UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

CENTER FOR TAXPAYER RIGHTS et al., *Plaintiffs*, v. INTERNAL REVENUE SERVICE et al., *Defendants*.	Civil Action No. 25-cv-457-CKK

MEMORANDUM IN OPPOSITION TO DEFENDANTS' MOTION TO DISMISS

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Statutes

Other Authorities

Rules and Regulations

INTRODUCTION

The "Department of Government Efficiency" or "DOGE"—a loose affiliation of individuals spread out across the Executive Branch and directed by individuals in the Executive Office of the President—was purportedly created for the purpose of rooting out "fraud, waste, and abuse" in the federal government. But although the quintessential abuse of tax evasion occurs disproportionately at the top end of the income distribution,[1] DOGE personnel embedded at and working with the Internal Revenue Service ("IRS") have trained their sights on accessing and sharing the protected data of the most vulnerable groups of taxpayers: immigrants, low–income taxpayers, and recipients of public benefits.

At the IRS, DOGE pursued reversal of decades of IRS policy, ignoring laws protecting the confidentiality of tax return information, to enable the large–scale disclosure of taxpayer data to other agencies for purposes having nothing to do with tax administration, including to the Department of Homeland Security ("DHS") to use in immigration enforcement. They advanced this agenda over the objections of IRS leadership and long–serving senior executive service IT staff, such that scores of senior agency staff have either been put on administrative leave or quit. The IRS ultimately followed DOGE's direction, adopting a new interagency data–sharing policy, with concrete steps taken to implement that policy; data sharing on a massive scale is expected imminently.

The IRS's decision to authorize and build infrastructure to facilitate large–scale access to and inter–agency sharing of taxpayer return information (the "Data Policy") is arbitrary and capricious, was undertaken without legal authority, and will necessarily lead to widespread violations of the Internal Revenue Code's confidentiality provisions, 26 U.S.C. § 6103 and 26

[1] John Guyton, et al., *Tax Evasion at the Top of the Income Distribution: Theory and Evidence*, Wash. Ctr. for Equitable Growth (Mar. 2021), https://perma.cc/L9JV-3XT3.

U.S.C. § 7213A, as well as the Privacy Act. The Data Policy not only endangers the privacy interests of taxpayers; it also risks the integrity of the tax system as a whole. Plaintiffs bring this challenge to set aside this policy change and enjoin further actions to implement it.

Plaintiffs filed this case to protect sensitive data systems at Defendant Agencies and shield their members' and clients' data from unauthorized access by DOGE Affiliates, from unlawful disclosure to other agencies, and from other unauthorized use, access, and disclosure resulting from the IRS's new Data Policy. Plaintiffs argue that the Data Policy violates the Internal Revenue Code, the Privacy Act, and the Administrative Procedure Act, and that DOGE's actions are *ultra vires*.

Plaintiffs' allegations are sufficient to make their standing plausible and to state a claim. Plaintiffs' members and clients are among those groups whose information DOGE seeks to access and share via the new Data Policy, and Plaintiffs have provided specific, detailed factual allegations that make the imminence of these privacy injuries plausible. For example, the IRS has already entered into at least one memorandum of understanding with another agency to share taxpayer return information and is working with a government contractor to build the technical infrastructure necessary to facilitate mass data sharing. And Plaintiff Center for Taxpayer Rights has already suffered harm as a result of the Data Policy, as it has been forced to expend significant resources to counteract the effects of the policy of the core services the Center provides. Equitable relief to prevent these injuries is unavailable under the Internal Revenue Code and the Privacy Act, making relief under the Administrative Procedure Act necessary. Finally, the DOGE Defendants have acted with such lawlessness that Plaintiffs also have a plausible claim that this behavior is *ultra vires*. Plaintiffs respectfully request that the Court deny Defendants' motion to dismiss.

BACKGROUND

I. At DOGE's Direction, the IRS Has Changed its Policy, Creating Unprecedented Broad Sharing Mechanisms for Sensitive, Protected Data.

A. The IRS's Longstanding Protective Data Sharing Policy was Implemented to Protect People Against Government Abuses of their Confidential Information

The IRS collects and maintains the sensitive and confidential data of more than 150 million individual taxpayers and millions more businesses. Plaintiffs' First Amended Complaint ("Am. Compl.") ECF No. 20, ¶ 75. This data includes social security numbers ("SSNs"), individual taxpayer identification numbers ("ITINs"), addresses, bank account and employment information, medical expense information, and confidential business information. *Id*. In the wake of abuses by the Nixon Administration, including efforts to use confidential information to target political enemies, Congress passed the Tax Reform Act of 1976, which implemented significantly more protective controls and limitations on the sharing of IRS tax information within the federal government. *Id.* ¶¶ 79–81.[2] The IRS policy manual implements these statutory requirements with detailed requirements and limitations on how taxpayer information may be accessed and disclosed. *Id.* ¶¶ 83–93. The Privacy Act, another post-Watergate recalibration, was enacted two years earlier to protect sensitive personal data held by all federal agencies across the federal government. 5 U.S.C. § 552a.[3]

[2] Citing Taxpayer Advoc. Serv., *National Taxpayer Advocate: 2003 Annual Report to Congress* at 245 (Dec. 31, 2003), https://perma.cc/T6ZD-Q6VL [hereinafter "Taxpayer Advocate Report"] (explaining that the Act significantly limited "the rules governing the availability of tax information to Federal agencies for purposes of nontax criminal cases," and that the Senate Finance Committee determined that an individual's tax information is "entitled to essentially the same degree of privacy as those private papers maintained in his home").

[3] Sam Berger and Alex Tausanovitch, *Lessons From Watergate*, Ctr. for Am. Progress (July 30, 2018), https://perma.cc/M8XB-NDF8.

Each of these statutes requires that Plaintiffs' members' information be kept confidential. Section 6103 specifies that "[r]eturns and return information shall be confidential," and it prohibits any inspection or disclosure of that information unless the requirements for one of the listed exceptions have been established. 26 U.S.C. § 6103(a). Its exceptions are either connected with tax administration or permit inspection or disclosure to other federal agencies only for specific, limited purposes. *See id.* §§ 6103(i), (j), and (l). Treasury Department officers and employees can only be granted access to inspect or disclose tax information where their "official duties require such inspection or disclosure for tax administration purposes." *Id*. § 6103(h)(1). And 26 U.S.C. § 7213A prohibits IRS employees and officers from inspecting returns or return information without authorization. Similarly, the Privacy Act permits disclosure of protected information within systems of records without consent only "to those officers or employees" who have a "need for the record in the performance of their duties," or to another agency in response to a specific law enforcement request, or under other specific conditions. *See* 5 U.S.C. § 552a(b).

Beyond these statutory limitations, the IRS has long restricted how personal and business information can be shared within and outside of the IRS. *Id*. ¶¶ 83, 93.[4] For IRS employees, tax return information could be accessed only when there is a "need to know" the information for tax administration duties, and that need to know must be established on a case-by-case basis. Am. Compl. ¶ 86. The IRS also strictly limits the sharing of sensitive tax information data with other agencies. *Id*. ¶ 93.[5] For example, the IRS policy manual requires employees to complete rigorous

[4] *See, e.g.,* Internal Revenue Manual § 10.5, "Privacy and Information Protection," IRS (last updated Jan. 27, 2020), https://perma.cc/JP7T-9WEX [hereinafter "IRM"].

[5] Citing IRM § 11.3.28.2, "Disclosure of Returns and Return Information Pursuant to IRC 6103(i)(1), IRC 6103(i)(5), and IRC 6103(i)(7)(c)," IRS (last updated Apr. 17, 2025), https://perma.cc/SF8W-HQWR ("Congress decided that federal law enforcement officials should not have easier access to information about a taxpayer maintained by the IRS than they would have if they sought to compel the production of that information from the taxpayer themselves.")

steps prior to disclosing any tax information under each provision of Sec. 6103. *Id*. ¶ 84. Historically, the IRS limits interagency sharing or combining of taxpayer information, permitted "only where the agency can demonstrate, using established criteria, a need for the information that clearly outweighs taxpayer privacy interests and concerns about the effect on voluntary tax compliance."[6] *Id*. ¶¶ 79, 93. Specifically, the Department of the Treasury has explained, "if IRS [taxpayer] data is to be provided [to other agencies] at all, the IRS should be the last stop—not the first—for information for purposes unrelated to tax administration."[7]

The combination of IRS's adherence to statutory requirements, compliance with the IRS policy manual, and IRS leadership's prioritization and implementation of privacy-protective practices has established a longstanding policy (the "Privacy Policy") that has spanned decades and administrations. The Privacy Policy was grounded in key principles, which were integrated into data-sharing and data-access decisions made by IRS leadership, based on statutory requirements and longstanding agency judgment. These included the following:

- Prioritizing public trust[8]

---

[6] Am. Compl. ¶ 79 n.5 (quoting Taxpayer Advocate Report at 241); Taxpayer Advocate Report at 83.

[7] Taxpayer Advocate Report at 233 n.1 (quoting Dep't of Treasury, *Report to the Congress on Scope and Use of Taxpayer Confidentiality and Disclosure Provisions, Vol. I: Study of General Provisions* at 34 (Oct. 2000), *available at* https://perma.cc/2LC2-M9F5).

