UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

LEAGUE OF WOMEN VOTERS
1233 20th Street, NW, Suite 500
Washington, DC 20036,

LEAGUE OF WOMEN VOTERS OF VIRGINIA
1011 East Main Street, Suite 214A
Richmond, VA 23219,

LEAGUE OF WOMEN VOTERS OF LOUISIANA
P.O. Box 851068
New Orleans, LA 70185,

LEAGUE OF WOMEN VOTERS OF LOUISIANA EDUCATION FUND
P.O. Box 851068
New Orleans, LA 70185,

ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Avenue, NW
Washington, DC 20036,

J. DOES 1 – 5, on behalf of themselves and others similarly situated,
c/o Citizens for Responsibility and Ethics in Washington
P.O. Box 14596
Washington, DC 20044,[1]

Plaintiffs,

v.

U.S. DEPARTMENT OF HOMELAND SECURITY
245 Murray Ln., SW
Washington, DC 20528,

CLASS ACTION COMPLAINT FOR INJUNCTIVE AND DECLARATORY RELIEF

Case No. _____

[1] Plaintiffs' motion to proceed under pseudonyms is forthcoming.

KRISTI NOEM, in her official capacity as Secretary of the U.S. Department of Homeland Security
245 Murray Ln., SW
Washington, DC 20528,

SOCIAL SECURITY ADMINISTRATION
6401 Security Blvd.
Baltimore, MD 21235,

FRANK BISIGNANO, in his official capacity as Commissioner of the Social Security Administration
6401 Security Blvd.
Baltimore, MD 21235,

U.S. DEPARTMENT OF JUSTICE
950 Pennsylvania Ave., NW
Washington, DC 20530,

PAMELA BONDI, in her official capacity as U.S. Attorney General
950 Pennsylvania Ave., NW
Washington, DC 20530,

Defendants.

TABLE OF CONTENTS

INTRODUCTION 1

PARTIES 8

JURISDICTION AND VENUE 12

LEGAL FRAMEWORK 13

FACTUAL ALLEGATIONS 19

I. The Trump administration creates DOGE and tasks it with government-wide data consolidation 19

II. DOGE, DHS, and USCIS secretly consolidate Americans' sensitive personal data from multiple agencies without statutorily required notice to the public and Congress or any assessment of the privacy implications or risks of error 23

A. Defendants unlawfully transform USCIS's SAVE system into a national citizenship data bank that pools unreliable SSA data, which states are using to purge voter rolls and open criminal investigations 25

1. The prior SAVE system's limited authorized scope and functionality 26

2. Defendants "overhaul" SAVE by turning it into an interagency system that directly queries SSA records systems and allows bulk searches of millions of Americans' sensitive data 28

3. The overhauled SAVE system utilizes unreliable SSA citizenship data 32

4. States' use of the overhauled SAVE system threatens to disenfranchise eligible voters in impending elections and subject them to unwarranted criminal investigations 35

5. Defendants are ingesting state voter roll data through the SAVE system and incorporating it into DHS Interagency Data Systems. 39

B. Defendants unlawfully pool interagency data in the USCIS Data Lake. 40

INJURIES TO PLAINTIFFS 46

CLASS ACTION ALLEGATIONS 52

CLAIMS FOR RELIEF 55

COUNT ONE
Violation of the APA (Privacy Act)
Agency Action Contrary to Law and Required Procedure, 5 U.S.C. § 706(2)..... 55

COUNT TWO
Violation of the APA (Privacy Act)
Agency Action Unlawfully Withheld or Unreasonably Delayed, 5 U.S.C. § 706(1)..... 57

COUNT THREE
Violation of the APA
Arbitrary and Capricious Agency Action, 5 U.S.C. § 706(2)..... 57

COUNT FOUR
Violation of Non-Discretionary Official Duties
Mandamus, 28 U.S.C. § 1361 58

COUNT FIVE
Ultra Vires 59

COUNT SIX
Violation of the Separation of Powers 60

PRAYER FOR RELIEF 60

INTRODUCTION

1. Americans do not want the government to combine their sensitive personal information into a centralized database. The American people have spoken clearly and loudly on this topic through their elected representatives in Congress for decades, resulting in numerous laws requiring that the collection and use of Americans' personal data be transparent, limited, and rigorously justified. Congress passed and presidents signed these laws clear-eyed that they would constrain the executive branch's ability to consolidate Americans' personal information. But that trade-off was worth it to prevent Americans' private data from being compromised or, worse, weaponized as a tool for abuse.

2. Unfortunately, the Defendants in this case are ignoring these laws to create comprehensive databases of American citizens' data, centralized at the Department of Homeland Security ("DHS"). The Plaintiffs in this case include a proposed class of millions of American citizens and permanent residents whose records have been unlawfully pooled into new or revised centralized records systems at DHS, as well as organizations whose members and missions are harmed by Defendants' attempts to ignore the laws protecting Americans' privacy.

3. Congress passed the Privacy Act of 1974 specifically to prevent the government from creating "formal or de facto national data banks" or "centralized Federal information systems" that would consolidate sensitive personal data of Americans stored at separate agencies.[2] Congress established robust safeguards against such "interagency computer data banks" to make it "legally impossible for the Federal Government in the future to put together anything resembling

[2] S. Comm. on Gov't Operations and H.R. Comm. on Gov't Operations, 94th Cong., 2d Sess., Legislative History of the Privacy Act of 1974 – S. 3418 (Pub. L. No. 93-579), Source Book on Privacy at 168 (1976), https://perma.cc/9W9F-R5ZL ("Privacy Act Legis. History").

a '1984' personal dossier on a citizen," and to ensure "proper regard for privacy of the individual, confidentiality of data, and security of the system."[3]

4. Congress reaffirmed this objective in 1988 by amending the Privacy Act to prohibit "computer matching programs" that compare data across agencies unless participating agencies execute and disclose to Congress and the public written "matching agreements" detailing their interagency data sharing. 5 U.S.C. §§ 552a(o), 552a(a)(8). Congress further instructed that nothing in the Privacy Act "shall be construed to authorize" the "establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies"; the "direct linking of computerized systems of records maintained by Federal agencies"; or "the computer matching of records not otherwise authorized by law." Computer Matching and Privacy Protection Act of 1988, Pub. L. No. 100-503, § 9, 102 Stat. 2507, 2514, *codified at* 5 U.S.C. § 552a note.

5. For decades, these protections have guarded against improper data pooling across federal agencies, preventing the government from building a potentially dangerous tool for surveilling and investigating Americans without guardrails. Until now.

6. DHS, with help from the Department of Government Efficiency ("DOGE"), is working rapidly to create precisely the type of "national data banks" the American people and Congress have consistently resisted, and the Privacy Act was designed to prevent. To that end, they have embarked on a months-long campaign to access, collect, and consolidate vast troves of personal data about millions of U.S. citizens and residents stored at multiple federal agencies.

[3] *Id.* at 884, 217.

7. Defendants' goal is to create a web of linked data systems that allow centralized queries and analyses of millions of Americans' most sensitive information.[4]

8. Defendants seek to unify data across the government to advance Trump administration priorities, including making it harder to vote, and ensuring that every contact between immigrants (regardless of their legal status) and government databases can be leveraged to support the administration's agenda. Defendants claim to be taking these actions under the artifice of reducing "waste, fraud, and abuse" in government. *See, e.g.*, Stopping Waste, Fraud, and Abuse by Eliminating Information Silos, Exec. Order No. 14,243, 90 Fed. Reg. 13681 (Mar. 20, 2025).

9. DHS's linked data systems unlawfully pool Americans' personal data from existing systems of records housed at, among other agencies, DHS, U.S. Citizenship and Immigration Services ("USCIS"), the Social Security Administration ("SSA"), the Department of Health and Human Services ("HHS"), the Internal Revenue Service ("IRS"), the Department of Labor ("DOL"), and several states' election databases.

10. The linked data systems DHS is creating—collectively referred to here as DHS's "Interagency Data Systems"—include at least two pooled data sets.

11. First, Defendants have unlawfully transformed USCIS's Systematic Alien Verification for Entitlements ("SAVE") tool into a searchable national citizenship data system that now draws from SSA systems of records, in addition to the DHS systems of records SAVE previously accessed.

[4] Linkages between disparate databases may take many forms, including but not limited to the creation of a discrete repository of records with data pooled from multiple agencies' systems of records, or the creation of an interoperable network by which multiple agency systems of records can be simultaneously queried using an application programming interface or other means.

12. The overhauled SAVE interagency system allows its more than 1,200 user agencies, for the first time ever, to query the U.S. citizenship or immigration status of any person—including U.S.-born citizens—using their Social Security Number ("SSN"). It also allows searches of potentially millions of individuals' sensitive SSA data with a single query.

13. These dramatic changes far exceed the SAVE system's limited authorized scope and functionality, which previously did not allow bulk searches or queries of U.S.-born citizens. Nor did it previously pool from SSA data or include any search-by-SSN function.

14. SSA itself has admitted that its citizenship data—especially for naturalized citizens and U.S.-born citizens born before 1981—is incomplete, unreliable, and not "definitive." SSA has repeatedly cautioned against relying on the data and stressed that SSA is not responsible for making citizenship determinations.[5]

15. Nonetheless, Defendants are now encouraging and enabling states to use unreliable SSA citizenship data pooled in the overhauled SAVE system to begin purging voter rolls ahead of fast-approaching November elections and to open criminal investigations of alleged non-citizen voting. States such as Virginia, Louisiana, and Texas are doing exactly that, imperiling the right to vote of naturalized citizens and others for whom SSA maintains outdated and inaccurate citizenship data.

16. Defendants are also keeping the voter roll data that states are bulk uploading into the SAVE system or providing through other means and consolidating it in unauthorized ways.

17. Second, in addition to the overhauled SAVE system, Defendants have created at least one other Interagency Data System that consolidates other data sources from around the

[5] Letter from SSA Off. of Gen. Counsel to Fair Elections Ctr. 2 (July 13, 2023), https://perma.cc/KS2N-U2US ("July 2023 SSA Ltr.").

government that might have information concerning immigrants into a centralized "data lake" housed at USCIS ("USCIS Data Lake").

18. The personal information Defendants are consolidating into the USCIS Data Lake is extraordinarily sensitive. It includes millions of Americans' SSNs, biometric data, tax information, wage and employment records, medical and disability records, detailed case files involving child abuse, and more.

19. Government agencies originally collected these records for several discrete purposes, including to facilitate and document employment arrangements, collect taxes, and ensure care and resources for children. The government did not collect these records to feed into any interagency data system. Nor did Americans ever consent to their personal data being aggregated in this way.

20. Defendants have pooled Americans' personal data into Interagency Data Systems in secret, without statutorily required notice to and comment from the public or Congress, and without assessing the privacy implications or risks of error posed by repurposing the data in this way.

21. Defendants' actions violate the Privacy Act's requirements and the core values it embodies. In the first instance, the Interagency Data Systems are prohibited "national data bank[s] that combine[], merge[], or link[] information on individuals maintained in systems of records by …. Federal agencies"; prohibited systems that "direct[ly] link … computerized systems of records maintained by Federal agencies"; and/or prohibited "computer matching[s] of records not otherwise authorized by law." 5 U.S.C. § 552a note.

