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

ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue, NW
Washington, D.C. 20036

DOE 1

Plaintiffs,

v.

Case No. 1:25-cv-00255

U.S. OFFICE OF PERSONNEL MANAGEMENT
1900 E Street NW
Washington, DC 20415

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

DEPARTMENT OF THE TREASURY
1500 Pennsylvania Avenue NW
Washington, DC 20220

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

U.S. DIGITAL SERVICE (U.S. DOGE SERVICE)
736 Jackson Place NW
Washington, D.C. 20503

ACTING U.S. DOGE SERVICE ADMINISTRATOR
736 Jackson Place NW
Washington, D.C. 20503

U.S. DOGE SERVICE TEMPORARY ORGANIZATION
736 Jackson Place
Washington, D.C. 20503

Defendants.

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

Plaintiffs have alleged a massive data breach: with the full cooperation of the Treasury and OPM Defendants, DOGE Defendants have unlawfully accessed personal and sensitive information of millions of people, including Plaintiff Doe and Plaintiff EPIC's members. Despite the scale and severity of this breach, Defendants offer essentially a single defense—that there has been no breach at all because Treasury and OPM systems have only been accessed by Treasury and OPM employees. But this defense holds no water.

Plaintiffs have demonstrated ample entitlement to a temporary restraining order. Contrary to Defendants' assertions about the employment status of DOGE operatives and Defendants' various other arguments, Plaintiffs have standing to bring their claims,[1] face irreparable harm, and have demonstrated a likelihood of success on the merits. Absent intervention by this Court, the unlawful data breach will continue to imperil Americans' information.[2]

[1] Plaintiffs submitted several declarations in support of their motion. Defendants asserted in their Opposition that the filed declaration of Plaintiff Doe is "blank," and that the filed declaration of EPIC President and Executive Director Alan Butler is "unsigned." Defs. Br. in Opp'n to Pls. Mot. for TRO (hereinafter "Defs. Opp'n.") at 13 n.6 (Feb. 18, 2025), ECF No. 19. Plaintiffs first learned of any issue when Defendants raised it in their Opposition. Counsel for Plaintiffs have confirmed that Butler's declaration is signed and appears as such on ECF. Counsel for Plaintiffs have also confirmed that Plaintiff Doe's declaration is not blank, though a formatting error appears to have truncated a portion (approximately half) of its content on ECF. Plaintiffs have included with this filing a correctly formatted copy of the same declaration previously submitted by Plaintiff Doe, and, at Defendants' request, have provided copies of the declarations by Plaintiff Doe and Butler directly to Defendants' counsel earlier today.

[2] Defendants seek to convert the pending motion for a temporary restraining order to a motion for preliminary injunction on the basis of authority that such conversion will not prejudice Defendants. Because of the abbreviated briefing schedule necessary for a motion for temporary restraining order, Plaintiffs have had 24 hours to prepare this Reply, including review of declarations submitted for the first time in support of

I. Defendants have not meaningfully disputed that non-agency employees have accessed OPM and Treasury's sensitive information systems

The thrust of Defendants' opposition is that every employee who has been granted access to data systems at the Department of Treasury and the Office of Personnel Management is a qualified employee of the relevant agency. But Defendants' declarations tell a different story. At Treasury, Thomas Krause, who describes himself as the sole "DOGE team" member, continues to take direction from DOGE and to report back on his progress. Defs. Opp'n, Ex. A ¶ 4.[3] At OPM, a single declarant with limited knowledge believes the individuals "central to" DOGE's mission are employed by OPM, Defs. Opp'n, Ex. C ¶ 8—but others, evidently, may not be, and Defendants state only selectively that such individuals have received the relevant security trainings.

According to Defendants, "currently, there is only one member of Treasury's [DOGE] team, Thomas Krause," Defs. Opp'n at 4, the self-described lead and sole member of the DOGE team at Treasury, Defs. Opp'n Ex. A ¶¶ 2-3. Defendants acknowledge that there was formerly at least one other member of the DOGE team at Treasury, *see* Defs. Opp'n at 4 n.2, and admit that individual had "read/write" access to Treasury systems. Defs. Opp'n Ex. A at 8 n. 3, Defs. Opp'n Ex. D ¶ 20. But neither Defendants nor their declarations indicate whether those two individuals are the only DOGE personnel who

---

Defendants' opposition. In light of the fast-developing and complex nature of this dispute, Plaintiffs believe the Court would benefit from the more robust, though expeditious, development of the factual circumstances and legal issues which would be possible in the context of a motion for Preliminary Injunction.