[8] *See, e.g*., IRS, Tax Information Security Guidelines at 23, https://perma.cc/9EEP-KZ6D ("The IRS must administer the disclosure provisions of the Internal Revenue Code (IRC) according to the spirit and intent of these laws, ever mindful of the public trust."); *Gardner v. United States*, 213 F.3d 735, 738 (D.C. Cir. 2000) (internal citation omitted) ("This general ban on disclosure provides essential protection for the taxpayer…The assurance of privacy secured by § 6103 is fundamental to a tax system that relies upon self-reporting."); *see also* Am. Compl. ¶ 171, citing Jacob Bogage and Shannon Najmabadi, *Acting IRS chief to quit over deal to share data with immigration authorities*, Wash. Post (Apr. 9, 2025), https://perma.cc/D7XE-7FDD (explaining "the tax agency's longtime guarantee that taxpayers suspected of being in the country illegally wouldn't have their information turned over to immigration enforcement").

- Protecting taxpayer information within the IRS *and* at agencies that receive taxpayer information, including by segregating taxpayer information across databases[9]
- Evaluating disclosures of taxpayer information on a case-by-case basis[10]
- Disclosing IRS data only when other data cannot suffice[11]
- Limiting political interference, including by limiting access to taxpayer information by political appointees[12]
- Ensuring that agencies receiving IRS taxpayer information must "have adequate programs in place to protect the data received"[13]

This Privacy Policy has been well understood by the IRS and the public alike. For decades, the IRS has assured the American public that their data in its possession is confidential. A 2013 publication for government employees stated it succinctly: "The General Rule - Tax Information Is Confidential!"[14]

---

[9] Am. Compl. ¶ 107, citing Hannah Natanson, et al., *DOGE aims to pool federal data, putting personal information at risk*, Wash. Post (May 7, 2025), https://perma.cc/9JCK-9K4W ("'Separation and segmentation is one of the core principles in sound cybersecurity,' said Charles Henderson of security company Coalfire. 'Putting all your eggs in one basket means I don't need to go hunting for them — I can just steal the basket.'"); *See, e.g.*, Tax Information Security Guidelines, https://perma.cc/9EEP-KZ6D.

[10] *See, e.g.*, IRM § 11.3.22.2, "Disclosure to certain Federal Officers and Employees for Tax Administration Purposes under IRC 6103(h)" (last updated Aug. 9, 2024), https://perma.cc/5ZN4-NM4E.

[11] *Supra note 7*.

[12] Am. Compl. ¶ 146 (citing Jacob Bogage and Jeff Stein, *Musk's DOGE seeks access to personal taxpayer data*, Wash. Post (Feb. 16, 2025), https://perma.cc/GJ38-S2M2) ("[I]t's highly unusual to grant political appointees access to personal taxpayer data, or even programs adjacent to that data, experts say.").

[13] Tax Information Security Guidelines at 23, https://perma.cc/9EEP-KZ6D.

[14] IRS, *Protecting Federal Tax Information for Government Employees*, Publication 4761 (Rev. 9-2013), https://perma.cc/5KYH-MNYB.

B. At DOGE's Direction the IRS Changed its Privacy Policy Quickly, Without Explanation, and Against the Advice of Legal and Privacy Experts.

On January 20, 2025, President Trump established the "Department of Government Efficiency" ("DOGE") Service (previously the U.S. Digital Service), and the U.S. DOGE Service Temporary Organization, to help the new Administration "dismantle," "slash," and "restructure" federal programs and services. *Id.* ¶ 94. The Executive Order establishing DOGE also required that each agency head establish a "DOGE Team," and take steps to ensure the team "has full and prompt access to all unclassified agency records, software systems, and IT systems." *Id.* ¶¶ 98, 99. As DOGE spread throughout the federal government, some DOGE employees have joined a DOGE Team, been detailed to an agency, and then been hired directly by the host agency. *See, e.g.*, ¶¶ 102–105. This has created a vast network of DOGE Affiliates throughout the federal government tasked with carrying out the President's DOGE agenda, to include broad access to, and use and disclosure of data at agencies across the government, including the IRS. *Id.* Regardless of their formal employer, DOGE Affiliates are often identified as representatives of DOGE and appear to work to implement DOGE's agenda and directives. *Id.*

DOGE team members across the government have sought to gather up as much data as possible, with little regard for legal protections on inter-agency data sharing. Am. Compl. ¶¶ 107–113. DOGE team members have also disregarded existing legal protections and policies: publicly disclosing classified information, Am. Compl. ¶ 113, emailing unencrypted personal information to another agency, *id*., providing access to sensitive data to a DOGE affiliate in the State Department who had previously been terminated from an internship for disclosing sensitive, protected commercial information, Am. Compl. ¶ 114, and evading common cybersecurity measures used at agencies to log and monitor system access, after which—at one agency—the agency detected suspicious log-in attempts from an IP address in Russia, Am. Compl. ¶ 125.

Consistent with this reckless approach, upon arriving at the IRS, DOGE team members Gavin Kliger and Sam Corcos demanded access to systems of confidential tax records, without apparent authority to do so and before appropriate background checks and onboarding steps had been taken. Am. Compl. ¶¶ 146, 156, 159, 160.

As Plaintiffs allege, following DOGE's arrival at IRS, the agency adopted a new policy on data access and sharing (hereinafter the "Data Policy").[15] In so doing, IRS abandoned its prior promise that taxpayer information be kept confidential, including within the government, and that access and disclosures be strictly minimized. *See* Am. Compl. ¶¶ 83–91, 184.

The new Data Policy (1) greatly expands access to and use of taxpayer information within the IRS *see* Am. Compl. ¶ 182; (2) consolidates data systems to facilitate broad, not segregated access within the agency, *see id.*; and (3) permits large-scale data-sharing with other agencies, unrelated to tax administration, *see id.* ¶¶ 185–187. The Data Policy:

- Prioritizes data sharing above public trust and privacy
- Directs the consolidation of data to facilitate broad access by IRS employees
- Permits broad access to taxpayer information by political appointees and/or for political purposes
- Promotes the use of IRS data by other agencies as a comprehensive data source
- Permits large-scale disclosures of information on an automated basis
- Facilitates interagency sharing through omnibus or template agreements

[15] *See also* Am. Compl. ¶ 161 (citing Makena Kelly, *Palantir Is Helping DOGE With a Massive IRS Data Project*, WIRED (Apr. 11, 2025), https://perma.cc/AF3S-6QP7) ("The goal is to have [the mega API] completed within 30 days"); *see also* Am. Compl. ¶ 160 (detailing an HR official being dismissed "after Kliger's demand for an expedited background check for his DOGE partner had not been fulfilled *over the weekend*") (emphasis added).

While IRS has not announced the Policy publicly, it is apparent from IRS actions over the past few months.[16] The fact of the new Data Policy's adoption began to become apparent when DOGE Affiliates sought and were ultimately granted broad access to IRS tax systems and datasets. Am. Comp. ¶¶ 145–46.[17] Previously, access to taxpayer information by political appointees was highly unusual, particularly for the purposes they purportedly needed the data. *See, e.g.*, ¶¶ 150–151. However, under the new Data Policy, the sharing of taxpayer information with political appointees, and the use of taxpayer information for political purposes, was not only permissible, it was prioritized and expedited. *See* Am. Compl. ¶¶ 155–160; *see also* Am. Compl. ¶¶ 82, 145–46, 150–51. These political appointees would "randomly drop by people's offices, demanding access to systems." Am. Compl. ¶ 160.

The adoption of the Data Policy is made clear by and has resulted in IRS's abandonment of data segregation as a privacy-protective measure. Traditionally, taxpayer data is stored across multiple different databases and systems across the IRS, accessed and used for specific purposes. Am. Compl. ¶ 91. Now, DOGE Affiliates are building a single, unified database of taxpayer information within the IRS including through the use of a software tool—known as an application programming interface ("API")—that will permit automated access to all IRS taxpayer information by IRS employees in one interface *Id.* ¶ 161.

[16] It appears the IRS and DOGE Affiliates are taking pains to keep its Data Policy and plans for inter-agency disclosures quiet and private. Much of the information in Plaintiffs' Amended Complaint and in news coverage is only public because a concerned employee or former employee has shared it. *See, e.g.,* William Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, ProPublica (July 15, 2025), https://perma.cc/6XGQ-KX6T ("The plan has been shrouded in secrecy even within the IRS, with details of its development withheld from regular communications. Several IRS engineers and lawyers have avoided working on the project out of concerns about personal legal risk.").

[17] *See* Opinion, *New York v. Trump*, 1:25-cv-01144 (S.D.N.Y. May 27, 2025), ECF No. 156 (showing Corcos access to Treasury systems).

Finally, the new Data Policy is revealed by, and led to significant changes in, how the IRS shares taxpayer information with other federal agencies for non-tax purposes. DOGE Affiliates have worked to create an "omnibus" agreement, Am. Compl. ¶¶ 169–170, and quick template agreements, Am. Compl. ¶¶ 187, to allow federal agencies broad access to taxpayer information for the purported purpose of cross-referencing with other government benefits and identifying fraud. The agency finalized at least one broad agreement to share IRS data with Immigration and Customs Enforcement ("ICE"), for use in immigration enforcement. Am. Compl. ¶¶ 171. Reflective of the Data Policy, a whistleblower disclosed to Congress in April that DOGE was building "massive database of SSA data and data from across the federal government, including the Internal Revenue Service (IRS), Department of Health and Human Services (HHS), and other agencies" and doing so "in a manner that disregards important cybersecurity and privacy considerations, potentially in violation of the law." *Id.* ¶ 135. The Administration has also articulated its intention to cross-reference and "reconcile" databases at different agencies for the purpose of "eliminat[ing] the waste and fraud." Am. Compl. ¶¶ 110, 113. And, since the Amended Complaint was filed, the Administration has moved forward with its efforts to gather data on SNAP recipients into a federal database that can be cross-referenced with other data,[18] like IRS taxpayer data. *See* Am. Compl. ¶ 170.