22. Defendants have also violated the Privacy Act's numerous safeguards by creating and significantly changing existing agency "systems of records" without advance notice published

in the Federal Register or opportunity for public comment, *see* 5 U.S.C. §§ 552a(e)(4), (11); failing to keep accurate accountings of disclosures of information from the new and revised systems, *id.* § 552a(c); failing to establish appropriate administrative, technical, and physical safeguards for the new and revised systems, *id.* § 552a(e)(10); and creating and significantly changing interagency "computer matching programs" without first executing or disclosing to Congress written "matching agreements" detailing their parameters, *id.* § 552a(o), or notifying the public, *id.* § 552a(e)(12).

23. Defendants are running roughshod over these privacy protections, hoping the speed, audacity, and opacity of their work will render all legal constraints meaningless.

24. Defendants' actions not only run contrary to these explicit prohibitions designed to protect the privacy of the American public, but also far exceed any limited lawful authority Defendants have.

25. Defendants' unlawful and *ultra vires* compilation of the personal data of millions into Interagency Data Systems also creates massive cybersecurity risks. It draws a bullseye for hackers to target individuals' most sensitive—and until recently, most closely protected—personal information.

26. Defendants' actions have harmed and will continue to harm Americans whose sensitive data is being unlawfully consolidated, including the individual plaintiffs—J. Does 1, 2, 3, 4, and 5—who seek to represent a class of millions of similarly situated Americans ("Individual Plaintiffs" or "Proposed Class Representatives"). Among those individuals are members of the League of Women Voters of Virginia and the League of Women Voters of Louisiana, who are also members of the League of Women Voters (collectively, "the League Plaintiffs"), and members of Plaintiff Electronic Privacy Information Center ("EPIC"). These individuals reasonably fear the

mishandling and misuse of their sensitive personal data, which they did not consent to being repurposed as Defendants have. They include naturalized citizens at risk of being wrongfully purged from voter rolls and disenfranchised in states with imminent November elections, and wrongfully investigated for lawful voting, based on inaccurate SSA data that Defendants are illegally pooling into the overhauled SAVE system, as well as U.S.-born citizens for whom SSA lacks data on citizenship status. And all Plaintiffs have been deprived of statutorily required information about Defendants' secretive pooling of their personal data and any opportunity to surface concerns about it, contrary to the Privacy Act's transparency and notice-and-comment requirements.

27. Defendants' unlawful actions are also directly harming the League Plaintiffs and EPIC. They too have been denied statutorily guaranteed information about the Interagency Data Systems, which they need to further their core missions—for the League Plaintiffs, empowering voters through voter registration, education, and engagement, and for EPIC, ensuring that Americans' privacy rights are safeguarded. They have also been denied their notice-and-comment rights under the Privacy Act, stripping them of the opportunity to convey, and have the government consider, their concerns about the Interagency Data Systems' impact on the voting and privacy rights of the many thousands of Americans they serve, including their members.

28. Plaintiffs request that the Court declare unlawful and vacate Defendants' *ultra vires* actions, enjoin Defendants from continuing to operate the unlawful Interagency Data Systems, and order them to erase all misappropriated data, disconnect the disparate systems they have unlawfully linked, and publish notices in the Federal Register disclosing statutorily required details about their illegal Interagency Data Systems.

PARTIES

29. Plaintiff League of Women Voters ("LWV") is a nonprofit, nonpartisan, grassroots, community-based membership organization headquartered in Washington, D.C., that promotes political responsibility by encouraging Americans to participate in the electoral process. Founded in 1920 as an outgrowth of the struggle to win voting rights for women, LWV now has more than a million members and supporters and is organized in more than 750 communities and in every state and the District of Columbia. LWV comprises two entities: the League of Women Voters of the United States ("LWVUS") and the League of Women Voters Education Fund ("LWVEF"). LWVUS is a 501(c)(4) social welfare organization that encourages informed and active participation in government, works to increase understanding of major public policy issues, and influences public policy through education and advocacy. LWVEF is a 501(c)(3) organization and works to register and provide voters with election information through its election resource VOTE411.org, candidate forums, and debates.

30. As part of its mission, LWV—with its state and local Leagues—operates one of the longest-running and largest nonpartisan voter registration efforts in the nation. Through its work, LWV registers many thousands of voters every election cycle and is instrumental in ensuring access to voter registration for all eligible voters, including naturalized and derived U.S. citizens, and U.S.-born citizens born before 1981.[6] LWV maintains—with its state and local Leagues—

[6] A "derived citizen" refers to an individual born outside of the U.S. who automatically becomes a U.S. citizen by operation of law where: (1) the person is the child of a parent who is a U.S. citizen by birth or becomes a U.S. citizen through naturalization, (2) the child is under 18 years old, (3) the child is a lawful permanent resident, and (4) the child is residing in the U.S. in the legal and physical custody of the U.S. citizen parent. *See* Policy Manual, Chapter 4 - *Automatic Acquisition of Citizenship after Birth (INA 320)*, USCIS, https://perma.cc/L95Q-H2HL.

VOTE411.org, an award-winning, nonpartisan, online resource committed to ensuring voters have the information they need to successfully participate in every election—local, state, and federal.

31. Plaintiff League of Women Voters of Virginia ("LWVVA") is a 501(c)(3) nonpartisan, nonprofit, membership organization that seeks to encourage informed and active participation in government. LWVVA is the Virginia affiliate of the national League, and is headquartered in Richmond, Virginia. LWVVA has approximately 2,000 members across the state of Virginia. LWVVA's members include naturalized citizens, as well as U.S.-born citizens born before 1981.

32. Plaintiffs League of Women Voters of Louisiana and League of Women Voters of Louisiana Education Fund (together, "LWVLA"), formed under Section 501(c)(4) and 501(c)(3) of the Internal Revenue Code, respectively, are nonpartisan, nonprofit, membership organizations that seek to encourage informed and active participation in government. LWVLA is the Louisiana affiliate of the national League, and is headquartered in New Orleans, Louisiana. LWVLA has approximately 300 members across six chapters in the state of Louisiana. LWVLA's members include naturalized citizens, as well as U.S. born citizens born before 1981.

33. Both LWVVA and LWVLA comprise dues-paying members, who are also members of the national League. LWVVA and LWVLA members volunteer in their communities to provide voter services. Neither LWVVA nor LWVLA has paid employees or staff involved with the operation of LWV. Through their volunteer leaders, LWVVA and LWVLA provide regular training to their members and to their nonpartisan partners to assist Virginians and Louisianans, respectively, registering to vote, voting, and confirming their voter registration status. LWVVA and LWVLA do this work as a part of their missions to empower Virginia and Louisiana voters, including naturalized citizen voters, and to defend their right to vote. They consider their

work registering voters, encouraging them to vote, and confirming their registration to be an expression of those core values. LWVVA and LWVLA use voter registration assistance as a part of a larger dialogue about a citizen's voter registration, voting plan, and the importance of voter participation in elections. Their goal is to ensure all eligible Virginia and Louisiana voters—including naturalized and derived U.S. citizens—are registered to vote, have a plan to vote, and can and do actually vote.

34. Plaintiff EPIC is a nonprofit organization, headquartered in Washington, D.C., established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities that impact individual privacy. EPIC is a membership organization. An individual member of EPIC is any person who contributes to the advancement of EPIC's mission, who acts in accordance with the core values and policies of EPIC, and who has been recognized and registered as a member by EPIC, by virtue of payment of annual dues or having been granted a dues waiver. This includes members of EPIC's Advisory Board, who are distinguished experts in law, technology, and public policy.

35. Plaintiff J. Doe 1 lives and is qualified and registered to vote in Texas. J. Doe 1 plans to vote in Texas's upcoming election in November 2025. J. Doe 1 was born outside of the United States and became a naturalized U.S. citizen in 2017. J. Doe 1 is a university professor. J. Doe 1 has started a new job within the past two years. J. Doe 1 has personally identifiable information ("PII") in SSA databases, HHS's National Directory of New Hires ("NDNH"), other federal agency databases, and Texas election databases. J. Doe 1's PII has been transferred, copied, ingested, or otherwise incorporated into the overhauled SAVE system at DHS, and, upon information and belief, J. Doe 1's PII has also been incorporated into the USCIS Data Lake. J. Doe 1's SSA records incorrectly represent that J. Doe 1 is not a U.S. citizen.

36. Plaintiff J. Doe 2 is an attorney who lives and is qualified and registered to vote in Washington, D.C. J. Doe 2 is a derived U.S. citizen who gained U.S. citizenship as a child through parental naturalization. J. Doe 2 was a longtime civil servant and federal prosecutor who was fired by political leadership in the Trump administration. J. Doe 2 started a new job within the past two years. J. Doe 2 has PII in SSA databases, the NDNH, and other federal agency databases. J. Doe 2's PII has been transferred, copied, ingested, or otherwise incorporated into the overhauled SAVE system at DHS, and, upon information and belief, J. Doe 2's PII has also been incorporated into the USCIS Data Lake.

37. Plaintiff J. Doe 3 is an attorney who lives and is qualified and registered to vote in Maryland. J. Doe 3 was born prior to 1981 and is a U.S. citizen by birth. As a child, J. Doe. 3 lived abroad with family, and, upon returning to the U.S., they were subjected to surveillance by the U.S. government. J. Doe 3 has served in various leadership roles in Maryland state government. J. Doe 3 started a new job within the past two years. J. Doe 3 has PII in SSA databases, the NDNH, and other federal agency databases. J. Doe 3's PII has been transferred, copied, ingested, or otherwise incorporated into the overhauled SAVE system at DHS, and, upon information and belief, J. Doe 3's PII has also been incorporated into the USCIS Data Lake.

38. Plaintiff J. Doe 4 lives and is qualified and registered to vote in Louisiana. J. Doe 4 has voted in Louisiana elections and intends to vote in an upcoming election in October 2025. J. Doe 4 was born outside of the United States and became a naturalized U.S. citizen in 2014. J. Doe 4 has PII in SSA databases, other federal agency databases, and Louisiana election databases. J. Doe 4's PII has been transferred, copied, ingested, or otherwise incorporated into the overhauled SAVE system at DHS. J. Doe 4's SSA records incorrectly represent that J. Doe 4 is not a U.S. citizen.

39. Plaintiff J. Doe 5 lives and is qualified and registered to vote in Virginia. J. Doe 5 has voted in Virginia elections and intends to vote in an upcoming election in November 2025. J. Doe 5 was born outside of the United States and became a naturalized U.S. citizen in 2020. J. Doe 5 has PII in SSA databases, other federal agency databases, and Virginia election databases. J. Doe 5's PII has been transferred, copied, ingested, or otherwise incorporated into the overhauled SAVE system at DHS. J. Doe 5's SSA records incorrectly represent that J. Doe 5 is not a U.S. citizen.

40. Defendant DHS is an agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), and the APA, 5 U.S.C. § 551(1), that is headquartered in Washington, D.C.

41. Defendant Kristi Noem is the Secretary of DHS and is sued in her official capacity.

42. Defendant SSA is an agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), and the APA, 5 U.S.C. § 551(1), that is headquartered in Baltimore, Maryland.