[3] Krause's deposition contains a photograph of a "wet" signature. That photograph shows that Krause signed page 3 of an unidentified document. His declaration is 11 pages long. Plaintiffs promptly contacted counsel for Defendants to confirm whether Krause had in fact reviewed and attested to the full contents of his declaration; Defendants' counsel have stated that he did so.

have ever had access to Treasury systems. While Defendants insist that Krause is "not an employee of" DOGE, Defs. Opp'n at 4, his own declaration makes clear that DOGE directs his work and that he provides DOGE with regular updates and coordinates his work with them, Defs. Opp'n, Ex. A ¶ 4.

Functionally, Krause is a DOGE employee. Defendants observe that Krause was hired directly by Treasury and treat that fact as *per se* proof that he is a Treasury employee. Defendants cite to no authority in support of this formulaic inference, which would be susceptible to all manner of abuse, and which contradicts the "functional approach," Defs. Opp'n at 15, that Defendants advocate for identifying the true employer of detailees. "[A]ll the circumstances," *Judicial Watch, Inc. v. Dep't of Energy*, 412 F.3d 125, 131 (D.C. Cir. 2005) (quoting *Spirides v. Reinhardt*, 613 F.2d 826, 831 (D.C. Cir. 1979)), of Krause's employment make clear that he is functionally a DOGE employee: he takes direction from DOGE, Defs. Opp'n Ex. A ¶ 4, occupies a position "created to help effectuate the mission of" DOGE, *id.* ¶ 2, and performs work in support of DOGE's mission, *id*.

And while Krause apparently currently is the sole DOGE Team member, Executive Order 14158 instructs that at least three more employees join his Treasury "DOGE Team" by today. Exec. Order No. 14158, 90 Fed. Reg. 8441, Establishing and Implementing the President's 'Department of Government Efficiency' (Jan. 20, 2025) (hereinafter "Exec. Order No. 14158") § 3(c) ("DOGE Team" of at least four members to be "hired or assigned" within 30 days of order). Krause makes does not explain the status of those additions, who those individuals will be, or the process for ensuring protections for records they seek to access.

Krause explains that Treasury's Bureau of the Fiscal Service ("BFS") recommended "multiple mitigation measures" to combat the risks of DOGE access to sensitive information and notes that "a number" of those measures were implemented. Defs. Opp'n Ex. A ¶ 15. But neither Defendants, Krause, nor any other declarant indicate how many—or which—of those measures went unimplemented. Krause's declaration not only calls his own employment status and qualifications to access data into question, but raises even more questions about whether Treasury has any safeguards in place for other DOGE operatives.

The picture at OPM is even hazier. Defendants rely on a single declaration from Greg Hogan, Chief Information Officer at OPM, that "All individuals with access to sensitive OPM records systems . . . who are central to implementing [DOGE's mission] are employees of OPM," Defs. Opp'n at 5—but even that assurance is made only "to the best of [the] knowledge" of Hogan, whose role does not include human resources functions and only reviewed information from OPM's human resources department. Defs. Opp'n. Ex. C ¶¶ 1, 3, 12. Hogan states his awareness that "some OPM employees also have employment relationships, such as detail agreements, with other agencies," *id.* ¶¶ 1, 13, but does not state whether any of those individuals have such arrangements with DOGE specifically. His declaration provides no assurances that personnel "onboarded directly by OPM" are not also employed by DOGE, reporting to DOGE, or taking direction from DOGE, akin to Krause's role at Treasury. And there is no indication that all individuals "central to" DOGE's work encompasses all DOGE personnel with access to OPM data systems. Nor does Hogan rule out additional access in the future.

While Hogan attests that he has personally "completed OPM's required privacy, IT security, and ethics trainings," *id.* ¶ 5, he cannot say the same for those "central to" DOGE's work at OPM, let alone all DOGE personnel who might have access. Hogan declares that "OPM employees who have participated in workforce reform . . . are subject to applicable privacy, ethics, and other requirements," *id.* ¶ 9, but again, does not indicate whether there are DOGE employees who are not covered by that statement. And Hogan refers to one engineer from another agency (presumably DOGE) currently serving as a Special Government Employee at OPM who "has received records training" and is subject to an agreement that he "shall not share any OPM data with the other agency," *id.* ¶ 13. But he cannot say the same of the other personnel referenced. And unlike Defendants' allegations as to Treasury, Defendants do not name a single member of the DOGE team at OPM nor provide any evidence of the training they have received or limitations on their systems access.