DOGE Affiliates are developing a "mega API" to create "a system for sharing protected taxpayer data broadly across the federal government." *Id.* ¶¶ 179–186. To do this, DOGE Affiliates engaged federal contractor Palantir, in a highly irregular procurement process, to rapidly transform a project originally intended to improve IRS customer service into one focused on creating a "mega API" that would allow access to broad swaths of IRS taxpayer data, including

[18] 90 Fed. Reg. 26521 (June 23, 2025).

names, addresses, social security numbers, tax returns, and employment information. *Id*. ¶ 180. DOGE reportedly intends for this work to facilitate use of Palantir's Foundry platform as a central access point for all IRS systems. *Id*. ¶ 182. A person with access could then view and potentially alter any records in any of those systems, and other Palantir tools, such as its Artificial Intelligence Platform, could be applied to the data. *Id*. The goal of the creation of this "mega API" is also to facilitate large scale sharing of IRS data across the federal government. *Id.* ¶¶ 183–184.

This adoption of the Data Policy is apparent not only through the changes in data access and sharing at the IRS, but also through examination of what has happened to any IRS employee who has raised concerns with the new Data Policy, or appeared to continue to adhere to the prior, longstanding Privacy Policy. At every step, DOGE Affiliates have put on leave, fired, or caused the resignation of IRS employees, including senior leadership, who resisted the new policy, including on the basis that the Data Policy violated the law. Am. Compl. ¶¶ 162–166. These included the Acting IRS Commissioner, the Chief Risk Officer, the Chief Privacy Officer, the Chief Financial Officer, the Chief Information Officer, the subsequent Chief Information Officer, Treasury's Acting Chief Information Officer, and approximately 50 senior IRS IT executives. *Id*. ¶¶ 162–167.[19] Each of these departures was linked to concern or resistance to the IRS's new Data Policy. *Id.* DOGE Affiliate Sam Corcos, on the other hand, was named the Chief Information Officer at Treasury. Am. Compl. ¶ 166. He is intricately involved in the implementation of the new Data Policy. *See id*. ¶ 161.

And though the Data Policy puts at risk millions of individuals' and businesses' taxpayer information, the Administration has expressed clear intentions about which groups of people it

[19] *See also* Natanson, et al., *DOGE aims to pool federal data, putting personal information at risk*, https://perma.cc/9JCK-9K4W/ (losing even "three agency leaders in three months is 'unprecedented'), cited at Am. Compl. 171.

intends to focus on, in its push to share, inspect, and cross-reference IRS data under the Data Policy. These groups include immigrants targeted for removal, Am. Compl. ¶¶ 171–173,[20] and lower-income taxpayers who receive particular tax credits, like the EITC[21] and participate in public benefits programs like the Supplemental Nutrition Assistance Program ("SNAP") and student loan and aid programs, Am. Compl. ¶ 170. And, as has been publicly reported, "the actions taken by DOGE inside IRS appear to be aimed at finding ways to use the agency's protected data to find undocumented immigrants."[22]

II. Since the Filing of the Amended Complaint, IRS Has Taken Further Steps to Implement this Policy, Seeking to Share Millions of Taxpayers' Data with ICE.

As Plaintiffs alleged in the Amended Complaint, the "IRS has already decided to begin large-scale data sharing with other government agencies," and such sharing "is posed to dramatically expand, within weeks or months." *Id*. at ¶ 140. Further details regarding such allegations have emerged since the filing of the Amended Complaint, demonstrating that the anticipated injuries to Plaintiffs' members and clients as a result of the Data Policy are imminent. Plaintiffs have learned that last month, then-acting general counsel of the IRS, Andew De Mello reportedly "refused to turn over the addresses of 7.3 million taxpayers sought by ICE" after

[20] Compl. ¶ 160, citing Rene Marsh and Marshall Cohen, *''Delete' is one of their favorite terms': Inside DOGE's IRS takeover ahead of tax season*, CNN (Mar. 15, 2025), https://perma.cc/8QNY-P6T9 ("the actions taken by DOGE inside IRS appear to be aimed at finding ways to use the agency's protected data to find undocumented immigrants.").

[21] Am. Compl. ¶ 150, citing Alexander Rifaat, *Musk's Team Enters IRS; Trump Vows Scrutiny of Improper Payments*, TaxNotes (Feb. 14, 2025), https://perma.cc/PG6S-QXNU ("This is why we're doing what we're doing"); Am. Compl. ¶ 72, citing Aimee Picchi, *Elon Musk's DOGE presence at the IRS raises concerns about taxpayer data security, refund delays*, CBS News (Feb. 17, 2025), https://perma.cc/D7TF-9CGK (Stephen Miller describing targeting child tax credit recipients).

[22] Compl. ¶ 160, citing Rene Marsh and Marshall Cohen, *''Delete' is one of their favorite terms': Inside DOGE's IRS takeover ahead of tax season*, CNN (Mar. 15, 2025), https://perma.cc/8QNY-P6T9.

identifying numerous legal deficiencies in the agency's request.[23] Two days later, he was forced out of his job.[24] Another former senior IRS official stated that demands for this amount of data, for these purposes, was "unprecedented" and amounted to "a big data dump."[25] Though a Memorandum of Understanding exists between the Department of Homeland Security ("DHS") and the IRS, and this request appears to have been made under this MOU, the agreement indicates that its purpose is limited to only seeking information regarding "aliens illegally present in the United States" who DHS represents are under final orders of removal *and* are under criminal investigation for violations of one or more Federal criminal statutes.[26] However, the Administration's own figures show that, as of late 2024, there were only around 1.45 million immigrants on ICE's non-detained docket with final orders of removal.[27] This data request appears to cover a significant majority of all undocumented immigrant taxpayers, who are estimated to number around 10.9 million in total.[28] Though statistics on the number of active investigations by ICE do not appear available, there is no evidence to find it plausible that one agency is conducting *bona fide* criminal investigations of 7.3 million people at once.

Available evidence indicates that such disclosures, as contemplated under the Data Policy, are unprecedented. For example, in 2023, the IRS reported no disclosures to the Department of

[23] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T.

[24] *Id.*; *see also* Am. Compl. ¶¶ 138, 162–167 (alleging and detailing pattern of IRS employees being forced out or leaving as the Data Sharing Policy was implemented).

[25] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE,* https://perma.cc/6XGQ-KX6T.

[26] Aravind Vodupalli, *The New ICE-IRS Data Sharing Agreement Has Three Problems*, Tax Pol'y Ctr. (Apr. 21, 2025), https://perma.cc/FY7J-VTL8 (citing IRS, Mem. of Understanding Between IRS and ICE, *available at* https://perma.cc/BHH8-ZQXM); Am. Compl. ¶ 171.

[27] Finding of Mass Influx of Aliens, 90 Fed. Reg. 13622 (Mar. 25, 2025).

[28] Carl Davis, et al., *Tax Payments by Undocumented Immigrants*, Inst. on Taxation and Econ. Pol'y (July 30, 2024), https://perma.cc/3N7E-3S48.

Homeland Security. It reported 75,647 disclosures to the Department of Justice, U.S. Attorneys, and other federal law enforcement agencies.[29] The year before, it reported 43,141 disclosures to those agencies, and no disclosures to the Department of Homeland Security.[30] Under the Data Policy, the contemplated disclosures from the IRS to ICE alone would result in a 9500% increase in a single year.[31]

The new plan to respond to ICE's request, "permissible" under the new Data Policy, will reportedly "give ICE automated access to home addresses en masse."[32] There would be little ability to evaluate the legality of such transfers, let alone to do so on a case-by-case basis. *See* Am. Comp. ¶¶ 184–187, 227 (alleging that the Data Policy does not allow for consideration of privacy, security, or legality of disclosures). Experts have expressed concerns, including the high likelihood for "dangerous mistakes."[33] These include returning the address of an unrelated person with the same name or similar address.[34] In addition, the IRS has no way to independently verify "that each targeted individual is the subject of a valid criminal investigation."[35] There is also no limitation on the amount of data or how often DHS can request it.[36] And given the system's automation, it is

[29] IRS, Joint Comm. on Taxation, *Disclosure Report For Public Inspection Pursuant To Internal Revenue Code Section 6103(P)(3)(C) For Calendar Year 2023 (JCX-14-24)*, Apr. 25, 2025, *available at* https://perma.cc/5A86-ZSJN.

[30] IRS, Joint Comm. on Taxation, *Disclosure Report For Public Inspection Pursuant To Internal Revenue Code Section 6103(p)(3)(C) For Calendar Year 2022 (JCX-6-23)*, Apr. 18, 2023, *available at* https://perma.cc/GM8S-R5KU.

[31] Comparing 75,647 disclosures to 7.3 million disclosures.

[32] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T; *see also* Am. Compl. ¶ 171.

[33] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T; *see also* Am. Compl. ¶¶ 184–187

[34] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T.

[35] *Id.*; Am. Compl. ¶¶ 184–187.

[36] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T.

ripe for unauthorized disclosures beyond those contemplated.[37] Said one engineer, "The system could easily be expanded to acquire all the information the IRS holds on taxpayers."[38] Another explained that "By shifting a single parameter, the program could return more information than just a target's address…including employer and familial relationships."[39] Reporting suggests that these disclosures, pursuant to the Data Policy, were set to begin as early as the end of July and thus may already be occurring.[40]

III. Plaintiffs Are Harmed by Defendants' New Data Policy.

Plaintiffs are a non-profit organization, a nationwide network of small businesses, and two labor unions seeking to protect themselves, their members, and the communities and clients they serve from Defendants' Data Policy. The non-profit Center for Taxpayer Rights ("the Center" or "CTR") asserts organizational standing on its own behalf and third-party standing on behalf of its clients. The network of small businesses, Main Street Alliance ("MSA"), and unions National Federation of Federal Employees ("NFFE") and Communications Workers of America ("CWA") assert associational standing on behalf of their members.