43. Defendant Frank Bisignano is the Commissioner of SSA and is sued in his official capacity.

44. Defendant U.S. Department of Justice ("DOJ") is an agency within the meaning of the Privacy Act, 5 U.S.C. § 552a(a)(1), and the APA, 5 U.S.C. § 551(1), that is headquartered in Washington, D.C.

45. Defendant Pamela Bondi is the U.S. Attorney General and is sued in her official capacity.

JURISDICTION AND VENUE

46. This Court has jurisdiction under 28 U.S.C. § 1331 because this action arises under the laws of the United States. This Court has further remedial authority under the Declaratory

Judgment Act, 28 U.S.C. §§ 2201-2202, and the Administrative Procedure Act, 5 U.S.C. §§ 701, *et seq.*

47. The Court further has jurisdiction under the mandamus statute, 28 U.S.C. § 1361.

48. Venue lies in this District under 28 U.S.C. § 1391(e)(1)(C) because Defendants include officers and agencies of the United States headquartered in this District.

LEGAL FRAMEWORK

The Privacy Act

49. "Enacted in the wake of the Watergate and the Counterintelligence Program (COINTELPRO) scandals involving illegal surveillance on opposition political parties and individuals deemed to be 'subversive,' the Privacy Act sought to restore trust in government and to address what at the time was seen as an existential threat to American democracy."[7]

50. The Privacy Act's "raison d'etre" is "to provide for protection against possible abuses of governmental power to affect an individual's privacy and confidential information." *Williams v. Dep't of Veterans Affs.*, 104 F.3d 670, 676 (4th Cir. 1997). The Act does so through a "comprehensive and detailed set of requirements for the management of confidential records held by Executive Branch agencies." *FAA v. Cooper*, 566 U.S. 284, 287 (2012).

51. The Act imposes mandatory requirements for any agency "system of records," which it defines as a "group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual." 5 U.S.C. § 552a(a)(5).

52. The Act defines "record" as "any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial

[7] U.S. Dep't of Just., *Overview of the Privacy Act of 1974*, at 1 (2020 ed.), https://perma.cc/6SB9-XAEK (cleaned up).

transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph." *Id.* § 552a(a)(4).

53. The Act defines "individual" as any "citizen of the United States or [] alien lawfully admitted for permanent residence." *Id.* § 552a(a)(2).

54. "[T]he determination" of whether a "system of records exists triggers virtually all of the other substantive provisions of the Privacy Act." *Henke v. U.S. Dep't of Com.*, 83 F.3d 1453, 1459 (D.C. Cir. 1996). This fact-intensive inquiry requires courts to "take into account 'the entirety of the situation, including the agency's function, the purpose for which the information was gathered, and the agency's actual retrieval practices and policies.'" *Maydak v. United States*, 363 F.3d 512, 520 (D.C. Cir. 2004) (quoting *Henke*, 83 F.3d at 1461).

55. The Privacy Act prohibits agencies from "disclos[ing] any record which is contained in a system of records … except pursuant to a written request by, or with the prior written consent of, the individual to whom the record pertains," or unless such disclosure fits an enumerated exception. 5 U.S.C. §§ 552a(b)(1)-(13). The Act also requires agencies to create and maintain an "accounting of certain disclosures," *id.* § 552a(c); confers rights on individuals to request access to and amendment of their records, *id.* § 552a(d); and imposes other "agency requirements" for the maintenance, collection, use, or dissemination of covered information, *id.* §§ 552a(a)(3), (e), (f).

56. The Act, as amended by the Computer Matching and Privacy Protection Act of 1988, further prohibits disclosure of records contained in a system of records "to a recipient agency or non-Federal agency for use in a computer matching program except pursuant to a written

agreement between the source agency and the recipient agency or non-Federal agency." *Id.* § 552a(o)(1).

57. The Act defines "matching program" to include "any computerized comparison of … two or more automated systems of records or a system of records with non-Federal records for the purpose of … establishing or verifying the eligibility of, or continuing compliance with statutory and regulatory requirements by, applicants for, recipients or beneficiaries of, participants in, or providers of services with respect to, cash or in-kind assistance or payments under Federal benefit programs, or … recouping payments or delinquent debts under such Federal benefit programs." *Id.* § 552a(a)(8).

58. "Matching agreements" must include detailed data elements and meet strict requirements designed to ensure public transparency and participation, congressional oversight, and rigorous legal compliance concerning interagency data transfers. *See id.* §§ 552a(o)(1)-(2).

59. In enacting the 1988 amendments, Congress codified clear instructions that nothing in the Privacy Act "shall be construed to authorize" the "establishment or maintenance by any agency of a national data bank that combines, merges, or links information on individuals maintained in systems of records by other Federal agencies"; the "direct linking of computerized systems of records maintained by Federal agencies"; or "the computer matching of records not otherwise authorized by law." Pub. L. No. 100-503, § 9, 102 Stat. at 2514, *codified at* 5 U.S.C. § 552a note.

60. When an agency "establish[es] or revis[es]" any "system of records" containing retrievable information about individuals, it must "publish in the Federal Register … a notice of the existence and character of the system of records," 5 U.S.C. § 552a(e)(4), commonly called a System of Records Notice ("SORN"). Each SORN "shall include":

> (A) the name and location of the system;
>
> (B) the categories of individuals on whom records are maintained in the system;
>
> (C) the categories of records maintained in the system;
>
> (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
>
> (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
>
> (F) the title and business address of the agency official who is responsible for the system of records;
>
> (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
>
> (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
>
> (I) the categories of sources of records in the system.

Id.

61. At least 30 days before publishing a SORN, the agency must also "publish in the Federal Register a notice of any new use or intended use of the information in the system" and "provide an opportunity for interested persons to submit written data, views, or arguments to the agency." *Id.* § 552a(e)(11). "In no circumstance may an agency use a new or significantly modified routine use as the basis for a disclosure fewer than 30 days following Federal Register publication." Off. of Mgmt. & Budget Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication under the Privacy Act*, at 7 (2016), https://perma.cc/N9QK-SDLE ("OMB Circular No. A-108").

62. Similarly, at least 30 days before establishing or revising a "matching program," an agency must "publish in the Federal Register notice of such establishment or revision." 5 U.S.C. § 552a(e)(12).

63. The "requirement for agencies to publish a SORN allows the Federal Government to accomplish one of the basic objectives of the Privacy Act–fostering agency accountability through public notice." OMB Circular No. A-108 at 5. Similarly, "[t]he requirement for agencies to publish a matching [program] notice allows the Federal Government to foster transparency and accountability with respect to agencies' matching programs." *Id.* at 18.

64. Binding OMB guidelines mandate that federal agencies "shall" review and consider any "public comments on a published SORN" or "a published matching [program] notice." *Id.* at 7, 19; *see also* 5 U.S.C. § 552a(v)(1).

65. To further ensure transparency and congressional oversight, any time an agency "proposes to establish or make a significant change in a system of records or a matching program," it must "provide adequate advance notice of any such proposal" to Congress and the Office of Management and Budget "to permit an evaluation of the probable or potential effect of such proposal on the privacy or other rights of individuals." 5 U.S.C. § 552a(r).

66. Congress enacted these requirements to "assure knowledge by Congress, the executive branch, and interested groups of new Federal data banks and pooling of informational and computer resources to constitute centralized data systems not foreseen by Congress"; to "prevent [] de facto national data banks on individuals free of all restraints on Federal power established by Constitution and statutes"; and to "prevent creation of data banks and new personal information systems without statutory authorization from Congress and without proper regard for privacy of the individual, confidentiality of data, and security of the system." Privacy Act Legis. History at 217.

67. To further protect the security of individuals, the Privacy Act requires agencies to implement both human safeguards (*i.e.*, rules of conduct and training) and administrative,

technical, and physical safeguards for any systems of records. 5 U.S.C. §§ 552a(e)(9)-(10). These requirements are designed to prevent "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained." *Id.* § 552a(e)(10).

Other Federal Privacy Laws

68. Information technology has evolved dramatically since the Privacy Act's passage in 1974, and Congress has passed several laws to reinforce and supplement the Act's protections.

69. The E-Government Act of 2002 requires federal agencies to conduct, review, and, "if practicable," publish, a Privacy Impact Assessment ("PIA") before either "developing or procuring information technology that collects, maintains, or disseminates" PII or "initiating a new collection of information" involving PII that will be "collected, maintained, or disseminated using information technology." Pub. L. No. 107-347, §§ 208(b)(1)(A)-(B), 116 Stat. 2899, 2921-23 (2002), *codified at* 44 U.S.C. § 3501 note.

70. A PIA must address, at a minimum, what information will be collected, why it is being collected, how it will be used, how it will be secured, with whom it will be shared, whether a system of records is being created under the Privacy Act, and what "notice or opportunities for consent" will be provided to those impacted. *Id.* § 208(b)(2)(B)(ii)(V).

71. The Federal Information Security Modernization Act of 2014 ("FISMA") requires agency heads to "provid[e] information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, [or] disclosure" of agency information or information systems. 44 U.S.C. § 3554(a)(1)(A).

FACTUAL ALLEGATIONS

I. The Trump administration creates DOGE and tasks it with government-wide data consolidation

72. On November 12, 2024, then-President-elect Trump announced the creation of the "Department of Government Efficiency," saying it would "pave the way" for the Trump-Vance Administration to "dismantle," "slash," and "restructure" federal programs and services.[8]

73. This vision would turn into the President's "DOGE Agenda"—an amorphous initiative that includes the rapid dismantling of federal agencies, evisceration of the federal workforce, and government-wide consolidation of sensitive personal data.

The DOGE Executive Order

74. On January 20, 2025, President Trump signed Executive Order 14,158, Establishing and Implementing the President's "Department of Government Efficiency" ("DOGE EO"), renaming the former U.S. Digital Service as the U.S. DOGE Service ("USDS") and establishing it as a new component of the Executive Office of the President, headed by the USDS Administrator. 90 Fed. Reg. 8441.

75. The DOGE EO requires the installation of "DOGE Teams" at federal agencies, appointed by each agency head in consultation with the USDS Administrator. *Id.* Agency heads are required to "ensure that DOGE Team Leads coordinate their work with USDS and advise their respective Agency Heads on implementing the President's DOGE Agenda." *Id.*

76. Pertinent here, the DOGE EO requires that "Agency Heads shall take all necessary steps, in coordination with the USDS Administrator and to the maximum extent consistent with law, to ensure USDS has full and prompt access to all unclassified agency records, software

[8] *See* Donald J. Trump (@realDonaldTrump), Truth Social (Nov. 12, 2024, at 7:46 PM ET), https://perma.cc/V5H7-QZP6.

systems, and IT systems," and nominally provides that "USDS shall adhere to rigorous data protection standards," which the order does not define. *Id.*

The Data Consolidation Executive Order

77. On March 20, 2025, President Trump signed Executive Order 14,243, Stopping Waste, Fraud, and Abuse by Eliminating Information Silos (the "Data Consolidation EO"), which states that "[r]emoving unnecessary barriers to Federal employees accessing Government data and promoting inter-agency data sharing are important steps toward eliminating bureaucratic duplication and inefficiency while enhancing the Government's ability to detect overpayments and fraud." 90 Fed. Reg. 13681l (Mar. 25, 2025).

