Finally, Defendants offer a variation on their argument regarding the remedial schemes of the Privacy Act and the IRC. Rather than offering "adequate remed[ies]" that foreclose APA relief pursuant to 5 U.S.C. § 704, Defendants argue, those statutes

also "expressly or impliedly forbid[]" Plaintiffs' desired relief and so foreclose relief under 5 U.S.C. § 702. Defendants, however, cite no authority for that proposition, and the Supreme Court has held that the Privacy Act does not foreclose relief under other statutes. *See Dep't of Agric. Rural Dev. Rural Housing Serv. v. Kirtz*, 601 U.S. 42, 63 (2024). The one case that Defendants cite, *Match-E-Be-Nash-She-Wish Band of Pottawatomi Indians v. Patchak*, 567 U.S. 209 (2012), *cited at* Opp. 19–20, is wholly inapposite. That case involved the Quiet Title Act, 28 U.S.C. § 2409a(a), which authorizes the federal government "to be named as a party" in certain lawsuits but states that the authorization "does not apply" under certain conditions. The Supreme Court observed that a party could not evade that statutory exception by bringing an APA claim against the government that would otherwise fall within the exception to the Quiet Title Act's waiver of sovereign immunity. *Match-E-Be-Nash-She-Wish Band*, 567 U.S. at 216. That observation has no application here. Unlike the Quiet Title Act, neither the Privacy Act nor the IRC contains language evincing a congressional desire to preserve the government's sovereign immunity with respect to particular claims or under particular circumstances. Accordingly, neither statute forbids this Court from granting the relief that Plaintiffs seek under the APA.

III. Plaintiffs are entitled to a preliminary injunction.

A. Plaintiffs are likely to succeed on the merits of their claims.

The Privacy Act and the IRC do not give federal agencies *carte blanche* to do as they please with the personal information contained in their records. The Privacy Act requires agencies to adopt "safeguards to insure the security and confidentiality of records," 5 U.S.C. § 552a(e)(1), and strictly limits the individuals—both inside and

outside the federal government—to whom those records may be disclosed without the consent of the individual affected, *id.* § 552a(b). The IRC imposes even stricter controls on tax return and return information and expressly limits the Treasury Department's use of such information for tax administration purposes. *See* 26 U.S.C. § 6103(a), (h)(1). Secretary Bessent's decision to grant the "DOGE team" unfettered access to the Bureau's records notwithstanding these statutory protections is unlawful and unreasonable.

The Privacy Act. Defendants seek to defend the decision to grant Mr. Krause (and potentially future DOGE team members) full access to personal information in the Bureau's records on the ground that he is an officer or employee of the Treasury Department who has "a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1); *see* Opp. 20. That argument is flawed.

First, even assuming that Mr. Krause "has been a Treasury employee since January 23" by virtue of his consultancy contract under 5 U.S.C. § 3109, *see* Wenzler Decl. ¶¶ 3, 5; *see also* Krause Decl. ¶ 1, he appears to be wearing two hats. Mr. Krause is also a special government employee (SGE), *see* 18 U.S.C. § 202, and the declarations submitted by Defendants do *not* aver that Mr. Krause is an SGE of the Treasury Department. *See* Wenzler Decl. ¶ 4 ("Thomas is designated as a Special Government Employee (SGE) under 18 U.S.C. § 202.); Krause Decl. ¶ 1 ("I am also designated as a Special Government Employee (SGE)."). And there is reason to believe that Mr. Krause may not be an SGE of the Treasury Department. Mr. Krause states that he not only "coordinate[s] with" and "updates" officials at "USDS/DOGE," but also

"receive[s] high-level policy direction from them." Krause Decl. ¶ 4.[6] Moreover, Mr. Krause reportedly "conducted some interviews of employees" at the U.S. DOGE Service immediately before joining the Treasury Department as a consultant.[7] And none of the declarations reveal who at the Treasury Department Mr. Krause was appointed by or whether he remains "subject to the supervision" of that person. 5 U.S.C. § 2501(a) (defining "employee"). To the extent Mr. Krause is simultaneously an employee of another component of the federal government, any disclosure of Bureau records to him necessarily is made to someone other than "employees of the agency which maintains the record." *Id.* § 552a(b)(1).

Second, section 552a(b)(1) is a "need-to-know" exception that asks whether an official "had to" view personal information "in order to perform [his] duties properly." *Bigelow v. Dep't of Def.*, 217 F.3d 875, 876–77 (D.C. Cir. 2000). The Bureau's privacy impact statement for the PAM database, for instance, certifies that personal information will not be shared within the Treasury Department except on a "need to know" basis and will not be "shared with agencies, organizations, or individuals external to Treasury."[8] Neither Defendants nor Mr. Krause explain, however, why

---

[6] Mr. Krause asserts that he is "not an employee of USDS/DOGE," but it is unclear whether "USDS/DOGE" refers to the U.S. DOGE Service, the U.S. DOGE Service Temporary Organization, or both. *See* Krause Decl. ¶¶ 2, 4; Exec. Order No. 14158, § 3.

[7] Theodore Schleifer & Madeleine Ngo, *Elon Musk and His Allies Storm Into Washington and Race to Reshape It*, N.Y. Times, Jan. 29, 2025.