Plaintiff Center for Taxpayer Rights' ("the Center" or "CTR") mission is to advance taxpayer rights, promote trust in systems of taxation, and increase access to justice in the tax system. Am. Compl. ¶ 35. CTR works to achieve this mission in myriad ways, including with education and outreach services through its Low Income Tax Clinic ("LITC"), which provides direct services to clients in tax disputes with the IRS and state and local tax agencies. Am. Compl.

---

[37] *Id.*; Am. Compl. ¶¶ 184–187.

[38] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T; Am. Compl. ¶¶ 184–187.

[39] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T; Am. Compl. ¶¶ 184–187.

[40] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T.

¶¶ 35–42; Decl. of Nina E. Olson ("Olson Decl.") ¶ 3–4. CTR also operates LITC Connect, a network created and run to advise and support statutorily created member LITCs nationwide. Olson Decl. ¶ 5. The Data Policy has impaired CTR's ability to pursue these mission critical activities, requiring the allocation of additional resources to continue to provide LITC services required by the statute authorizing LITC funding. Olson Decl. ¶¶ 6–12. The Center's clients will also be harmed by the unlawful access and disclosure of their personal information, for potential use in criminal investigations unrelated to tax purposes. Am. Compl. ¶¶ 38–42, 194–96.

Plaintiff unions NFFE and CWA are national unions that have hundreds of thousands of public and private sector union members and employees whose sensitive information—including their Social Security or taxpayer identification numbers; names and addresses; taxable income; marital status; and information, such as medical expenses, relating to eligibility for tax deductions and credits—is held by the IRS. Am. Compl. ¶¶ 47–53. They each have members who are low–income workers eligible for the Earned Income Tax Credit ("EITC") and the Child Tax Credit ("CTC"). Am. Compl. ¶¶ 49–50, 53.

Plaintiff MSA also seeks to protect confidential, competitively sensitive information held by the IRS on itself and its members. It has members who are small businesses and small business owners include low–income sole proprietors eligible for the EITC, CTC, and other refundable credits. Am. Compl. ¶¶ 43–46, 201–03.

All Plaintiffs and their members have understood the information they submit to IRS to be private, barring a discrete list of specific exceptions. Am. Compl. ¶¶ 199, 206, 212.

And though the Data Policy puts at risk millions of individuals' and businesses' taxpayer information, the Administration has expressed clear intentions about which groups of people it intends to focus on, in its push to share, inspect, and cross-reference IRS data under the Data

Policy. MSA, NFFE, and CWA's low–income members are particularly likely to be members of the groups—low-income people who file for refundable credits and are eligible for public benefits—targeted by the Data Policy. CTR's clients who speak a language other than English or are low-income are, likewise, likely to be among the groups particularly targeted by the Data Policy. Am. Compl. ¶¶ 190–196; Olson Decl. ¶ 8.

LEGAL STANDARD

In deciding Defendants' motion to dismiss, under either Federal Rule of Civil Procedure 12(b)(1) or 12(b)(6), the Court must "treat the complaint's factual allegations as true . . . and must grant [P]laintiff the benefit of all inferences that can be derived from the facts alleged." *Sparrow v. United Air Lines, Inc*., 216 F.3d 1111, 1113 (D.C. Cir. 2000) (citation omitted); *see, e.g*., *Grell v. Trump*, 330 F. Supp. 3d 311, 315 (D.D.C. 2018).

At the pleading stage, standing arguments are evaluated under the motion to dismiss standard, *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 913 (D.C. Cir. 2015), and Plaintiffs are required only to state a "plausible claim" to standing, *Humane Soc'y of the U.S. v. Vilsack*, 797 F.3d 4, 8 (D.C. Cir. 2015), accepting as true the allegations of the Complaint and construing the allegations in favor of the Plaintiffs, *Warth v. Seldin*, 422 U.S. 490, 501 (1975).

To determine whether Plaintiffs have stated a claim, "detailed factual allegations" are not necessary, *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 555 (2007), but "a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face,'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009) (quoting *Twombly*, 550 U.S. at 570). Thus, the complaint's "[f]actual allegations must be enough to raise a right to relief above the speculative level," *Twombly*, 550 U.S. at 555, although Defendants' motion may be denied even if "recovery is very remote and unlikely," *id*. at 556.

ARGUMENT

The Data Policy represents a stark departure from prior taxpayer data protection requirements. Am. Compl. ¶¶ 168–188. It prioritizes sharing information in bulk, not on a case–by–case basis. *See, e.g., id*. ¶¶ 179–187.[41] It erases the bold lines limiting political interference in the tax system. *See, e.g., id.* ¶¶ 156, 174–178, 188.[42] It scraps the principle that any need for the disclosure of taxpayer information must clearly outweigh taxpayer privacy interests and concerns about the effect on voluntary tax compliance. *See, e.g., id.* ¶¶ 160, 169.[43] It reverses the IRS's commitment to housing taxpayer information in separate systems and granting access to such systems on an individual basis, instead prioritizing combining data and facilitating broad access to taxpayer information across systems. *See, e.g., id.* ¶¶ 161, 162, 168–188.[44] Since its implementation, the policy has been neither explained nor legally justified. *Id*. 183–84, 225–27.

Plaintiffs have standing to challenge the Data Policy as it imminently threatens concrete harms to their members and clients and to the Center itself, among whom are low-income people and immigrants most likely to have their data unlawfully shared and inspected. Courts in this Circuit have recognized that such unlawful inspection of sensitive information constitutes a harm sufficient to establish standing, and indeed this Court has recognized that principle in the context

---

[41] *See, e.g*., Am. Compl. ¶ 180, *citing* Kelly, *Palantir Is Helping DOGE With a Massive IRS Data Project*, https://perma.cc/AF3S-6QP7 (explaining that an API enabled by the Data Sharing Policy would mean "anyone with access could view and have the ability to possibly alter all IRS data in one place").

[42] *See also* Am. Compl. ¶ 144, *citing* Hunter Walker, *Inside The 'Bizarre' Meeting Where DOGE Requested 'Extensive System Access' At IRS*, Talking Points Memo (Feb. 14, 2025), https://perma.cc/KP6B-D6ZY (DOGE is "just trying to snap up data right now.")

[43] *See also* Am. Comp. ¶ 161, citing Kelly, *Palantir Is Helping DOGE With a Massive IRS Data Project*, https://perma.cc/AF3S-6QP7 ("It's basically an open door controlled by Musk for All Americans' most sensitive information with none of the rules that normally secure that data").

[44] *See also* Am. Comp. ¶ 161, citing Kelly, *Palantir Is Helping DOGE With a Massive IRS Data Project*, https://perma.cc/AF3S-6QP7 ("The cloud platform could be come the 'read center of all IRS systems,'" and "anyone with access could view and possibly manipulate all IRS data in one place").

of other DOGE-directed disclosures of protected information. *See Alliance for Retired Americans v. Bessent*, 770 F. Supp. 3d 79, 102 (D.D.C. 2025). Further, the limited damages provisions of the Internal Revenue Code and Privacy Act do not offer an adequate remedy to address the broad, cascading sharing of sensitive taxpayer information sufficient to overcome the APA's strong presumption of reviewability. *See Garcia v. Vilsack*, 563 F.3d 519, 523 (D.C. Cir. 2009). Finally, as a court in this district has recognized in the context of an *ultra vires* challenge to DOGE action, *ultra vires* review is available when an entity like DOGE is "operating without any legal authority whatsoever," not solely when an executive entity exceeds specific statutory limitations. *AFL-CIO v. Dep't of Lab.*, No. 1:25-cv-00339, 2025 WL 1129227, at *22 (D.D.C. Apr. 16, 2025).

I. Plaintiffs Have Standing to Challenge Defendants' Data Policy.

The Plaintiff organizations have standing to challenge the Data Policy and seek to set aside conduct that poses an imminent threat to the privacy of their members' and clients' confidential tax return information, under associational, organizational, and third-party standing.

A. Plaintiffs MSA, NFFE, and CWA Have Adequately Alleged Associational Standing.

To demonstrate associational standing, a plaintiff must establish that "(1) its members would otherwise have standing to sue in their own right; (2) the interests it seeks to protect are germane to the organization's purpose; and (3) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Ctr. for Sustainable Econ. v. Jewell*, 779 F.3d 588, 596 (D.C. Cir. 2015) (quoting *Hunt v. Wash. State Apple Adver. Comm'n*, 432 U.S. 333, 343 (1977) (internal quotation marks omitted); *Travelers United, Inc. v. Hyatt Hotels Corp.*, 761 F. Supp. 3d 97, 112 (D.D.C. 2025). Defendants have only contested the first element

of associational standing, arguing that Plaintiffs' members lack standing to challenge the Data Policy.[45]

Plaintiffs MSA, NFFE, and CWA have alleged "concrete and particularized injury to their members to be . . . sufficiently 'imminent' for standing purposes." *Attias v. Carefirst, Inc.*, 865 F.3d 620, 627 (D.C. Cir. 2017) (citations omitted). Defendants' arguments to the contrary focus on two points: first, that Plaintiffs have alleged no improper sharing or use of their members' data has occurred, Defendants' Motion to Dismiss ("Mot.") at 14, and second, that unlawful access to or sharing of data does not constitute an injury-in-fact under Article III of the Constitution, Mot. at 8–14.