78. Echoing the DOGE EO, the Data Consolidation EO instructs that "Agency Heads shall take all necessary steps, to the maximum extent consistent with law, to ensure Federal officials designated by the President or Agency Heads (or their designees)"—which would include DOGE personnel—"have full and prompt access to all unclassified agency records, data, software systems, and information technology systems … for purposes of pursuing Administration priorities related to the identification and elimination of waste, fraud, and abuse." *Id.* The Data Consolidation EO adds that "[t]his includes *authorizing and facilitating both the intra- and inter-agency sharing and consolidation of unclassified agency records*." *Id.* (emphasis added).

79. The Data Consolidation EO also directs agency heads to "take all necessary steps, to the maximum extent consistent with law, to ensure the Federal Government has unfettered access to comprehensive data from all State programs that receive Federal funding, including, as appropriate, data generated by those programs but maintained in third-party databases." *Id.*

The Elections Executive Order

80. On March 25, 2025, President Trump signed Executive Order 14,248, Preserving and Protecting the Integrity of American Elections (the "Elections EO"), which, among other things, directs DHS to provide State and local officials with "access to appropriate systems for verifying the citizenship or immigration status of individuals registering to vote or who are already registered." 90 Fed. Reg. 14005 (Mar. 28, 2025).

81. The Elections EO directs DHS to coordinate with DOGE in reviewing: (1) each state's publicly available voter registration list, (2) available records concerning voter list maintenance activities, (3) Federal immigration databases; and (4) state records, "for consistency with federal requirements." *Id.*

82. The Elections EO further instructs that the "Commissioner of Social Security shall take all appropriate action to make available the Social Security Number Verification Service, the Death Master File, and any other Federal databases containing relevant information to all State and local election officials engaged in verifying the eligibility of individuals registering to vote or who are already registered." *Id.*

83. The Elections EO also instructs DOJ to prioritize prosecuting noncitizens who register to vote, whether they actually voted or not, using "databases or information maintained by the Department of Homeland Security." *Id.*

84. Apart from generic statements that they should be construed "consistent with law," none of the foregoing executive orders specifically mention the Privacy Act, E-Government Act, FISMA, or their restrictions on interagency data sharing and requirements for rigor and transparency in safeguarding Americans' privacy.

DOGE's Structure and Operations

85. As presently constituted, "DOGE" refers to the network of operatives within the government who are housed at multiple federal agencies but coordinated from outside of them. Many DOGE Team members are working at multiple agencies concurrently, collecting sensitive data from disparate systems of records and combining and cross-referencing them in ways expressly prohibited or never contemplated by the SORNs and security plans for those systems.[9]

86. While the DOGE EO only formally created two entities—USDS and the USDS Temporary Organization—DOGE does not operate exclusively out of either. DOGE has set up "home bases" within other federal agencies as well.

87. Agency DOGE Teams do the bulk of the work to carry out the DOGE Agenda, including demanding and obtaining unfettered access to sensitive agency systems to consolidate Americans' data.

88. Agency DOGE Team members formally assume titles as employees of or detailees to those agencies; however, DOGE Team members do not serve as normal agency employees. DOGE Teams carry out an externally imposed agenda coordinated by DOGE leaders outside of their host agencies.

[9] *See*, *e.g.*, Tim Marchman & Matt Giles, *This DOGE Engineer Has Access to the National Oceanic and Atmospheric Administration*, WIRED (Feb. 5, 2025), https://perma.cc/T6BT-XJKF; Vittoria Elliott, Leah Feiger, & Tim Marchman, *The US Treasury Claimed DOGE Technologist Didn't Have 'Write Access' When He Actually Did*, WIRED (Feb. 6, 2026), https://perma.cc/WB4M-6FG6; Avi Asher-Schapiro *et al.*, *Elon Musk's Demolition Crew*, ProPublica (Feb. 6, 2025), https://projects.propublica.org/elon-musk-doge-tracker/ (DOGE staffer Nikhil Rajpal working at NOAA, CFPB, and OPM and DOGE staffer Gavin Kliger working at CFPB, OPM, and USAID); Ella Nilsen & Sean Lyngaas, *Trump Energy Secretary Allowed 23-Year-Old Doge Rep To Access It Systems Over Objections From General Counsel*, CNN (Feb. 7, 2025), https://perma.cc/77DY-4KDU (DOGE staffer Luke Farritor working at HHS and Department of Energy); Evan Weinberger, *Musk's DOGE Descends on CFPB With Eyes on Shutting It Down*, Bloomberg Law (Feb. 7, 2025), https://perma.cc/A39S-J24B.

89. DOGE Team members work for DOGE and are, in reality, DOGE employees, even when they have formal management or employment relationships with their host agencies or other non-USDS entities.

II. DOGE, DHS, and USCIS secretly consolidate Americans' sensitive personal data from multiple agencies without statutorily required notice to the public and Congress or any assessment of the privacy implications or risks of error

90. DOGE leadership has confirmed that governmentwide data consolidation is a top priority for the entity. In a March 2025 interview, Elon Musk, whom at the time the President called DOGE's leader,[10] stated that

> [t]hese [government] databases don't talk to each other. And that's really the source of, that's the biggest vulnerability for fraud, is the fact that these databases don't talk to each other. So we need to reconcile the databases. It's, frankly, painful homework, but it has to be done, and will greatly improve the efficiency of the government systems.[11]

91. DOGE's data consolidation efforts have been carried out furtively, haphazardly, and with little regard for the security of Americans' sensitive personal data. Whistleblower disclosures to Congress show that, "[i]n an apparent attempt to sidestep network security controls, … DOGE engineers have tried to create specialized computers for themselves that simultaneously give full access to networks and databases across different agencies. … [I]ndividuals associated with DOGE have assembled backpacks full of laptops, each with access to different agency systems, that DOGE staff is using to combine databases that are currently maintained separately by multiple federal agencies."[12]

---

[10] Andrea Shalal & Nandita Bose, *Trump appears to contradict White House, says Elon Musk in charge of DOGE*, Reuters (Feb. 20, 2025), https://perma.cc/F6WL-FAD3.

[11] Fox News, *Elon Musk and DOGE team give behind the scenes look at their mission*, You Tube (Mar. 27, 2025), https://perma.cc/UNB9-F56Y.

[12] Letter from Gerald E. Connolly, Ranking Member, H. Comm. on Oversight and Gov't Reform, to Michelle L. Anderson, Assistant Inspector Gen. for Audit of the Soc. Sec. Admin., at 5 (Apr. 17, 2025), https://perma.cc/7YVB-Y5KH.

92. In another whistleblower disclosure to Congress, SSA's now-former Chief Data Officer Chuck Borges reported that DOGE team member Aram Mogaddassi—while serving as the SSA Chief Information Officer—created "a live copy of the country's Social Security information in a cloud environment that circumvents oversight."[13] "This vulnerable cloud environment is effectively a live copy of the entire country's Social Security information from the Numerical Identification System (NUMIDENT) database, that apparently lacks any security oversight from SSA or tracking to determine who is accessing or has accessed the copy of this data."[14] Borges stated these "serious data security lapses … risk the security of over 300 million Americans' Social Security data" and "involve wrongdoing including apparent systemic data security violations, uninhibited administrative access to highly sensitive production environments, and potential violations of internal SSA security protocols and federal privacy laws by DOGE personnel," including the Privacy Act.[15]

93. One of DOGE's highest priority projects concerns the consolidation of records related to immigrants. DOGE reportedly established a "specialized DOGE immigration task force that's embedded engineers and staffers across nearly every nook of the Department of Homeland Security" and is "working with DOGE operatives stationed at other agencies like the Social Security Administration and the Department of Health and Human Services, which house sensitive data on undocumented immigrants."[16]

---

[13] Letter from Gov't Accountability Project, *Protected Whistleblower Disclosure of Charles Borges Regarding Violation of Laws, Rules & Regulations, Abuse of Authority, Gross Mismanagement, and Substantial and Specific Threat to Public Health and Safety at the Social Security Administration*, at 3 (Aug. 26, 2025), https://perma.cc/G2AV-QUDE.

[14] *Id.*

[15] *Id.* at 1-2.

[16] Sophia Cai *et al.*, *Inside the DOGE immigration taskforce*, Politico (Apr. 11, 2025), https://perma.cc/JQ9B-SN77.

94. For the past few months, DOGE Teams assigned to agencies outside DHS have identified databases across the government containing records about immigrants and those associated with them—family members, employers, housemates, and others—to pool into DHS systems.[17]

95. These records contain PII about documented and undocumented immigrants, including U.S. citizens and lawful permanent residents.[18]

96. DOGE and DHS have repurposed pre-existing technology at USCIS to pool, merge, and consolidate individuals' sensitive personal data across agencies—all without statutorily required notice to the public or Congress, and without publicly assessing the privacy implications or risks of error posed by repurposing the data in this way. Those technological mechanisms include, but are not limited to, USCIS's SAVE system—which Defendants have unlawfully repurposed into a searchable national citizenship data system that utilizes unreliable SSA citizenship data—and a "data lake" housed at USCIS.

A. Defendants unlawfully transform USCIS's SAVE system into a national citizenship data bank that pools unreliable SSA data, which states are using to purge voter rolls and open criminal investigations

97. The SAVE program is "an inter-governmental initiative" administered by USCIS that is "designed to help federal, state, tribal, and local government agencies confirm citizenship and immigration status prior to granting benefits and licenses, as well as for other lawful

[17] Makena Kelly & Vittoria Elliott, *DOGE is Building a Master Database to Surveil and Track Immigrants*, WIRED (Apr. 18, 2025), https://perma.cc/64BE-VGED; Hannah Natanson *et al.*, *DOGE aims to pool federal data, putting personal information at risk*, Wash. Post (May 7, 2025), https://perma.cc/J528-AMVN.

[18] *Id.*

purposes."[19] SAVE's functionality allows queries of different records systems primarily within DHS.

98. SAVE user agencies "are required to formalize the purpose and use in which they use SAVE through a Memorandum of Agreement (MOA) or Computer Matching Agreement (CMA)," which establish "the terms and conditions for the user agency's participation in SAVE."[20]

99. Over 1,200 federal, state, and local agencies have access to SAVE.[21]

100. In recent years, election officials in some states have used the SAVE system to verify the citizenship of voter registrants and registered voters.[22]

101. Prior to 2025, ten states had MOAs to use SAVE for voter registration and/or voter list maintenance purposes: Arizona, Colorado, Florida, Georgia, Idaho, Mississippi, Ohio, South Carolina, Tennessee, and Virginia.[23]

1. The prior SAVE system's limited authorized scope and functionality

102. USCIS last published a SORN for SAVE on May 27, 2020.[24]

103. USCIS last published a PIA for SAVE on June 30, 2020.[25]

104. SAVE's operative SORN does not authorize or contemplate queries of U.S.-born citizens. Under the SAVE SORN and SAVE PIA, the SAVE system only permits queries "to verify

[19] Dep't of Homeland Sec., *Privacy Impact Assessment for the Systematic Alien Verification Entitlements Program*, DHS Ref. No. DHS/USCIS/PIA-006(c) at 2 (June 30, 2020), https://perma.cc/HU2M-NTL8 ("SAVE PIA").

[20] *Id.* at 2-3.

[21] Fair Elections Ctr., *Eligible Voters at Risk: Examining Changes to USCIS's Save System*, Issue Brief (July 2025), https://perma.cc/ZN5K-ATUC.