[8] Privacy and Civil Liberties Impact Assessment, Payment Automation Manager §§ 5.3(b), 5.4(a) (July 11, 2019), https://www.fiscal.treasury.gov/files/pia/pampclia.pdf.

Mr. Krause specifically (as opposed to career Bureau employees) needs "full" access to all personal information stored in the Bureau's systems for a legitimate Bureau purpose. *See* Krause Decl. ¶¶ 2, 15; Opp. 20. Instead, DOGE team members are being given capacious and elastic job descriptions, apparently to avoid the need to satisfy the statutory requirement that access to personal data must be based on "need." For example, Mr. Krause's role "is to find ways to use technology to make the Treasury Department more effective, more efficient, and more responsive to the policy goals of this Administration," Krause Decl. ¶ 4; and Mr. Elez's was to conduct "'special and confidential studies on a variety of strategies and issues related to Treasury's information technology,' and identify[], analyz[e], and mak[e] 'recommendations to strengthen Treasury's hardware and software.'" Wenzler Decl. ¶ 10. Defendants' approach is not sufficient to satisfy the requirements of the Privacy Act. *Cf. Doe v. Stephens*, 851 F.2d 1457, 1466 (D.C. Cir. 1988) ("It is by now well-established that agencies covered by the Privacy Act may not utilize the 'routine use' exception to circumvent the mandates of the Privacy Act.").

The IRC. Defendants argue that the DOGE team's work falls under the tax administration exception to confidentiality. 26 U.S.C. § 6103(h)(1). That argument fails as to Mr. Krause to the extent that he wears two hats, because the exception is limited to "officers and employees" of the Treasury Department. Defendants, moreover, never explain why the DOGE team's purported mission to improve the Bureau's technology systems requires access to confidential tax information. Opp. 23. The GAO Report on which they rely (Krause Decl. ¶ 8), discusses actions that the

Internal Revenue Service should take to reduce improper Earned Income Tax Credit payments; it provides no role for the Bureau to play.[9] And to the extent the DOGE team seeks access to tax information to carry out a presidential directive to block payments, *see supra* p. 5, that purpose would be unrelated to "tax administration" because it would not arise from the "execution and application of the internal revenue laws." 26 U.S.C. § 6103(b)(4)(A)(i).

Arbitrary and capricious action. Plaintiffs are likely to succeed on their claim that Defendants' decision to grant DOGE unfettered access to the Bureau's system is arbitrary and capricious. Defendants' primary argument is that this decision cannot be arbitrary if it was lawful under the Privacy Act and the IRC. *See* Opp. 24. But even when "an agency's discretion is unfettered at the outset," an "irrational departure" from a prior "general policy by which its exercise of discretion will be governed" may be "action that must be overturned" as arbitrary. *INS v. Yueh-Shaio Yang*, 519 U.S. 26, 32 (1996). Here, Defendants do not dispute the reports that DOGE was denied full access to the Bureau's systems until Secretary Bessent intervened and removed the career Bureau official who had enforced the agency's prior policy. And Defendants' own declarant confirms that DOGE was provided access to "multiple systems and data records" that "was broader in scope than what has occurred in the past. Gioeli Decl. ¶ 13. Defendants had a duty under the APA to justify this change and take account of the reliance and expectation interests of the millions

[9] GAO, GAO-24-107660, *Payment Integrity: Significant Improvements Are Needed to Address Improper Payments and Fraud* 19, 35 (2024).

of individuals whose private information would be implicated by it. Because they did not do so, their action should be set aside as arbitrary.

B. The remaining factors of irreparable harm, the equities, and the public interest support grant of a preliminary injunction.

Defendants cannot seriously dispute Plaintiffs' showing of irreparable injury. Unlike other situations, Defendants here have not committed to keeping personal information secure within the Bureau; to the contrary, they appear to believe that "an exchange internal to the federal government" is not a public disclosure of private information. Opp. 11. And here there is already evidence of a breach of security: one week after Mr. Elez's departure, Defendants still do not know whether Mr. Elez's actions compromised the Bureau's systems or the personal information contained therein. *See supra* p.6.

The government suffers no harm from an injunction that ends an unlawful practice. Defendants maintain that the public has an interest in preventing the misspending of government funds and in ensuring that the duly elected President can pursue his policy aims. Opp. 25. But there is no public interest in pursuing these goals through unlawful means. And Defendants have not explained why they could not achieve their objectives without putting Plaintiffs' personal information at risk. The balance of equities and public interest therefore support an injunction that would stop Defendants from placing sensitive government records in the hands of unaccountable third parties.

CONCLUSION

The Court should grant the motion for a preliminary injunction.

February 18, 2025

Respectfully submitted,

/s/ Nandan M. Joshi
Nandan M. Joshi (DC Bar No. 456750)
Nicolas Sansone (DC Bar No. 1686810)
Allison M. Zieve (DC Bar No. 424786)
Public Citizen Litigation Group
1600 20th Street NW
Washington, DC 20009
(202) 588-1000

Norman L. Eisen (DC Bar No. 435051)
State Democracy Defenders Fund
600 Pennsylvania Avenue SE
#15180
Washington, DC 20003