However, Plaintiffs' claims do not depend upon a showing that Defendants have already violated the Internal Revenue Code's privacy protections or the Privacy Act. Rather, Plaintiffs allege that the Data Policy creates a substantial increased risk of injury, including violations of statutorily granted privacy rights.[46] Where, as here, parties allege standing on the basis of an increased risk of harm, the D.C. Circuit has explained that courts should "consider the ultimate alleged harm ... as the concrete and particularized injury and then [ ] determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for

[45] Defendants correctly did not dispute that the other two elements of associational standing are satisfied. The privacy interests of the membership organization Plaintiffs—which advocate on behalf of small businesses (MSA) and on behalf of workers (NFFE and CWA)—are germane to their missions. *See* Am. Compl. ¶¶ 44, 47, 51. And there is no reason that Plaintiffs' members need to participate directly in this case rather than allow their associations to advocate on their behalf.

[46] Although Plaintiffs allege that these injuries are imminent, it is distinctly possible that they are already occurring, but the sharing of Plaintiffs' members data is shrouded in secrecy as a result of the generally opaque approach Defendants have taken to the Data Policy. *See, e.g.,* William Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, ProPublica (July 15, 2025), https://perma.cc/6XGQ-KX6T ("The plan has been shrouded in secrecy even within the IRS, with details of its development withheld from regular communications. Several IRS engineers and lawyers have avoided working on the project out of concerns about personal legal risk.").

standing purposes.'" *Food & Water Watch*, 808 F.3d at 915. Plaintiffs satisfy both requirements here, alleging an ultimate harm that courts have recognized as sufficient for standing with allegations that this harm—based on Defendants' concrete steps to share data at an enormous scale likely to include the data of Plaintiffs' members—is imminent.

1. Plaintiffs Allege Concrete and Particularized Injury Analogous to Those Recognized by Common Law Torts.

The injury to their members that Plaintiffs allege an increased risk of here—unlawful inspection or disclosure of confidential tax return information under the Data Policy, in violation of the Internal Revenue Code at 26 U.S.C. § 6103 and 26 U.S.C. § 7213A and the Privacy Act—is sufficiently concrete and particularized to satisfy Article III's requirements. Each of these statutes requires that Plaintiffs' members' information be kept confidential, with strict exceptions for sharing that data even within the federal government. *See supra* Background A.1. Any violation of these statutory rights to confidentiality is an injury akin to long recognized injuries sufficient to confer standing. Injuries are concrete when they have "a close historical or common-law analogue." *TransUnion LLC v. Ramirez*, 594 U.S. 413, 424 (2021). Here, there are two common–law torts that recognize the harm of improper access and sharing of protected information: intrusion upon seclusion and breach of confidence.

First, as this Court recently ruled in *Alliance for Retired Americans v. Bessent*, unlawful disclosure of tax return data in violation of Section 6103 "has a close relationship to the harm to privacy vindicated by the common-law tort of intrusion upon seclusion." 770 F. Supp. 3d at 102; *see also TransUnion*, 594 U.S. at 425 (recognizing "intrusion upon seclusion" as a concrete harm). Contrary to Defendants' arguments, this tort does not require intrusion into a physical space or unwanted communications. Mot. at 10–12. Examination or inspection of sensitive non-public information is itself an injury. For example, examination of a plaintiff's private bank account was

among the types of privacy invasion that constituted an intrusion upon seclusion, along with other non-physical invasions of privacy like opening personal mail or eavesdropping on private conversations. *See Wolf v. Regardie*, 553 A.2d 1213, 1217–18 (D.C. 1989) (collecting cases); *see also* Restatement (Second) of Torts § 652B (1977) (defining tort as when one "intentionally intrudes, physically *or otherwise*, upon the solitude or seclusion of another or his private affairs") (emphasis added). Here, Plaintiffs have alleged that Defendants' Data Policy greatly expands access to their members' data through new permissive sharing within IRS and permitting broader sharing with other agencies. *See supra* Background A.2; Am. Compl. ¶¶ 145–46, 150–151, 155–160, 160–166. This allows for inspection and examination of sensitive personal information Plaintiffs' members have submitted with the understanding it would be protected and private, permitting examination of private affairs squarely in line with cases finding such non-physical invasions constituted intrusion upon seclusion. *Id.* ¶¶ 199, 206, 212. The tort of intrusion upon seclusion does not require that this private information be "*use*[d]" for a particular purpose to show a traditionally recognized harm, as Defendants seem to contend, Mot. at 10 (emphasis in original), and Plaintiffs do not need to show such "use" here to show injury akin to that traditionally recognized by this tort.

And Defendants' argument—relying primarily on a pair of concurrences to the Fourth Circuit's ruling on a motion, in *Am. Fed'n of Teachers v. Bessent*, No. 25-1282, 2025 WL 1023638 (4th Cir. Apr. 7, 2025)—ignores the fact that even if the common law tort might not have protected Plaintiffs' members against this type of conduct, Congress has created "a new sphere in which individuals not only expect privacy, but have a right to it—i.e., a sphere of seclusion. As a result, an intrusion upon that sphere—even if the sphere literally encompasses only one row of millions in a dataset—amounts to an injury similar to the intrusion upon other private spheres, such as one's

home." *AFL-CIO v. DOL*, 2025 WL 1129227, at *8; *see also New Mexico v. Musk*, No. 1:25-cv-00429, 2025 WL 1502747, at *8 (D.D.C. May 27, 2025) (finding unauthorized access to states' private and proprietary information sufficient to allege an injury in fact, at the motion to dismiss stage, and analogous to the tort of intrusion upon seclusion).[47]

Additionally, this tort—in contrast to the tort of defamation, relied upon in *TransUnion*—does not require publication of the information obtained, *Wolf*, 553 A.2d at 1217, making it irrelevant whether there is subsequent disclosure or publication of the unlawfully disclosed data, Mot. at 10, or whether plaintiffs themselves know that a disclosure has taken place, Mot. at 13. *See Dalley v. Dykema Gossett*, 287 Mich. App. 296, 314, 788 N.W.2d 679, 691 (2010) ("irrespective of whether defendants ever viewed the copied information . . . [plaintiff] adequately pleaded an invasion of plaintiff's seclusion.").

Second, unlawful disclosure of information that taxpayers provided to the IRS, in reliance on the legal protections for its confidentiality, is analogous to the common–law tort of breach of confidence. *See Jeffries v. Volume Servs. Am., Inc.*, 928 F.3d 1059, 1064 (D.C. Cir. 2019). In *Jeffries*, the D.C. Circuit considered a case against a merchant that violated a statutory requirement to truncate a customer's credit card number on a receipt. And even though there was no evidence the credit card number had actually been disclosed to a third party, the court held that this statutory violation was sufficiently analogous to the tort of breach of confidence because the statutory requirement had been designed to protect against the same kind of harms that the tort makes actionable. *Id*. The Court in *AFL-CIO* similarly found that DOGE Affiliates access to plaintiffs'

[47] Similarly, Defendants citation to the Supreme Court's stay in *Social Security Admin. v. Am. Fed'n of State, Cnty. & Mun. Emps*., 145 S. Ct. 1626 (Mem.) (2025), does not provide relevant authority here. Mot. at 12 n.1. The Supreme Court did not provide reasoning for its stay, and it came in the context of a preliminary injunction.

members' data there was sufficient to show an injury akin to breach of confidence, where [n]othing beyond 'the plaintiff's trust in the breaching party [being] violated' must occur for the harm to be actionable." 2025 WL 1129227, at *8 (quoting *Jeffries*, 928 F.3d at 1064). Likewise here, Sections 6103 and 7213A of the Internal Revenue Code and the Privacy Act's protections vest taxpayers with a concrete interest in submitting information to the IRS in connection with their tax returns without incurring a risk that this information will be shared with other government agencies, for purposes having nothing to do with tax administration, other than within the narrow legally permissible exceptions. Where the IRS discloses a taxpayer's information in violation of these statutory provisions, it causes a concrete injury akin to the common-law tort of breach of confidence. Plaintiffs have, therefore, alleged an increased risk of an injury that is both concrete and particularized to its members.

2. Plaintiffs' have Adequately Alleged that the Injury to their Members' is Imminent.

Plaintiffs have also alleged that the privacy injuries discussed above are imminent, sufficient to satisfy the legal standard at the Motion to Dismiss stage of the case. *Attias*, 865 F.3d at 627. As alleged in the Complaint, at least some IRS data is reportedly already available in a "data lake" (i.e., repository) at the U.S. Citizenship and Immigration Services ("USCIS") to which DOGE personnel have access. Am. Compl. ¶¶ 172–178. IRS has imminent plans to expand the scope of its data–sharing to other agencies. *Id*. ¶ 225. And IRS has taken concrete steps to implement its policy shift towards large–scale information sharing: tasking Palantir with construction of a "mega API" to facilitate data transfers at scale through an interconnected technological platform, *id*. ¶¶ 180–185, and to develop a system for quick, template agreements to enable cross-agency sharing, *id*. ¶ 187. As Plaintiffs also allege, the Administration plans to target certain vulnerable groups for this data-sharing—immigrants targeted for removal, Am. Compl. ¶¶

171–173, and lower-income taxpayers who receive particular tax credits, like the Earned Income Tax Credit ("EITC") and participate in public benefits programs like the Supplemental Nutrition Assistance Program ("SNAP") and student loan and aid programs. Am. Compl. ¶ 170. NFFE and CWA's low–income members are particularly likely to be members of these targeted groups. Am. Compl. ¶¶ 46, 49–50, 53.

Since the Amended Complaint was filed, further public reporting has emerged consistent with these allegations and demonstrating the imminence of harm caused by mass data sharing: the June 2025 request from ICE for the home addresses of 7.3 million taxpayers, to which—as described in the Background, *supra*—IRS now appears to be preparing to respond. Although the IRS General Counsel reportedly initially refused the request, he has been forced out, and the IRS is reportedly standing up a process to allow ICE officials to request "enormous swaths of confidential data in bulk through an automated, computerized process,"[48] rather than through the careful process previously used at IRS to ensure that the requirements of a relevant exception under Section 6103 are satisfied before any data is shared. Am. Compl. ¶ 93. Although this consequence of the Data Policy occurred after the Amended Complaint was filed, "[i]n determining standing," the court may also "consider materials outside of the complaint." *Food & Water Watch*, 808 F.3d at 913.