[22] *Id.*

[23] *Id.*

[24] Privacy Act Notice of Modified System of Records, 85 Fed. Reg. 31798 (May 27, 2020) ("SAVE SORN").

[25] SAVE PIA, *supra* n.19.

the citizenship and immigration status of an immigrant, nonimmigrant, and certain *naturalized and derived* U.S. citizens."[26]

105. The SAVE SORN also does not authorize or contemplate queries of records systems housed at SSA. It only states that the system may contain certain records sourced from SAVE user agencies, DHS systems, three immigration-related records systems housed at the State Department, and one immigration-related records system housed at DOJ.[27]

106. Similarly, SSA's operative SORN for its "Master Files of Social Security Number (SSN) Holders and SSN Applications" does not authorize or contemplate SSA data being pooled into USCIS's SAVE system.[28]

107. While the SAVE SORN says the system will contain certain immigration-related "[r]ecords … obtained from" other federal agencies (not including SSA),[29] nothing in the SORN purports to allow *directly linking* DHS and non-DHS federal agency systems of records or automated data pooling across federal agencies.

108. Neither the SAVE SORN nor the SAVE PIA authorize, contemplate, or assess the privacy implications or reliability of using the SAVE system for bulk searches of thousands of individuals' records housed within DHS or at external agencies—whether for voter verification or other purposes. Rather, the SAVE PIA outlines a three-step verification process for conducting individualized queries of a single "applicant."[30]

---

[26] SAVE PIA, *supra* n.19, at 2 (emphasis added); *see also* SAVE SORN, *supra* n.24, at 31801 ("individuals who have been granted naturalized or derived U.S. citizenship").
[27] SAVE SORN, *supra* n.24, at 31802.
[28] *See* Privacy Act Notice of Modified System of Records, 90 Fed. Reg. 10025 (Feb. 20, 2025).
[29] SAVE SORN, *supra* n.24, at 31802.
[30] SAVE PIA, *supra* n.19, at 3-4.

109. Apart from a generic authorization to use SAVE for "any other lawful purpose," the SAVE SORN does not explicitly authorize or contemplate using SAVE for voter registration or voter list maintenance purposes.

110. Consistent with the SAVE SORN and SAVE PIA, a "fact sheet" on USCIS's website previously stated (as late as April 26, 2025) that "SAVE does not verify U.S. born citizens under any circumstances," that "SAVE does not access databases that contain U.S.-born citizen information (for example, birth certificate databases)," and that "SAVE cannot verify an individual's naturalized or acquired citizenship status using a Social Security Number."[31]

2. Defendants "overhaul" SAVE by turning it into an interagency system that directly queries SSA records systems and allows bulk searches of millions of Americans' sensitive data

111. Pursuant to the Elections EO, DHS, USCIS, and DOGE announced on April 22, 2025, that they were unilaterally transforming the SAVE system to "ensure government officials can swiftly verify legal status, halting entitlements and voter fraud."[32] They described this transformation as an "overhaul" of SAVE that "breaks down silos for accurate results, streamlines mass status checks, and integrates criminal records, immigration timelines, and addresses," and that it will include "[a]utomatic status updates" to user agencies.[33]

112. On May 22, 2025, Defendants consummated the overhaul of SAVE into what they call "a single, reliable source for verifying immigration status and U.S. citizenship nationwide."[34]

113. The overhauled SAVE system has at least two new major functionalities.

---

[31] *Voter Registration and Voter List Maintenance Fact Sheet*, USCIS (Jan. 24, 2025), https://perma.cc/QW29-JZK8 (captured on Apr. 26, 2025) ("Archived SAVE Fact Sheet").

[32] Press Release, *DHS, USCIS, DOGE Overhaul Systematic Alien Verification for Entitlements Database*, DHS (Apr. 22, 2025), https://perma.cc/Y8A5-YX3M.

[33] *Id.*

[34] Press Release, *USCIS Deploys Common Sense Tools to Verify Voters*, USCIS (May 22, 2025), https://perma.cc/HBZ5-RW2E.

114. First, user agencies can now "input Social Security numbers" to "help verify U.S. citizenship," based on a "new partnership with the Social Security Administration" and USCIS.[35]

115. USCIS explained that "[t]his new partnership … allows cases to verify citizenship or immigration status to be created using Social Security numbers rather than a DHS identifying number, which most state and local agencies do not collect."[36]

116. Second, "for the first time, agencies can submit more than one case at a time," using a new bulk upload function that allows searches of potentially "millions" of individuals' records in a single query.[37]

117. On or about June 5, 2025—*i.e.*, after Defendants overhauled the SAVE system—Defendants confirmed that the SAVE system is "subject to the Privacy Act of 1974 (5 U.S.C § 552a)," and still subject to its operative SORN, "System of Records Notice DHS/USCIS-044 Systematic Alien Verification for Entitlements (SAVE) Program System of Records, May 27, 2020, 85 Fed. Reg. 31798."[38]

118. On or around June 13, 2025, USCIS made significant changes to the above-referenced SAVE "fact sheet" to reflect that the overhauled SAVE interagency system can now "verify U.S.-born citizens for voter verification agencies."[39] It made additional changes to the fact sheet on August 27, 2025.[40]

---

[35] *Id.*

[36] *Id.*

[37] *Id.*; *see also* Jonathan Shorman, *Trump wants states to feed voter info into powerful citizenship data program*, Stateline (Aug. 15, 2025), https://perma.cc/A9ZU-SEKH.

[38] *SAVE User Reference Guid*e Ch. 1.4, USCIS (June 4, 2025), https://perma.cc/DE8W-9US6.

[39] *Voter Registration and Voter List Maintenance Fact Sheet*, USCIS (June 13, 2025), https://perma.cc/XCG8-V88X.

[40] *Voter Registration and Voter List Maintenance Fact Sheet*, USCIS (Aug. 27, 2025), https://perma.cc/PP4H-T7CK ("Updated SAVE Fact Sheet").

119. The current fact sheet explains that, unlike the prior version of SAVE, users can now "create[] a case using an SSN," at which point "*SAVE first queries SSA databases*."[41] "Based on *SSA data*, SAVE can verify the U.S. citizenship of most U.S.-born individuals as well as check the SSA Death Master File."[42]

120. While the prior fact sheet said that SAVE could verify citizenship "if found in *DHS records*,"[43] the new fact sheet says that the overhauled SAVE system "can verify U.S. citizenship *based on SSA* or DHS records."[44]

121. Thus, the overhauled SAVE system now directly links to or pools from SSA systems of records.

122. This interagency data pooling is consistent with the Election EO's directive that SSA "make available" to states "the Social Security Number Verification Service, the Death Master File, and any other Federal databases containing relevant information" for voter registration and list maintenance purposes. 90 Fed. Reg. 14005 (Mar. 28, 2025).

123. A July 17, 2025 USCIS tutorial on the overhauled SAVE system further confirms the linkage of USCIS and SSA data systems.[45] The tutorial explains that "[c]ases created with a Social Security number (SSN) are compared against Social Security Administration (SSA) records," and that "[i]f there is an error with an applicant's SSA records, user agencies should direct applicants to contact SSA to update their records."[46]

---

[41] *Id.* (emphasis added).

[42] *Id.* (emphasis added).

[43] Archived SAVE Fact Sheet, *supra* n.31 (emphasis added).

[44] Updated SAVE Fact Sheet, *supra* n.40 (emphasis added).

[45] *Tutorial: Introduction to SAVE and the Verification Process for SAVE Users*, USCIS (July 17, 2025), https://perma.cc/QLA3-P5BL.

[46] *Id.* at 25.

124. The tutorial also describes the overhauled SAVE system's new "bulk uploader" feature, which allows user agencies to query many thousands and even millions of cases in a single search, in contrast to the individualized search function of the prior SAVE system.[47]

125. On September 25, 2025, SSA published on its website a May 15, 2025 letter agreement between DHS and SSA for the overhauled SAVE system.[48] The agreement purports to authorize "information sharing" between the agencies "by matching data submitted through SAVE to SSA records in SSA's Master Files of Social Security Number (SSN) Holders and SSN Applications, System of Record Notice 60-0058, 90 Fed. Reg. 10025 (Feb. 20, 2025)."[49] The agreement adds that USCIS "will maintain information provided by SSA in its system of records entitled, 'DHS/U.S. Citizenship and Immigration Services (USCIS)-004 Systematic Alien Verification for Entitlements (SAVE) Program System of Records.'"[50]

126. Thus, Defendants' public statements confirm they have dramatically expanded the scope and functionality of the SAVE system by adding a new search-by-SSN function that pools directly from SSA data systems (not just DHS systems), by enabling queries of information on U.S.-born citizens (not just foreign-born citizens and non-citizens), and by permitting "bulk" uploads and searches of potentially millions of individuals' sensitive SSA data in a single query.

127. USCIS has also reportedly offered election officials in some states the opportunity to participate in a "soft launch" of a new feature that allows searching the overhauled SAVE system

---

[47] *Id.* at 10, 15-17; s*ee also* Shorman, *supra* n.37.

[48] Letter Agreement Providing for Information Sharing Between DHS, USCIS, and SSA Regarding Citizenship (May 15, 2025), https://www.ssa.gov/foia/resources/proactivedisclosure/2025/May%2015,%202025%20SSA-DHS-USCIS%20Agreement_Redacted.pdf (posted Sept. 25, 2025) ("DHS-SSA SAVE Agreement").

[49] *Id.* at 4.

[50] *Id.* at 5.

using "just the last four digits of voters' Social Security numbers," and plans to roll out this feature to all SAVE users.[51] The DHS-SSA SAVE Agreement allows searches by either "full or partial SSN."[52]

128. Despite undertaking this self-described "overhaul" of the SAVE system, Defendants have failed to publish a SORN, PIA, or matching agreement notice detailing that transformation, failed to solicit public comment on their actions, and failed to assess the privacy implications or risks of error posed by overhauling the SAVE system in this manner.

129. In a July 15, 2025 letter, three U.S. Senators sought information from DHS regarding the overhauled SAVE system, confirming that "DHS has not issued any of the routine and required documentation about the program's operations and safeguards or issued any public notice or notice to Congress" as required by the Privacy Act.[53] The letter requested that DHS provide by July 29 any MOAs, computer-matching agreements, PIAs, and other documentation for the overhauled SAVE system. As of September 11, the senators had received no response.[54]

3. The overhauled SAVE system utilizes unreliable SSA citizenship data

130. Experts have sounded the alarm about the unreliability and incompleteness of the SSA citizenship data the overhauled SAVE system is now ingesting and utilizing, which SSA

[51] Jude Joffe-Block & Miles Parks, *33 million voters have been run through a Trump administration citizenship check*, NPR (Sept. 11, 2025), https://perma.cc/QWL3-DCVR; A.P. Dillon, *State Board of Elections tables SAVE invitation*, N. State J. (Sept. 4, 2025), https://perma.cc/X2GM-Y88R*; see also* Marilyn Odendahl, *VOTING CASE: Morales Touts 'Proof' Of Noncitizens On Rolls, Sends Voter Info to DOJ*, Ind. Citizen (Sept. 12, 2025), https://perma.cc/44A5-DSPS; Shorman*, supra* n.37.