Defendants assert there is nothing "sensational" here, because "it is the agencies' employees, and only those employees, who have access to the data systems containing" Plaintiffs' confidential personal information. Defs. Opp'n at 1–2. But the Treasury "DOGE Team" consists of only a DOGE employee, and Defendants' declarations offer no meaningful assurance that the numerous DOGE operatives at OPM are OPM employees, have received requisite trainings, or are subject to any meaningful limits on their system access. Defendants' opposition to Plaintiffs' motion depends on DOGE operatives being employees of the respective agencies whose data they access; but Defendants provide no basis to conclude they are beyond conclusory statements contradicted by facts and inconclusive impressions from sources without relevant knowledge.

Nor is it any answer that Executive Order 14158 supposedly creates a "need to know" for DOGE access to agency systems under the Privacy Act. Defs. Opp'n at 16. The "need to know" Privacy Act exception allows access by "officers and employees *of the agency,*" 5 U.S.C. 552a(b)(1), (emphasis added) with a "need to know," an assessment that should be made by the relevant agency in the first instance, not Presidential fiat untethered from specific agency authorities and the particular requirements of various record systems.[4] Nor can the need to know exception reach DOGE operatives who are not employees of the relevant agencies here.

II. Plaintiffs have demonstrated standing to challenge Defendants' intrusion into their privacy.

Plaintiffs have pled that the intrusion on their privacy has caused an injury with a "close relationship to a harm traditionally recognized as providing a basis for a lawsuit in American courts." *Fernandez v. RentGrow, Inc.*, 116 F.4th 288, 295 (4th Cir. 2024) (internal citations and quotation marks omitted). "Those include, for example, reputational harms, disclosure of private information, and intrusion upon seclusion." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 425 (2021). "The common law has long recognized a right to personal privacy," and "it has long been the case that an unauthorized dissemination of one's personal information, even without a showing of actual damages, is an invasion of one's privacy that constitutes a concrete injury sufficient to confer standing to sue." *Witt v.*

[4] Nor does Executive Order 14158 purport to create a "need to know" for Privacy Act purposes; to the contrary, it merely instructs agencies to grant the US DOGE Service access to systems, Exec. Order 14158 § 4(b), and instructs that implementation shall be "consistent with applicable laws." *Id.* § 5(b). Insofar as the instruction concerns agencies granting system access to people who are, by the Order's terms, not employees of the granting agency, there is no plausible way to read the Order as creating a "need to know" for agency employees within the meaning of 5 U.S.C. §552a(b)(1).

CoreLogic Saferent, LLC, No. 3:15-cv-386, 2016 WL 4424955, at *12 (E.D. Va. Aug. 18, 2016). And "Congress may create a statutory right to privacy in certain information that *strengthens or replaces* the common law, and citizens whose statutory right to informational privacy has been invaded may bring suit under the statute to vindicate that right." *Id.* at *13 (emphasis added). Congress did so when it passed the Privacy Act and when it codified data protections in the Internal Revenue Code. Defendants' access to Plaintiffs' data in violation of those statutes has effected a disclosure of their personal confidential information.

That invasion of privacy has also violated Plaintiffs' constitutional rights; Defendants' musings as to whether the Supreme Court has recognized that right do not change that the Fourth Circuit has done so expressly. *See Payne v. Taslimi*, 998 F.3d 648, 655 (4th Cir. 2021) ("The [Supreme] Court [has] assumed, without deciding, that the Constitution protects an informational privacy right . . . we have gone beyond assuming. . . . the constitutional right to privacy extends to ... 'the individual interest in avoiding disclosure of personal matters.") (cleaned up). Defendants' arguments against the availability of that right are similarly unavailing. Defendants point to authority suggesting that statutory and regulatory duties to protect information may "allay" privacy concerns which might otherwise caution against government *collection* of information, but those authorities provide no basis to believe that a robust statutory scheme allays those concerns when it comes to the government's failure to abide by those same duties. Defendants then advance the evidently unprecedented argument that a violation of Plaintiffs' constitutional privacy rights is cognizable only if the violation meets the wholly separate standard for substantive due process claims. Defendants point to no authority to for this novel theory,

other than arguing that substantive due process claims challenging executive action must show that the action "shock[ed] the conscience." Defs. Opp'n at 26. This Court should decline Defendants' invitation to import that high bar to the constitutional right to privacy. If this Court should do so, Plaintiffs nevertheless believe that an organized effort by the government to divulge highly sensitive and personal information of millions of Americans in violation of legal protections meets the "shocks the conscience" standard.