This effort to share data with ICE is just one example of information–sharing with a single agency, targeting one particular vulnerable population. The Administration has also articulated its intention to cross–reference and "reconcile" databases at different agencies for the purpose of "eliminat[ing] the waste and fraud," like data on SNAP recipients. *Supra* Background II.; Am.

[48] Turton, et al., *The IRS Is Building a Vast System to Share Millions of Taxpayers' Data With ICE*, https://perma.cc/6XGQ-KX6T.

Compl. ¶¶ 110, 113. This is another concrete step towards the imminent, large–scale disclosure or inspection of taxpayer data that Plaintiffs have alleged under the Data Policy.

Given the scale of the forthcoming information sharing alleged in the Amended Complaint and the concrete steps the IRS is already taking to implement this policy shift, the risk to Plaintiffs' members and clients is concrete and imminent. This case is not, contrary to Defendants' assertion, like *Clapper*. Mot. at 8–9. There, plaintiffs contended that the government policy would target "*other individuals*" and "an attenuated chain of possibilities" would lead to plaintiffs' injuries. *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 411 (2013) (emphasis in original). Here, Plaintiffs have alleged that groups that include their members will be targeted and that the Data Policy will result in sharing at enormous scale that will inevitably harm them. This fact pattern is instead comparable to the one the D.C. Circuit addressed in *Sierra Club v. Jewell*, where the court held the plaintiffs had standing based on the "'substantial probability' of injury" reflected in the undisputed facts. 764 F.3d 1, 7 (D.C. Cir. 2014). Although mining operations had not yet commenced on the protected historic battlefield, in that case, the court looked to the mining companies' statements of their intentions (to mine the area of the battlefield, under their existing permits) and their concrete actions in furtherance of those intentions (proceeding with mining activities up to approximately 800–1,200 meters away from the battlefield) to conclude that the plaintiffs' alleged injury was imminent. *Id*. at 7–8. Similarly here, the Administration repeatedly has stated its intentions to share data broadly across the government, including from the IRS, and has taken actual, concrete steps—including building the necessary computer network infrastructure—to carry out those intentions.

The manner in which DOGE personnel—including those embedded at the IRS—have handled personal data also demonstrates another imminent risk posed by the Data Policy. DOGE

team members across the government have sought to gather up as much data as possible, with little regard for legal protections related to restrictions on use of date or inter-agency data sharing, since the beginning of the Administration, emailing and disclosing classified and personal information. *Supra* Background A.2; Am. Compl. ¶¶ 107–114. At the IRS, DOGE team members demanded access to systems, without apparent authority to do so and before appropriate background checks, and pushed out dozens of senior leaders who raised concerns about their plans. *Supra* Background 2.A; Am. Compl. ¶ 156–162. Another court found that the risk of unlawful exposure of data from Treasury resulting from the "rushed and ad hoc process that has been employed to date by the Treasury DOGE Team" was imminent and substantial, and their speed in directing the reversal of decades-long privacy policy at IRS shows similar imminence. *New York v. Trump*, 767 F. Supp. 3d 44, 68 (S.D.N.Y. 2025); *see also Am. Fed'n of Gov't Emps., AFL-CIO v. U.S. Off. of Pers. Mgmt.*, 777 F. Supp. 3d 253, 270 (S.D.N.Y. 2025) (holding that allegations of sweeping and uncontrolled access being provided to inadequately vetted and trained DOGE personnel "amply plead the existence of risk necessary to support a finding of standing").

Under these facts, the risk Plaintiffs allege is sufficiently concrete and imminent to support Article III standing.

B. CTR has adequately alleged both Organizational and Third-Party Standing.

Plaintiff CTR asserts organizational standing on its own behalf and third-party standing on behalf of its LITC clients.

To adequately allege organizational standing, CTR's allegations must make plausible that it has suffered an "'actual or threatened injury in fact that is fairly traceable to the defendants' allegedly unlawful conduct and likely to be redressed by a favorable court decision.'" *Am. Anti-Vivisection Soc'y v. USDA.*, 946 F.3d 615, 618 (D.C. Cir. 2020). As to injury its allegations must

make plausible that "first, …. the agency's action or omission to act 'injured the [organization's] interest' and, second, … the organization 'used its resources to counteract that harm.'" *PETA v. USDA*, 797 F.3d 1087, 1094 (D.C. Cir. 2015) (quoting *Equal Rts. Ctr. v. Post Props., Inc.*, 633 F.3d 1136, 1140 (D.C. Cir. 2011)). Sufficient injury can be found when an organization's "ability" to provide "services" or conduct "core business activities" is "perceptibility impaired" by agency action. *Food & Drug Admin. v. All. for Hippocratic Med.*, 602 U.S. 367, 395 (2024).

To assert the rights of others, under the doctrine of third-party standing: "(1) [t]he litigant must have suffered an injury in fact, thus giving him or her a sufficiently concrete interest in the outcome of the issue in dispute, (2) the litigant must have a close relation to the third party, and (3) there must exist some hindrance to the third party's ability to protect his or her own interests." *Wilmer Cutler Pickering Hale & Dorr LLP v. Exec. Off. of President*, No. 1:25-cv-00917, 2025 WL 1502329, at *9 (D.D.C. May 27, 2025) (internal quotations omitted). Though third-party standing frequently arises in the context of Constitutional claims, it is not limited to this context. *See Penn. Psychiatric Soc. v. Green Spring Health Servs., Inc.*, 280 F.3d 278, 291 (3d Cir. 2002).

First, CTR's allegations make plausible that the new Data Policy injured its organizational interests sufficient to confer standing in its own right. Plaintiff CTR has already had its mission and statutorily required education functions harmed. Olson Decl. ¶¶ 8, 10–12.[49] As a result of the new Data Policy CTR and its LITC have been forced to expend additional resources to reach vulnerable taxpayers, provide legal services, and facilitate trust in the taxpayer system. Am. Compl. ¶¶ 190, 192; Olson Decl. ¶¶ 11–12. Specifically, as a recipient of federal funding, the LITC is required by statute to identify and advocate for issues impacting low-income taxpayers, and

[49] "In determining standing," the court may also "consider materials outside of the complaint." *Food & Water Watch*, 808 F.3d at 913.

specifically to inform individuals for whom English is a second language about their rights and responsibilities under the Internal Revenue Code. Olson Decl. ¶ 7 (discussing LITC requirements under 26 U.S.C. § 7526 (b)(1)(A)(ii)(II)). CTR's education and outreach efforts include these non-English speaking taxpayers who are more likely to be immigrants. Olson Decl. ¶ 8.[50] CTR also serves populations like domestic violence survivors who are especially concerned about the security of personal information and interact with the IRS in connection with the EITC and/or CTC payment issues. Olson Decl. ¶ 8. Following recent public reporting on the IRS's Data Policy, CTR has found that these vulnerable groups of taxpayers—including those the LITC is statutorily charged to protect and advocate for—have become less willing to attend Center events, seek its guidance, or engage with its education and outreach. Olson Decl. ¶ 8–10. Accordingly, the Center has been forced to increase staffing in order to pursue these mission critical services, at significant expense to the organization. Olson Decl. ¶ 11–12. These expenses, concretely reflected in its recent LITC grant application, are significant, totaling nearly 10 percent of CTR's LITC operating expenses. *Id*. CTR has also needed to dedicate more time and resources to efforts to support and advise its nationwide member network of LITCs, LITC Connect, as its LITC members' interests have been similarly injured by the Data Policy. Olson Decl. ¶ 9.

These are not merely setbacks to CTR's abstract social interests, as Defendants argue. CTR, through its LITC, counsels clients regarding their tax obligations and interactions with the IRS and provides resources supporting other low-income tax clinics that do the same, and its work is being made substantially more difficult by the IRS's actions. *See id*. ¶ 8, 11–12; Am. Compl. ¶¶ 35–42, 194–95. Under similar facts, in *Havens Realty Corp. v. Coleman*, the Supreme Court held

[50] The Internal Revenue Code's protections apply to all "taxpayer[s]," without regard for immigrant or citizenship status. 26 U.S.C. § 6103(b)(6).

standing was appropriate for an organization that provided counseling and referral services to homeseekers because it was "perceptibly impaired" in its provision of those services due to the defendants' alleged actions. 455 U.S. 363, 379 (1982); *see also League of United Latin Am. Citizens v. Exec. Off. of the President*, No. 1:25-cv-00946, 2025 WL 1187730, at *31–32 (D.D.C. Apr. 24, 2025) (Kollar-Kotelly, C.) (finding organizational standing where voter identification requirements would impede effectiveness of organization's voter registration efforts and force additional investment of resources to achieve its mission). Here, as in those cases, the Center is being forced to adjust its operations and expend more of its limited resources to accomplish a core component of its mission, which is a concrete injury. As the Supreme Court recognized in *Alliance for Hippocratic Medicine*, the fact that the Center's "ability" to provide its counseling services—which here are core to the Center's mission and reflected in the statute authorizing funding for LITCs—has been "perceptibly impaired" demonstrates that the Center has established an injury sufficient for standing under *Havens*. 602 U.S. at 395. For purposes of organizational standing, the inquiry ends here; Plaintiff CTR has alleged injury sufficient to demonstrate standing at the Motion to Dismiss stage.