[52] DHS-SSA SAVE Agreement, *supra* n.48, at 5.

[53] Letter from Senators Padilla, Peters, and Merkley to Secretary Noem (July 15, 2025), https://perma.cc/3KD2-FCNQ.

[54] Joffe-Block & Parks, *33 million voters*, *supra* n.51.

"collected independently and without this sort of [data] integration in mind."[55]

131. A key limitation with SSA data is that the only citizenship data SSA possesses is provided by the individual at a single moment in time—*i.e.*, when someone applies for an SSN and the corresponding card.[56] SSA has no process for automatically updating the citizenship data it maintains, but rather relies on SSN-holders to inform SSA of any change in their status.[57]

132. SSA itself has admitted that because "the citizenship [data] SSA maintains merely represents a snapshot of the individual's citizenship status at the time of their interaction with SSA," its "records do not provide definitive information about an individual's citizenship status," and has cautioned against relying on SSA data to verify citizenship or immigration status.[58]

133. As SSA has explained, "SSA is not the agency responsible for making citizenship determinations" and "SSA is not the custodian of U.S. citizenship records."[59]

134. A 2006 audit by SSA's Office of Inspector General estimated that SSA's citizenship data inaccurately identified approximately 3.3 million U.S. citizens as non-citizens "because [they] had become U.S. citizens after obtaining their SSN" and "had not updated their records with SSA."[60]

135. SSA also lacks complete citizenship data for U.S.-born citizens born before 1981, the year SSA began consistently maintaining citizenship information.[61] According to SSA, "SSA's

---

[55] Jude Joffe-Block & Miles Parks, *The Trump administration is building a national citizenship data system*, NPR (June 29, 2025), https://perma.cc/N6ZN-8SEW.

[56] Fair Elections Ctr., *supra* n.21.

[57] *Id.*

[58] Letter from SSA Off. of Gen. Counsel to Fair Elections Ctr. 2 (July 13, 2023), https://perma.cc/KS2N-U2US.

[59] *Id.*

[60] SSA Off. of the Inspector Gen., Cong. Resp. Rep. No. A-08-06-26100, *Accuracy of the Social Security Administration's Numident File* 13 (Dec. 18, 2006), https://perma.cc/5G2J-FF4V.

[61] July 2023 SSA Ltr., *supra* n.58, at 2.

assessment of its citizenship data indicates that approximately ¼ of those records do not have an indication of citizenship present."[62]

136. Further, the Updated SAVE Fact Sheet states that USCIS cannot or will not conduct "additional verification" for queries with only an SSN and will only conduct additional verification if a DHS numeric identifier is provided by the user agency or found in querying SSA data.[63]

137. SAVE's additional verification procedures involve additional levels of manual verification conducted by USCIS employees and are "important for ensuring an accurate and complete response."[64] User agencies are required to escalate cases when prompted by SAVE or when requested by the applicant.[65]

138. However, SAVE user agencies have historically failed to comply with the additional verification procedures. A 2017 report by the U.S. Government Accountability Office ("GAO") reflects that, from approximately 2012 to 2016, "the majority of SAVE user agencies that received a SAVE response prompting them to institute additional verification did not complete the required additional steps to verify the benefit applicant's immigration status."[66]

139. USCIS has recently asserted that of the 33 million voters submitted to the overhauled SAVE system as of September 11, 2025, less than one percent have required manual additional verification.[67] Accordingly, initial queries in SAVE for as many as 300,000-plus

---

[62] *Id.* at 3.

[63] Updated SAVE Fact Sheet, *supra* n.40.

[64] U.S. Gov't Accountability Off., Rep. No. GAO-17-204, *Immigration Status Verification for Benefits: Actions Needed to Improve Effectiveness and Oversight* 17, 4 (Mar. 2017), https://perma.cc/CD6Y-48QV.

[65] *SAVE User Reference Guid*e Ch. 9.2, USCIS (July 16, 2025), https://perma.cc/DE8W-9US6.

[66] GAO-17-204, *supra* n.64, at 17-18.

[67] Joffe-Block & Parks, *33 million voters*, *supra* n.51.

registered voters have resulted in non-matches or matches that were suspected to be unreliable and not definitive, thus requiring additional, manual verification.

4. States' use of the overhauled SAVE system threatens to disenfranchise eligible voters in impending elections and subject them to unwarranted criminal investigations

140. If states rely on inaccurate SSA citizenship data to purge voters from rolls, millions of eligible voters could be wrongly disenfranchised, or face unwarranted burdens in exercising their right to vote.

141. Despite these intolerable risks, several states have already begun using the overhauled SAVE interagency system (and the unreliable SSA citizenship data pooled in it) for voter registration, voter list maintenance, and investigatory purposes.

142. According to recent reports, "more than 33 million voters" have already been run through the overhauled SAVE system.[68]

143. On May 21, 2025, the Louisiana Secretary of State's office announced Louisiana was "the first state to utilize a new voter list maintenance database from the federal Department of Government Efficiency," which "combines information on individuals' immigration status and death records."[69]

144. On September 4, 2025, the Louisiana Secretary of State announced "preliminary findings" of her investigation into alleged instances of non-citizen voting after running "names from Louisiana's voter rolls" through the overhauled SAVE system.[70] The Secretary said her office

[68] *Id*.

[69] Press Release, *Louisiana First State to Utilize New Voter List Maintenance Database*, La. Sec'y of State (May 21, 2025), https://perma.cc/MF6F-3DTU; La. Sec'y of State (@Louisiana_sos), X (May 23, 2025, 9:45 AM), https://perma.cc/92XN-5AHT (stating Louisiana was "the first state to use the new []DOGE voter list maintenance database!").

[70] Wesley Muller, *Louisiana election investigation finds 79 noncitizens have voted since 1980s,* La. Illuminator (Sept. 4, 2025), https://perma.cc/VE3G-J6VT.

"discovered 390 non-citizen registered voters in the state, with 79 voting in at least one election" since the 1980s.[71] The Secretary "acknowledged the possibility that some of her findings could be attributed to errors or outdated information."[72] She added that the 390 suspects "have been given notice we have reason to believe they are not a U.S. citizen," and that "[a]nyone who does not respond or provide proof within 21 days is removed from the rolls," and "will be referred for criminal prosecution."[73]

145. On June 5, 2025, the Texas Secretary of State announced she had "referred to the Office of [the Texas] Attorney General for investigation the names of 33 potential noncitizens who voted in the November 2024 General Election," based on information obtained from the overhauled SAVE system.[74]

146. On June 17, 2025, the Texas Attorney General confirmed he had opened investigations of the 33 potential noncitizen voters referred by the Secretary of State and likewise credited the overhauled SAVE system.[75]

147. Public records responses indicate that Texas's early use of the overhauled SAVE system has resulted in an error rate of approximately 18%.[76]

---

[71] *Id.*

[72] *Id.*

[73] Joffe-Block & Parks, *33 million voters*, *supra* n.51.

[74] Press Release, *After Gaining Access to SAVE Database, Secretary Nelson Refers Potential Noncitizen Voting Cases for Investigation*, Tex. Sec'y of State (June 5, 2025), https://perma.cc/WZ3C-FUXL.

[75] Press Release, *Attor-ney Gen-er-al Ken Pax-ton Opens Inves-ti-ga-tions into 33 Nonci-t-i-zens for Ille-gal-ly Vot-ing in the 2024 Election*, Att'y Gen. of Tex. (June 17, 2025), https://perma.cc/MC8L-6RJ4; *see also* Dep't of Gov't Efficiency (@DOGE), X (June 20, 2025, 11:24 AM), https://perma.cc/4A2X-Q3YZ (quoting press release and stating "Great work by Texas using the new (and free) federal SAVE database to ensure voter integrity!").

[76] Natalia Contreras, *As Texas Embraces Federal Immigration Database to Verify Voter Citizenship, Some Experts are Worried*, The Tex. Tribune (July 22, 2025), https://perma.cc/39FY-UVEK.

148. On July 7, 2025, Indiana announced that it had entered into an MOA with USCIS to use the overhauled SAVE system "to verify the citizenship status of individuals on Indiana's voter rolls ensuring that only eligible U.S. citizens are registered to vote in Indiana."[77]

149. On September 12, 2025, Indiana Secretary of State Diego Morales alleged that a single noncitizen had been found on the state's voter rolls based on its use of the overhauled SAVE system.[78] Morales stated that Indiana's use of the overhauled SAVE system is ongoing and that Indiana is querying SAVE using only the last four digits of individuals' SSNs.[79] Morales also said Indiana had given the one alleged noncitizen's information to the Indiana State Police and FBI for criminal investigation, and that he had turned over the state's voter rolls to DOJ.[80]

150. Virginia has used the SAVE system for voter list maintenance since at least 2014.[81]

151. Since 2013, Virginia law has mandated that the Department of Elections participate in the SAVE program "for the purposes of verifying that voters listed in the Virginia voter registration system are United States citizens," Va. Elec. Code § 24.2-404(E), and that general registrars delete from voter rolls "any voter who … is known not to be a United States citizen . . . based on information received from" SAVE, *id.* §§ 24.2-404(A)(4).

---

[77] Press Release, *Indiana Sec'y of State Diego Morales Signs Agreement with Dep't of Homeland Sec'y to Identify Noncitizens on Indiana Voter Rolls*, Ind. Sec'y of State (July 7, 2025), https://perma.cc/WJ74-9EMB; Mem. of Agreement between the Dep't of Homeland Sec'y, U.S. Citizenship and Immigration Services and Indiana Secretary of State Regarding Participation in the SAVE Program for Voter Registration and Voter List Maintenance Purposes (July 1, 2025), https://perma.cc/A6LC-9CLQ (the "Indiana SAVE MOA").

[78] Marilyn Odendahl, *VOTING CASE: Morales Touts 'Proof' Of Noncitizens On Rolls, Sends Voter Info to DOJ*, Ind. Citizen (Sept. 12, 2025), https://perma.cc/44A5-DSPS.

[79] *Id.*

[80] *Id.*

[81] Mem. of Agreement between the Dep't of Homeland Sec'y, U.S. Citizenship and Immigration Services and the Virginia State Board of Elections (March 20, 2014), https://perma.cc/UV2V-G6UT.

152. On September 12, 2025, Virginia Governor Glenn Youngkin issued an Executive Order reaffirming Virginia's commitment to using the SAVE system and instructing that, "to the maximum extent possible under state and federal law," the Virginia Department of Elections must "coordinate with the federal government through partnerships with the Department of Homeland Security."[82]

153. Governor Youngkin's Executive Order also explicitly mandates that Virginia officials utilize the overhauled SAVE system's "bulk upload" feature, stating: "The Commissioner shall continue to use the Department of Homeland Security's SAVE database to identify non-citizens on Virginia's voter list using bulk upload functionality in accordance with state law, a requirement first implemented by my administration."[83]

154. Virginia is "one of only three states in the nation that require those registering to vote to provide their full 9-digit social security number for registration,"[84] rather than just the last four digits of an SSN. This uniquely positions Virginia to use SAVE's new search-by-SSN and bulk uploader functions, which (at least currently) generally require entry of full 9-digit SSNs.[85]

155. None of the states' SAVE MOAs address the unreliability and incompleteness of SSA citizenship data or the documented risks of error posed by using it for voter verification.