Plaintiffs clearly allege and substantiate via declarations that they have been injured by the disclosure of their private information and the invasion of their privacy. *See* Pls. Mot. for TRO at 1, 22–23. Plaintiffs have also suffered an injury similar to that recognized in the common law tort of intrusion upon seclusion. *See TransUnion*, 594 U.S. at 425 (listing intrusion upon seclusion as example of harm which traditionally served as the basis for lawsuit in American courts). 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 . . . if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts § 652B (Am. L. Inst. 1977). Here, the DOGE defendants have intentionally intruded upon Plaintiffs' private information through large-scale unlawful data access—the corresponding infringement on Plaintiffs' privacy has a "close relationship," *Fernandez*, 116 F.4th at 295, to the harm traditionally recognized as the basis for an intrusion upon seclusion suit.

And when evaluating whether an injury is sufficiently concrete for standing purposes, "Congress's views may be instructive. Courts must afford due respect to Congress's decision to impose a statutory prohibition or obligation on a defendant, and to grant a plaintiff a cause of action to sue over the defendant's violation of that statutory

prohibition or obligation." *TransUnion*, 594 U.S. at 425. Congress clearly recognized the value of privacy and the gravity of injuries arising out of the invasion thereof when it passed the Privacy Act and codified privacy protections into the Internal Revenue Code, and gave private individuals causes of action to recover for such injuries in both statutes.

Moreover, interagency sharing of information may cause injury to Plaintiffs' right to informational privacy, even absent disclosure outside the government. Defendants have articulated no reason that the right would be abrogated simply because disclosure occurs within the government. Congress passed the Privacy Act specifically in response to intragovernmental disclosures and misuse of private information within the government,[5] recognizing disclosures within the government as implicating privacy interests. 5 U.S.C. § 552a(b). The only authority Defendants cite to the contrary is inapposite. The D.C. Circuit, in *In re U.S. Off. Of Personnel Mgmt. Data Sec. Breach Litig*., 928 F.3d 42 (D.C. Cir. 2019), drew no distinction between intragovernmental and external disclosures; rather, it noted only that any constitutional right to privacy is implicated by intentional disclosure, not accidental disclosure. That conclusion is consistent with a theory of harm that relies in part on intrusion upon seclusion, and, in any event, poses no obstacle where, as here, the relevant disclosure is the result of government actors *intentionally* granting unlawful access to their systems. Defendants argue that there has been no specific disclosure of Plaintiffs' data, and that all that has happened is that DOGE employees have accessed systems containing their data. But that disclosure—DOGE's unlawful access to Plaintiffs'

[5] Ctr. for Am. Progress, *Lessons From Watergate* (Jul. 30, 2018), https://tinyurl.com/3muyyarj.

information housed by Treasury and OPM—is precisely the disclosure which has injured Plaintiffs.

Plaintiffs have also demonstrated that they will suffer irreparable harm if this Court does not grant their requested relief. "The denial of a constitutional right. . . constitutes irreparable harm for purposes of equitable jurisdiction." *Ross v. Meese*, 818 F.2d 1132, 1135 (4th Cir. 1987). Faced with this black-letter principle, Defendants again retreat to their argument that Plaintiffs have not adequately alleged a violation of their constitutional right against disclosure of private information. Defs. Opp'n at 28 n.13. But Plaintiffs have done so, and the violation of their constitutional right constitutes irreparable injury *per se*. Even absent the constitutional right, however, unauthorized disclosure of information is an archetypal irreparable harm: once information is released, it is "a bell that one cannot unring." *Senior Executives Ass'n v. United States*, 891 F. Supp. 2d 745, 755 (D. Md. 2012); *see also Council on Am.-Islamic Rels. v. Gaubatz*, 667 F. Supp. 2d 67, 76-77 (D.D.C. 2009) (access to "confidential employee personal information" constitutes irreparable harm); *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000) ("disclosure of confidential information . . . is the quintessential type of irreparable harm.") (cleaned up).

III. The decision of Treasury and OPM to grant access to DOGE personnel is subject to judicial review under the Administrative Procedure Act.

The Administrative Procedure Act, 5 U.S.C. § 704, allows judicial review of "final agency action for which there is no other adequate remedy in a court." Defendants' adoption of access policies at Treasury and OPM allowing DOGE and DOGE affiliates broad (if not unfettered) access to Defendants' systems is precisely such an action.

First, final agency actions are those (1) which "mark the consummation of the agency's decisionmaking process," as opposed to decisions of a "merely tentative or

interlocutory nature;" and (2) "by which rights or obligations have been determined, or from which legal consequences will flow." *U.S. Army Corps of Eng'rs v. Hawkes Co., Inc.*, 578 U.S. 590, 597 (2016) (quoting *Bennett v. Spear*, 520 U.S. 154, 177–178 (1997)). Defendants' action, like other agencies' adoption of access policies, *see, e.g. Venetian Casino Resort, L.L.C. v. EEOC*, 530 F.3d 925, 931 (D.C. Cir. 2008), satisfies both prongs.