CTR's allegations also meet the standard for asserting standing on behalf of its LITC clients, through the third-party standing doctrine, because (1) it has a close relationship with its clients, who have standing to sue, and (2) these clients face obstacles to protecting their own interests. *See Kowalski v. Tesmer*, 543 U.S. 125, 130 (2004). First, the attorney-client relationship between CTR's LITC and its clients allows CTR to advocate for their clients' interests, Am. Compl. ¶ 38, which is precisely the type of relationship the Supreme Court has recognized as being sufficient to support third-party standing. *See Caplin & Drysdale, Chartered v. United States*, 491 U.S. 617, 624 n.3 (1989). Although *Kowalski* found no standing because the attorneys there did

not yet have the clients they purported to sue on behalf of, here the Center already represents clients who face imminent injury from the Data Policy. The Center's immigrant and low-income clients, Am. Compl. ¶¶ 40–42, are among those most likely to be targeted by the Data Policy and face imminent injury through unlawful sharing and disclosure of their data, *see* Background I.A & II.

And second, CTR's LITC clients face obstacles to asserting their own interests, given that many of them are involved in disputes with the IRS and fear retribution, Am. Compl. ¶ 38, others lack the resources to protect their privacy interests and fear reputational harm, *id.*, and some are immigrants who fear providing sensitive personal information to the government will lead to harm, *id*. ¶ 42, a not-unreasonable fear under an Administration that is carrying out an extreme immigration agenda and frequently forgoing required legal process in doing so.[51] This prong of the analysis "does not require an absolute bar from suit, but some hindrance to the third party's ability to protect his or her own interests." *S. Poverty L. Ctr. v. U.S. Dep't of Homeland Sec.*, No. 1:18-cv-00760, 2020 WL 3265533, at *14 (D.D.C. June 17, 2020) (internal quotations omitted).

The obstacles CTR's LITC clients face here are comparable to those the Supreme Court considered in *Secretary of State of Md. V. Joseph H. Munson Co.*, where the Court was concerned that "[e]ven where a First Amendment challenge could be brought by one actually engaged in protected activity, there is a possibility that, rather than risk punishment for his conduct in challenging the statute, he will refrain from engaging further in the protected activity," thus leaving the law unchallenged and the whole of society made worse off. 467 U.S. 947, 956 (1984).

Similarly, in *Southern Poverty Law Center*, this Court found that a legal services organization had third-party standing to assert the rights of its incarcerated clients based on the

[51] *See generally* Memorandum Opinion, *J.G.G. v. Trump,* 1:25-cv-00766 (D.D.C. Apr. 16, 2025), ECF No. 81, *available at* https://perma.cc/GDY2-XWZ2.

hinderance caused by, among other things, chilling effects, privacy concerns, and the clients' limited resources and capacity for participating in litigation, including limited English proficiency. 2020 WL 3265533, at *14. CTR's immigrant clients face particularly imminent risks of privacy-related harm in light of the reported steps Defendants have taken under the Data Policy, with at least some IRS data already having been uploaded to a "data lake" at USCIS and the imminent sharing of more than 7 million ITIN holders' information. *Supra* Background B; Am. Compl. ¶¶ 171–174. Here, as in that case, the individuals most vulnerable to unlawful data sharing by the IRS are also in the worst position to safely advocate on their own behalf. Through third-party standing, CTR can and should be permitted to exercise their rights on their behalf.

II. Plaintiffs Can Challenge Treasury-IRS Defendants' Data Policy Under the APA.

Contrary to Defendants' arguments, the limited remedies available under the Privacy Act and Internal Revenue Code are not an adequate alternative to relief under the APA for plaintiffs that need equitable relief from systemic policy changes by defendant agencies. Courts in this circuit have repeatedly rejected the argument that APA review is precluded even in cases that presented closer calls than this one. *See Doe v. Stephens*, 851 F.2d 1457, 1460–61, 1463 (D.C. Cir. 1988).

Plaintiffs can challenge an action that is arbitrary, capricious, or otherwise unlawful under the APA unless another law provides an "adequate remedy at court." 5 U.S.C. § 704. In assessing whether such an alternative "adequate remedy" exists, there is a strong presumption that agency actions are reviewable under the APA. *Abbott Lab'ys v. Gardner*, 387 U.S. 136, 140 (1967). Courts should only restrict access to APA review if there is "clear and convincing evidence" that Congress intended to bar it. *Garcia v. Vilsack*, 563 F.3d 519, 523 (D.C. Cir. 2009) (citing *Abbott Lab'ys*, 387 U.S. at 141). The Supreme Court has said, further, that courts can set aside federal agency

action that is 'not in accordance with law'—which means, of course, *any law*," so violations of the Privacy Act or Internal Revenue Code are subject to APA review. *F.C.C. v. NextWave Personal Comms, Inc*., 537 U.S. 293, 300 (2003) (citing 5 U.S.C. § 706(2)(A)) (emphasis in original).

The Data Policy violates the protections of the Internal Revenue Code and the Privacy Act and that violation is subject to APA review. Those laws create stringent protections that limit the sharing of sensitive personal data, including taxpayer information, even within the federal government. *See* 26 U.S.C. § 6103; 5 U.S.C. § 552a(b–e). The statutes both contain limited provisions for individuals to bring suit for damages for particular unlawful disclosures. 26 U.S.C. § 7431; 5 U.S.C. § 552a(g)(4). As this court has recognized, these provisions are similar, including for the purpose of determining whether an "adequate remedy" exists such that APA review is precluded. *All. for Retired Americans*, 770 F. Supp. 3d at 106. The Privacy Act contains limited provisions for prospective relief related to the correction of inaccurate records or production of records that are unrelated to unlawful disclosure. 5 U.S.C. § 552a(g)(2, 3). These circumscribed provisions cannot plausibly provide an "adequate remedy" to an agency *policy* to unlawfully share en masse the sensitive data of Plaintiffs' members and clients. *See* Am. Compl. ¶¶ 9, 168–188. Such a broad and intentional disclosure policy as the Data Policy is here is not at all analogous to a single employee viewing a taxpayer's records without authorization and a consequent discrete, backward-looking damages action.

Analogously, in *Doe v. Stephens*, the D.C. Circuit concluded that equitable relief under the APA was available for an agency's unlawful disclosure of medical records in violation of the Privacy Act. 851 F.2d at 1460–61, 1463. Even though the "Privacy Act [did] not by itself authorize the injunctive relief sought by Doe," the Court explained that such relief nevertheless *was* available under the APA, because Doe's "clearly [was] a case of agency action 'not in accordance with law'

within the meaning of 5 U.S.C. 706(2) . . . [where] the disclosure of Doe's psychiatric records violated the Veterans' Records Statute, as amended by the Privacy Act." *Id.* at 1463, 1466. As is true here, *Doe* involved a VA disclosure *policy* that violated the Privacy Act. *Id*.

And in *Radack v. U.S. Department of Justice*, another Court in this district explicitly held that the Privacy Act does not provide an adequate remedy for plaintiffs who seek declaratory and injunctive relief, and that the APA is the source for equitable relief to such plaintiffs. 402 F. Supp. 2d 99, 104 (D.D.C. 2005). The court also noted that APA review was particularly appropriate because the plaintiff alleged a "violation of [an agency's] own internal policies" with respect to disclosures subject to the Privacy Act. *Id.* The Court reached this conclusion even though there had only been an unlawful disclosure as to a single person and that disclosure was not ongoing. *Id*. The inadequacy of the Privacy Act's remedies, and the similar Internal Revenue Code remedies, are even more apparent here where Plaintiffs challenge a sweeping, ongoing policy of continuous data sharing across the federal government.

Recently, in *AFL-CIO v. Department of Labor*, Judge Bates affirmed these precedents and the principle that the Privacy Act's limited damages provisions—which are similar to the Internal Revenue Code's provisions—do *not* preclude APA review because they do not offer an adequate remedy for plaintiffs' challenging policies. 2025 WL 1129227, at *16. The decision noted that the Supreme Court had repeatedly indicated that the Privacy Act's remedy provisions were *not* intended to be exclusive and comprehensive. *Id.* at *15 (citing *Doe v. Chao*, 540 U.S. 614, 619 n.1 (2004) (the Privacy Act's "inattention" to equitable relief may be "explained by the general provision for equitable relief within the . . . . APA.")). Noting this Court's recent discussion in *Alliance for Retired Americans*, 770 F. Supp. 3d at 105, the *AFL-CIO* court explained that the Supreme Court's finding that the Privacy Act was "complementary" to the Fair Credit Reporting

Act indicated it did *not* provide a "comprehensive and 'exclusive' remedial scheme" that would displace APA review. 2025 WL 1129227, at *15 (citing *Dep't Agric. Rural Dev. Rural Housing Serv. v. Kirtz*, 601 U.S. 42, 63 (2024)); *compare* with Mot. at 18 (arguing Internal Revenue Code and Privacy Act provide "comprehensive" remedial schemes).

The Internal Revenue Code and Privacy Act's limited damages provisions do not provide an adequate alternative remedy in the place of APA review for challenges, like Plaintiffs' here, to agency policies that seek equitable relief. Not one of the cases cited by Defendants stands for the proposition that the remedies within the Privacy Act or the Internal Revenue Code foreclose relief under the APA. In relying on *Wilson v. Libby*, Defendants point to a case where the court found a *Bivens* action was precluded because the Privacy Act already focused on penalizing federal officials who willfully disclose records in violation of the Act. 535 F.3d 697, 705 (D.C. Cir. 2008). That decision focused on the penalties for the defendants and *Bivens*—not relief for the plaintiffs and the APA—and thus is not relevant to this case. *Id.* And while recognizing *Bivens* causes of action is "a disfavored judicial activity," *Egbert v. Boule*, 596 U.S. 482, 491 (2022), there is a strong presumption of reviewability under the APA, *see Abbott Lab'ys*, 387 U.S. at 140. Similarly, in *Block v. Community Nutrition Institute* the Supreme Court found that Congress, in drafting the statute at issue—*not* the Privacy Act or Internal Revenue Code—"intended to preclude consumer challenges to the Secretary's market orders." *Block v. Cmty. Nutrition Inst*., 467 U.S. 340, 352 (1984). The Court pointed to significant legislative history to support its factual determination. But Defendants can point to no such history with respect to the Privacy Act or the Internal Revenue Code Sec. 6103.[52]

[52] Defendants cite three additional out-of-circuit cases, none of which concern the Privacy Act or Internal Revenue Code. *See* Mot. at 18–19 (citing *Dew v. United States,* 192 F.3d 366, 372 (2d

III. The DOGE Defendants' Direction of An Unprecedented Policy for Sharing Protected IRS Data is *Ultra Vires* and Subject to Challenge.