[82] Va. Exec. Order No. 53, *Enhancing Security for Election Preparedness* (Sept. 12, 2025), https://perma.cc/VY8P-UZGY.

[83] *Id.*

[84] Va. Exec. Order No. 35, *Comprehensive Election Security Protecting Legal Voters and Accurate Counting* (Aug. 7, 2024), https://perma.cc/Z6SM-EJE4.

[85] Letter from DHS to Va. Dep't of Elections (June 23, 2025), https://perma.cc/XJW9-NSUB.

5. Defendants are ingesting state voter roll data through the SAVE system and incorporating it into DHS Interagency Data Systems.

156. Critically, states' SAVE MOAs make data-sharing a two-way street. The MOAs authorize, not only state agencies to access federal data, but also DHS and USCIS to "use information" *provided by the states* "for any purpose permitted by law, including, but not limited to, the prosecution of violations of Federal administrative or criminal law."[86] This includes voter rolls that state agencies upload to the SAVE system using its new "bulk uploader" function.

157. Separately, pursuant to the Elections EO, DOJ has requested voter registration lists and data about individual voters from election administrators in at least 30 states, and it reportedly plans to make similar inquiries to all states.[87] At least 10 states—including Indiana—have either provided publicly available data or given DOJ directions on how to request public data.[88] DOJ has sued Oregon, Maine, California, Michigan, Minnesota, New York, New Hampshire, and Pennsylvania for refusing to provide requested voter roll data.[89]

158. On September 12, 2025, DOJ and DHS confirmed that DOJ is sharing state voter roll information with DHS to search for non-citizens for investigatory purposes.[90] DHS stated it is

[86] USCIS, *Voter Verification Agency Sample MOA Draft* (June 9, 2025), https://perma.cc/7X59-4DF4; Indiana SAVE MOA, *supra* n.77.

[87] Devlin Barrett & Nick Corasaniti, *Trump Administration Quietly Seeks to Build National Voter Roll*, N.Y. Times (Sept. 9, 2025), https://perma.cc/SJ85-P2CE; Ali Swenson & Gary Fields, *The Justice Department seeks voter and election information from at least 19 states, AP finds*, Associated Press (Aug. 3, 2025), https://perma.cc/EC7E-7U9X.

[88] *See* Jonathan Shorman, *DOJ is sharing state voter roll lists with Homeland Security*, Stateline (Sept 12, 2025), https://perma.cc/ZU9N-GHTC.

[89] Press Release, *Justice Department Sues Oregon and Maine for Failure to Provide Voter Registration Rolls*, DOJ (Sept. 16, 2025), https://perma.cc/R5LP-CB6P; Press Release, *Justice Department Sues Six States for Failure to Provide Voter Registration Rolls*, DOJ (Sept. 25, 2025), https://perma.cc/LXA8-GZNP.

[90] Shorman, *DOJ is sharing state voter roll lists*, *supra* n.88.

using the information to "scrub aliens from voter rolls" and that the federal government is "sharing information to solve problems."[91]

159. On information and belief, Defendants are incorporating, inputting, ingesting, or otherwise utilizing this state voter roll data in connection with the overhauled SAVE system and/or other DHS Interagency Data Systems.[92] Yet Defendants have failed to publish a SORN or PIA, failed to solicit public comment, and failed to assess the privacy implications or risks of error posed by these actions.

B. Defendants unlawfully pool interagency data in the USCIS Data Lake.

160. The USCIS Data Lake is a centralized repository of large volumes of data "ingested" from disparate sources, enabling those disparate sources to be combined, analyzed, or studied together.[93]

161. The USCIS Data Lake is variously referred to as the "USCIS Enterprise Data Lake," "eCISCOR Bigdata," or "DBIS," which stands for the Data and Business Intelligence Section, the name of the program that manages the Data Lake.[94]

162. USCIS last published a PIA concerning the Data Lake on July 26, 2018. It has not published a SORN for the Data Lake, and instead "relies on the source system SORNs to cover the collection, maintenance, and use of the source system data."[95]

---

[91] *Id.*; *see* Sarah N. Lynch, *US Justice Dept considers handing over voter roll data for criminal probes, documents show*, Reuters (Sept. 9, 2025), https://perma.cc/3QT4-AW2V.

[92] *See* Joffe-Block & Parks, *33 million voters, supra* n.51*; see also* Shorman, *DOJ is sharing state voter roll lists*, *supra* n.88; Lynch, *supra* n.91.

[93] *See* Databricks, *Introduction to Data Lakes*, https://perma.cc/CG83-Y8PV.

[94] *See*, *e.g.*, U.S. General Services Administration, Predictive Lake Analytics Nextgen eXchange Services (PLANXS) II (RFI # 70SBUR25I2) (Oct. 29, 2024), https://perma.cc/L9AQ-2LGW.

[95] Dep't of Homeland Sec'y, *Privacy Impact Assessment for the Enterprise Citizenship and Immigration Services Centralized Operational Repository*, at 5 (July 26, 2018), https://perma.cc/DK5U-K249; *see also* https://perma.cc/L9AQ-2LGW.

163. Data ingested into the USCIS Data Lake is retrieved "from connected source systems" and stored as "an exact copy" within the Data Lake.[96]

164. The Data Lake's operative PIA contains a list of all the "Source Systems" for the Data Lake, and it says that the list "will be updated as systems are added or removed."[97] All of the identified source systems are housed within DHS or one of its subcomponents.

165. The data in the Data Lake is highly compartmentalized—it is typically accessed from within the source systems, and data access is subject to "access controls . . . that determine what data a user of an interconnected system can access."[98]

166. While a small number of DHS employees have "privileged system accounts" that grant them more widespread access to the Data Lake's databases, these privileges are to be used strictly "for system maintenance purposes," and USCIS policy prohibits using administrator access for browsing the Data Lake's data.[99]

167. On information and belief, over the past few months, Defendants have secretly incorporated or ingested into the Data Lake retrievable records on U.S. citizens and residents pooled from systems of records housed at different agencies and are using the Data Lake to retrieve records about individuals by unique identifier.

168. DHS has provided no notice to the public or Congress—through a SORN, matching agreement notice, or PIA—of its ongoing efforts to pool or consolidate non-DHS agency data into the Data Lake, or to cross-check non-DHS agency data against the Data Lake. Nor has DHS publicly assessed the privacy implications of expanding the Data Lake in this way.

---

[96] *Id.* at 2.
[97] *Id.* at 20.
[98] *Id.* at 10-11.
[99] *Id.*

169. Members of DOGE's DHS Immigration Task Force have been given access to a number of sensitive systems at other agencies, and on information and belief, the Data Lake now includes or will include records from the following systems:

a. **The National Directory of New Hires ("NDNH"):**[100] The NDNH is a dataset managed by HHS, stored on SSA infrastructure, containing personal and financial data on any American who has started a new job within the past two years.[101] HHS is not authorized to disclose NDNH data for immigration enforcement;[102]

b. **The Unaccompanied Children Portal ("UC Portal"):**[103] HHS hosts a database called the Unaccompanied Children Portal, containing information related to migrant children temporarily placed in HHS custody while HHS identifies a custodian within the United States to sponsor them. The UC Portal is a highly sensitive system of records that contains a variety of information about children, including "[p]hotograph[s]" of children "at various ages and/or locations," the children's "Medical Notes (examples: vaccinations, medications, doctor visit

[100] *See* Cai, *supra* n.16; Rebecca Heilweil, *DOGE granted access to naturalization-related IT systems, memo shows*, FedScoop (Apr. 2, 2025), https://perma.cc/45A9-XYYB; Defs.' Obj. & Resp. to Pls.' Requests for Exp. Disc. at 9, 11-12, *AFL-CIO v. DOL* 25-cv-339 (D.D.C., filed Apr. 18, 2025), Dkt. No. 80-5 (listing Marko Elez and Aram Moghaddassi as DOGE staff given NDNH access). DOGE Staffer Marko Elez also served on the DOGE immigration task force and was given access to NDNH.

[101] *Id.*

[102] *See* Notice of Modified System of Records, 89 Fed. Reg. 25625 (Apr. 11, 2024).

[103] *See* Defs.' Obj. & Resp. to Pls.' Requests for Exp. Disc. at 10-11, *AFL-CIO v. DOL*, 25-cv-339 (D.D.C., filed Apr. 18, 2025), Dkt. No. 80-5 (DOGE staffer Kyle Schutt given access to the UC Portal); Cai, *supra* n.16 (Schutt is on the DHS DOGE Immigration Task Force); Heilweil, *supra* n.100 (Schutt has access to the USCIS Data Lake).

details)," "Biometric Identifiers," and an additional "2,000+ data elements."[104] The Portal also contains sensitive information about the sponsors of these children, including U.S. Citizens and legal permanent residents.[105] Under the relevant SORN, the Portal's records may not be used for immigration enforcement;[106]

c. **DOL foreign worker records:**[107] The Department of Labor hosts the Foreign Labor Certification System and Employer Application Case Files (collectively, "Foreign Worker Databases"), which stores records related to foreign workers approved to work in the United States.[108] The Foreign Worker Databases include a variety of sensitive PII on employers as well as U.S. citizen workers who applied for particular positions.[109] DOL is not authorized to transfer records from the Foreign Worker Databases to DHS for open-ended immigration enforcement purposes.[110]

170. In addition, DHS under the current administration has executed data sharing agreements with a number of agencies which, on information and belief, has resulted or will result

[104] U.S. Dep't of Health and Human Servs., *Privacy Impact Assessment*, Unaccompanied Children Portal (May 22, 2024), https://perma.cc/7YUA-DFTR.

[105] *See* Notice of Modified System of Records, 89 Fed. Reg. 100500 (Dec. 12, 2024).

[106] *Id*.

[107] *See* Cai, *supra* n.16; Heilweil, *supra* n.100 (Aram Moghaddassi is a member of the DHS DOGE Immigration Task Force); Leah Feiger & Vittoria Elliott, *DOGE Has Access to Sensitive Labor Department Data on Immigrants and Farm Workers*, Wired (Apr. 18, 2025), https://perma.cc/QC6G-ESEQ (Aram Moghaddassi has been granted access to the Foreign Worker Databases).

[108] *See* Notice of Modified System of Records, 87 Fed. Reg. 8292 (2022).

[109] *Id.*

[110] *See* 87 Fed. Reg. at 8294.

in the incorporation into the USCIS Data Lake of records from the following agencies, among others:

a. SSA,[111] where one DOGE staffer reportedly told SSA employees that DOGE planned to link various sources of SSA data with the goal of "joining all data across government."[112] SSA is not authorized to bulk transfer this data to be copied into DHS records.[113]

b. The IRS, from whom DHS has requested the addresses of 7.3 million taxpayers pursuant to a Memorandum of Understanding ("MOU"), resulting in the forced departure of IRS's acting general counsel after he refused the request.[114] Notably, even prior to the DHS-IRS MOU, DHS was reportedly pooling IRS data in the USCIS Data Lake. According to a DHS employee, DHS is "trying to amass a huge amount of data. It has nothing to do with finding fraud or wasteful spending … They are already cross-referencing immigration with SSA and IRS as well as voter data;"[115]

c. The Centers for Medicare and Medicaid Services ("CMS") at HHS, which has transferred millions of Medicaid enrollees' personal data to DHS, even after

[111] Kelly & Elliott, *supra* n.17 (reporting DHS's incorporation of SSA data into the USCIS data lake); Heilweil, *supra* n.100 (Mr. Moghaddassi is a member of the DHS DOGE Immigration Task Force); Social Sec'y Admin., *Social Security Announces Executive Leadership Team* (Sept. 3, 2025), https://perma.cc/T35X-E3YB (Mr. Moghaddassi has been appointed a Chief Information Officer at SSA).