Plaintiffs have alleged, and Defendants have not disputed, that the decision to grant DOGE affiliates to Treasury systems was made by Secretary Bessent. Compl. ¶ 55 (Feb. 10, 2025), ECF No. 1. And Defendants have not identified any policy that allows non-employees of the Department of Treasury to have such access. In short, the Secretary of the Treasury adopted a new access policy allowing unprecedented system access. Defs. Opp'n, Ex. D ¶ 13 (access was "broader in scope than what has occurred in the past"). That decision was the consummation of the agency's process and was in no way interlocutory: it was made at the highest level of the agency, and took effect almost immediately. *Id.* ¶ 16 (DOGE gained access to Treasury systems on January 28, one day after Bessent's adoption of the new policy). And the policy immediately determined Treasury *obligations* to provide data access to DOGE operatives, affected the legal rights of millions of Americans whose data were compromised, and had substantial legal consequences by virtue of altering existing privacy restrictions to provide access to sensitive information stored in government records systems to individuals who would not have had access under the prior restrictions.

The analysis is the same as to OPM's new access policy. Plaintiffs have alleged, and Defendants have not disputed, that OPM simply granted universal system access to DOGE operatives, who then locked career OPM employees out of those same system. That

decision was clearly OPM's last word on the matter, and was quickly effected, immediately creating the same legal consequences as the Treasury policy.[6]

Second, no other adequate remedy in a court is available to review these final agency actions. Plaintiffs' personal information is included in systems of record which have been deliberately breached by unauthorized actors affiliated with the federal government, with the full cooperation of the agencies responsible for protecting that information. Unlike other instances of government data breaches, the unlawful disclosure here is by government officials purporting to act under color of law; there is little reason to believe the government would ever inform affected individuals that their data had been unlawfully disclosed. Retroactive money damages under 5 U.S.C. § 552a(g)(4) cannot meaningfully remedy that breach. Nor can damages or any other relief provided in the Privacy Act halt an ongoing breach. Though the Privacy Act does not provide such a remedy, the APA does. Courts have acknowledged the APA as a mechanism for injunctive relief against prohibited disclosures, *see e.g. Doe v. Chao*, 540 U.S. 614, 619 n.1 (2004); *Doe v. Stephens*, 851 F.2d 1457, 1460–61, 1463 (D.C. Cir. 1988). Where, as here,

[6] Defendants say that "[f]or systems engineers who require access to sensitive systems, . . . OPM periodically reviews access permissions to ensure that they are limited to those with a need to know." Defs. Opp'n, Ex. C ¶ 11. But it is not clear whether that review process applies to DOGE personnel, because Defendants do not clarify whether DOGE personnel count as "systems engineers," or provide any other characterization of what role DOGE personnel play. And according to Defendants, all DOGE personnel always have a "need to know" "*all* unclassified agency records, software systems, and IT systems," Defs. Opp'n at 16, so it is not clear that OPM would ever revoke their access.

injunctive relief can prevent (or end) prohibited disclosures, the Privacy Act's remedial scheme does not bar injunctive relief under the APA.

IV. The Administrative Procedure Act allows judicial review of failure to follow FISMA.

Although *how* an agency implements FISMA is committed to agency discretion, *whether* an agency complies with FISMA is not. *See Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006) (declining to decide whether an agency's implementation of FISMA was sufficient, but also declining to find that "FISMA is a "statute[ ] preclud[ing] judicial review" under 5 U.S.C. § 701(a)"). Contrary to Defendants' characterization, Plaintiffs do not seek review of the specific security measures Defendants have adopted are adequate under FISMA—rather, Plaintiffs allege that Defendants have disregarded or replaced their own presumptively adequate security policies. Compl. ¶¶ 39-40, 46-47, 73, 95. Agencies set the specific parameters of information security policy squarely within their discretion under *Holbrook v. Tennessee Valley Auth.*, 48 F.4th 282 (4th Cir. 2022), but once those policies are set, *Holbrook* does not shield agencies from judicial review for wholly ignoring those same policies. Congress' rationale for insulating agencies' FISMA policies from judicial review—ensuring that agencies could exercise appropriate judgment and discretion in choosing among technical solutions, 44 U.S.C. § 3551(6)—does not mean that agencies have *carte blanche* to choose no security policy.

CONCLUSION

The Court should grant Plaintiffs' motion and enter a temporary restraining order.

Dated: February 19, 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

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)

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

*pro hac vice *application pending*
**pro hac vice *application forthcoming*

Counsel for Plaintiffs