An *ultra vires* claim seeks non-statutory 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). An action is *ultra vires* when it is "plainly beyond the bounds" of lawful authority. *Fed. Express Corp. v. Dep't of Com.*, 39 F.4th 756, 764 (D.C. Cir. 2022). And in some cases *ultra vires* review is available because officers or agencies "have acted *without* statutory authority" such that they are not acting within any recognized "jurisdiction." *Physicians Nat. House Staff Ass'n v. Fanning*, 642 F.2d 492, 496 (D.C. Cir. 1980) (citing *Leedom v. Kyne*, 358 U.S. 184, 188 (1958) (emphasis added)).

The DOGE Defendants—a network of components and individuals in the Executive Office of the President and affiliated agencies and individuals across many agencies of the executive branch—here lack any statutory authority at all to act. *See* Am. Compl. ¶¶ 221–223. Plaintiffs have alleged that they have nonetheless effected a change in IRS data sharing practices to facilitate large-scale transfers and create centralized mechanisms for accessing protected information across the federal government. Am. Compl. ¶¶ 217–219. Defendants have not pointed to any purported statutory authority empowering DOGE in their motion to dismiss. *See* Mot. at 16–19. Instead, Defendants argue that *ultra vires* review is inapplicable here because Plaintiffs have not pled "a specific statutory bound that Defendants have allegedly exceeded." Mot. at 16–17. But to support this claim, Defendants cite to inapposite cases where courts have considered whether *agency* defendants had acted "'in excess of [their] delegated powers and contrary to a *specific prohibition*'

Cir. 1999); *Rimmer v. Holder*, 700 F.3d 246, 261–62 (6th Cir. 2012); *Jones v. U.S. Dep't of Hous. & Urban Dev.*, No. 11-cv-0846, 2012 WL 1940845, at *6 (E.D.N.Y. May 29, 2012)).

in a statute." *Id*. at 18 (emphasis in original). Those precedents simply don't apply here, where the DOGE Defendants lack any statutory authority at all.

As another Court in this district has recently explained, and as D.C. Circuit has repeatedly recognized, *ultra vires* review is also available when the executive—here the DOGE Defendants—are "operating without any legal authority whatsoever." *AFL-CIO*, 2025 WL 1129227, at *22; *see also Physicians Nat. House Staff Ass'n*, 642 F.2d at 496 (Defendant "acted without statutory authority"). The Court in *AFL-CIO*, also considering claims that DOGE acted without authority, found that the government's nearly identical argument that "a specific statutory bound" must be identified was "barking up the wrong tree." *AFL-CIO*, 2025 WL 1129227, at *22. And even the authority Defendants rely on, in *Fed. Express Corp.*, 39 F.4th at 764, Mot. at 17, recognizes that *ultra vires* review is available not only when an agency has acted "clearly in defiance" of statutory authority, but also when the executive has "stepped so plainly beyond the bounds" of that authority.

Contrary to Defendants' suggestion, Mot. at 16, the Supreme Court's recent decision in *Nuclear Regulatory Commission v. Texas*, did not alter this standard. It affirmed—in the context of a challenge to an *agency*'s actions where the relevant agency had relevant existing statutory authority—the Court's holding in *Leedom v. Kyne*. *NRC v. Texas*, 145 S. Ct. 1762, 1776 (2025) (citing *Kyne*, 358 U.S. at 184). In discussing the facts before it, the Court considered whether "an agency" acted "contrary to a specific prohibition," but the entity before it was not—like DOGE—an executive component bereft of *any* statutory authority. Instead, *NRC* involves a lengthy discussion of the agency's licensing and regulatory authority under two successive acts of Congress. *NRC*, 145 S. Ct. at 1776–79. The DOGE Defendants point to no statutory authority at all.

Here, the DOGE Defendants directed a fundamental shift in the policy of protecting IRS data. Am. Compl. ¶¶ 217–221. DOGE has no authority to take the actions Plaintiffs have alleged they undertook, and it would be illogical to find that *ultra vires* review is only available where an agency has far exceeded some real authority, but not where an entity lacking any statutory authority has exercised sweeping powers.[53]

Even if *ultra vires* review did require the identification of a specific statutory prohibition, Plaintiffs *have* alleged that the conduct DOGE Defendants have directed IRS to violate statutory prohibitions with IRS's broad Data Policy, specifically provisions of the Internal Revenue Code and the Privacy Act. 26 U.S.C. § 6103; 5 U.S.C. § 552a(b–e). *See* Am. Compl. ¶¶ 162, 179, 217. Congress placed stringent and specific restrictions on when that data may be shared under the Plaintiffs have pled that the DOGE Defendants directed IRS to shift its policy to the new Data Policy of broad and open sharing within the executive branch, which violates the stringent protections in 26 U.S.C. § 6103 and 5 U.S.C. § 552a. Am. Compl. ¶¶ 159–162, 217–219. In doing this, the DOGE Defendants led the efforts to create a "mega API" to share IRS data and effected the removal of dozens of senior executive service IT staff. Am. Compl. ¶¶ 162. The DOGE Defendants have thus effected the violation of these stringent statutory prohibitions on sharing of taxpayer information.

While *ultra vires* review is limited to scenarios where there is no "meaningful and adequate opportunity for judicial review," that standard is met here. *NRC*, 145 S. Ct. at 1776. Should the Court dismiss the APA claim, it is certainly met for the same reasons discussed above. Nor should

[53] The Court in *New Mexico*, found that *ultra vires* review was available in a challenge to DOGE's actions under an analysis of whether it acted in excess of statutory authority as well where the Court considered whether the limited temporary organization statute afforded DOGE authority for challenged actions; it did not. 2025 WL 1502747, at *17.

the Court dismiss the *ultra vires* claim if it were to permit the APA claim to proceed. Although courts in this district, "with differing degrees of certainty," have sometimes dismissed *ultra vires* claims in circumstances where relief was available against a defendant under the APA, they have done so where both APA and *ultra vires* claims were pled against the same agency defendant. *Lewis v. U.S. Parole Comm'n*, 743 F. Supp. 3d 181, 200 (D.D.C. 2024) (both APA and *ultra vires* claims pled against the Parole Commission); *see also Jafarzadeh v. Duke*, 270 F. Supp. 3d 296, 311 (D.D.C. 2017) (Plaintiffs brought the "same claim" against agency defendants under the APA and *ultra vires* claim). And courts have particularly found that, at "an early stage" of litigation, dismissal of an *ultra vires* claim because of a separate APA claim is inappropriate, as logically the APA claim may no longer be available at a later stage. *Ctr. for Biological Diversity v. Trump*, 453 F. Supp. 3d 11, 48 (D.D.C. 2020); *AFL-CIO*, 2025 WL 1129227, at *22.

Here Plaintiffs have only brought an *ultra vires* claim against the DOGE Defendants, and, as DOGE is not itself an agency, they lack any other means of seeking a remedy that would enjoin DOGE's unlawful behavior. The DOGE Defendants have repeatedly ridden roughshod over IRS officials, pushed out those who offer pushback, and ultimately directed the IRS's conduct. *Supra* Background A.2.; Am. Compl. ¶¶ 162–166. An injunction that binds the DOGE defendants and prohibits their *ultra vires* conduct, as well as the Treasury-IRS defendants under the APA, is necessary to provide "meaningful and adequate" relief from this policy put in place at DOGE's direction. *Bd. of Governors of Fed. Rsrv. Sys. v. McCorp Fin.*, 502 U.S. 32, 43 (1991).

CONCLUSION

Plaintiffs have standing to challenge the Data Policy that imminently risks mass disclosure of the protected data of their members and clients. The discrete damages provisions of the Internal Revenue Code and Privacy Act do not provide an adequate alternative remedy to APA review of

this consequential, ongoing policy, and the DOGE defendants direction of this policy without any source of authority is *ultra vires*. Plaintiffs respectfully request that the Court deny Defendants' motion to dismiss.

Dated: August 1, 2025

Respectfully submitted,

/s/ Daniel A. McGrath
Daniel A. McGrath (D.C. Bar No. 1531723)
Johanna M. Hickman (D.C. Bar No. 981770)
Madeline H. Gitomer (D.C. Bar No 1023447)
Robin Thurston (D.C. Bar No. 1531399)
Democracy Forward Foundation
P.O. Box 34553
Washington, DC 20043
(202) 812-7824
dmcgrath@democracyforward.org
hhickman@democracyforward.org
mgitomer@democracyforward.org
rthurston@democracyforward.org

Counsel for Plaintiffs

CERTIFICATE OF SERVICE

I, Daniel A. McGrath, certify that I filed the foregoing and its attachments with the Clerk of the Court for the United States District Court for the District of Columbia by using the CM/ECF system, which sent a notice of such filing to all registered CM/ECF users who have appeared in this case.

/s/ *Daniel A. McGrath*
Counsel for Plaintiffs