[112] Natanson, *supra* n.17.

[113] Privacy Act Notice of Modified System of Records, 90 Fed. Reg. 10025 (Feb. 20, 2025); Proposed Routine Use, 75 Fed. Reg. 82121 (Dec. 29, 2010).

[114] William Turton, Christopher Bing, & Avi Asher-Schapiro, *The IRS is Building a Vast System to Share Millions of Taxpayers' Data with ICE*, ProPublica (July 15, 2025) https://perma.cc/BZG6-TZLY.

[115] Kelly & Elliott, *supra* n.17.

> CMS officials tried to block the data transfer based on concerns that the information sharing violated the Privacy Act.[116]

171. Finally, as alleged above, Defendants have collected and are collecting data on voters from several states. On information and belief, that data has been or will be ingested in the Data Lake and cross-referenced and combined with biometric data already housed by USCIS.[117]

172. Taken together, the actions above show that Defendants dramatically expanded the scope and functionality of the USCIS Data Lake. But Defendants have failed to publish a SORN, PIA, or matching agreement notice detailing the overhauled Data Lake, failed to solicit public comment on these actions, and failed to publicly assess the privacy implications of expanding the Data Lake in this manner.

173. Amid this flurry of activity, DHS shuttered its internal offices of privacy experts who would normally advise the agency about its legal obligations and conduct oversight. In March 2025, DHS effectively eliminated the Office for Civil Rights and Civil Liberties, USCIS's Ombudsman's Office, and the Office of the Immigration Detention Ombudsman, ordering the offices' employees to stop work ahead of their eventual termination because the offices "obstructed immigration enforcement."[118]

174. In sum, Defendants are rapidly building an unprecedented, unauthorized web of Interagency Data Systems in defiance of multiple laws, in secret, and without the internal functions or oversight staff that would normally advise DHS to respect privacy rights.

---

[116] Kimberly Kindy & Amanda Seitz, *Trump administration gives personal data of immigrant Medicaid enrollees to deportation officials*, Associated Press (June 14, 2025), https://perma.cc/3BVZ-DKBN.

[117] *See* Elections EO, 90 Fed. Reg. 14005; Kelly & Elliott, *supra* n.17.

[118] Ximena Bustillo, *Homeland Security makes cuts to civil rights and immigration oversight offices*, NPR (Mar. 21, 2025), https://perma.cc/KC7R-P8G2.

INJURIES TO PLAINTIFFS

Injuries to Individuals

175. The Individual Plaintiffs and members of LWVVA, LWVLA, and EPIC reasonably fear, and are emotionally distressed by, the aggregation and potential mishandling and misuse of their sensitive personal data. None of them consented to the pooling of troves of their personal information into Interagency Data Systems for undefined and potentially broad-ranging purposes, and without protection against abuse. They entrusted their personal information to federal agencies for particular, defined purposes, in reliance on longstanding privacy guarantees under federal law and the reasonable expectation that their sensitive information would not be secretly aggregated, repurposed, and made broadly accessible through insecure means to other federal and state actors and third parties.

176. The unlawful aggregation of the personal information of the Individual Plaintiffs and organizational members has caused and will continue to cause them significant unease and fears about the examination of their sensitive data by those who have accessed and will access it, the misuse and repurposing of their data by the government in unauthorized ways, the increased vulnerability of their data to theft and security breaches, and the increased risk that their data will be used to examine their private affairs and subject them to unwarranted investigations or impediments to their fundamental right to vote.

177. Individual Plaintiffs and organizational members have also been deprived of critical information in SORNs and matching agreement notices to which they are statutorily entitled. For instance, the Individual Plaintiffs and members do not know the precise purposes for which Defendants are using the personal records being pooled and made accessible via centralized queries; the policies and practices Defendants are following (if any) to store, control access to,

retain, and dispose of the data being consolidated; the procedures (if any) to ensure that interagency data-matching is technically secure and results in accurate and verified records; the procedures through which they can request to be notified if the Interagency Data Systems contain records pertaining to them; or the procedures to contest, correct, or update the contents of any such records. All of this information, and other related information, should have been provided to the Individual Plaintiffs through SORNs and matching agreement notices *before* Defendants established the Interagency Data Systems.

178. Without the SORN and matching agreement information guaranteed to them by law, the Individual Plaintiffs and organizational members cannot adequately understand how their personal data is being aggregated, repurposed, and pooled across the government; take steps to safeguard their privacy interests; or protect themselves against any attendant consequences to their personal lives, careers, or civic engagement. Deprivation of this information also impairs the individuals' abilities to exercise their rights under the Privacy Act to submit appropriately targeted requests to access or correct their own records.

179. Individual Plaintiffs and organizational members are also being deprived of required accountings of how their information is disclosed to any person or agency from the Interagency Data Systems. To Plaintiffs' knowledge, Defendants have not created any required accountings of disclosures from the Interagency Data Systems for any individual—including accountings of disclosures of their personal information to state agencies for purposes of voter list maintenance or law enforcement investigations. Individual Plaintiffs and organizational members have further been deprived of their ability to understand the details of any disclosure of their records because they lack the requisite information (from SORNs and matching agreements) to be able to submit an appropriately targeted accounting-of-disclosures request.

180. The Individual Plaintiffs and EPIC members have further been deprived of their right to comment on Defendants' data-pooling efforts through the Interagency Data Systems, and the right to have those comments considered. They have had no opportunity to participate in the process—which has been carried out in secret, rather than through the Privacy Act's public procedures—for determining how their personal data is being collected, aggregated, and used on a massive scale. They have been denied the opportunity to convey their significant and concrete privacy concerns about Defendants' unprecedented data-pooling efforts and their proposals for how Defendants can ensure their sensitive personal information is kept secure and not misused, and that data matching is accurate and verified.

181. Moreover, the Individual Plaintiffs and organizational members in states using the overhauled SAVE system for voter list maintenance and investigatory purposes reasonably fear that the system will cause them to be disenfranchised, face obstacles to voting, or be subjected to unwarranted criminal investigations, imperiling their fundamental right to vote.

182. As detailed above, the unlawfully expanded SAVE system now incorporates unreliable SSA citizenship data, and states such as Louisiana, Virginia, and Texas are using this incomplete and often-outdated data to systematically purge voter rolls and open criminal investigations of purported non-citizens for alleged illegal voting. These ongoing purges and investigations caused by the SAVE system, and additional ones in the offing as the Trump administration continues to encourage states to use the overhauled SAVE system for voter verification, place the naturalized citizen Individual Plaintiffs and organizational members (including both naturalized citizens and U.S.-born citizens) at risk of being improperly purged from state voter rolls based on faulty SSA data, and of being wrongfully investigated for illegal voting.

183. The harm to these voters is compounded by looming election deadlines. Virginia and Texas both have major elections on November 5, 2025,[119] and Louisiana has local primaries in October, with a municipal election in New Orleans on November 15.[120] Early voting is already underway in Virginia and Louisiana and fast approaching in Texas.

184. These voters now must constantly re-check their voter registration status, may need to provide additional documentation to both state and federal agencies or face other burdens in order to exercise their right to vote, and are intimidated by the overhauled SAVE system and the threat of unwarranted investigation and prosecution.

Injuries to EPIC

185. EPIC's mission is to secure the fundamental right to privacy in the digital age for all people through advocacy, research, and litigation. Among other activities, EPIC monitors, analyzes, and educates the public about the collection, use, retention, and transfer of personal information by federal agencies. EPIC routinely submits comments on SORNs published in the Federal Register and other proposed agency actions related to information databases and mobilizes its members and partners to do the same.

186. For decades, EPIC has relied extensively on information that the Privacy Act and E-Government Act mandate agencies to disclose, including information in SORNs, matching agreements, and PIAs. These documents are often the only publicly available records of how and why a federal entity is collecting personal information, what information is being collected, what burdens collection will impose, how that information may be used and shared, how it will be stored

[119] *Upcoming Elections*, Va. Dep't of Elections, https://perma.cc/QB37-EPJ4; *Important Election Dates*, Tex. Sec'y of State, https://perma.cc/SYA8-9P2Z.

[120] *Get Election Information*, La. Sec'y of State, https://perma.cc/S99M-8GRE; *2025 Lafayette Parish Elections*, Lafayette Par. Clerk of Ct., https://perma.cc/S8VG-FA3R.

and secured, and for how long it will be retained. EPIC depends on this public information to inform its research, advocacy, public education, and education of its members concerning the systems and databases used throughout the government. EPIC further relies on this information to craft targeted Freedom of Information Act requests for agency records. EPIC's ability to perform these mission-critical functions is directly impaired by Defendants' failure to publish SORNs, matching agreements, and other information concerning the Interagency Data Systems required to be disclosed by statute.

187. EPIC has also been denied statutorily guaranteed opportunities to comment on the creation of the Interagency Data Systems, to raise the privacy and security risks attendant to the federal government housing and consolidating such large volumes of personal information from so many individuals (including EPIC's members), and to offer potential solutions to safeguard sensitive personal information in a manner that could be constructive to Defendants' policy goals while protecting privacy rights.

188. Because of Defendants' failure to disclose information required by statute, EPIC must expend resources on more burdensome methods of research and information gathering, including time-intensive FOIA requests, and likely litigation, to attempt to obtain timely access to relevant records, none of which is a substitute for the unique information Defendants have failed to create and publish as required by the Privacy Act.

Injuries to LWV, LWVVA, and LWVLA

189. The League Plaintiffs' core mission is to empower voters and defend democracy, including by registering voters and increasing voter participation. The League Plaintiffs seek to increase the number of registered voters and voter participation in elections, and they accomplish this mission by providing voter outreach, education, and assistance not just to U.S.-born citizens,

but also to naturalized and derived citizens. The League Plaintiffs specifically provide voter outreach and education to assist naturalized citizens in checking their voter registration and encouraging and helping them to register or re-register.

190. When voters are unlawfully purged from voter rolls in any of the 50 states or the District of Columbia—all of which contain Leagues and members (including Virginia and Louisiana)—it decreases the number of voters, directly undermining LWV's mission of increasing the number of registered voters and voter participation. And when voters are intimidated or must take additional steps to register or remain registered, it directly harms LWV's mission of ensuring that the ballot box is accessible for all eligible voters in Virginia, Louisiana, and every other state and D.C.

191. The overhauled SAVE interagency system inflicts these very harms to LWV's core mission. Because the overhauled SAVE system utilizes SSA citizenship data that SSA itself has acknowledged is incomplete and unreliable, it directly undermines LWV's voter-registration and voter-education mission by threatening swaths of naturalized citizen voters—potentially millions—to be erroneously disenfranchised, face additional obstacles to voting, and be subjected to baseless criminal investigations into their lawful voting. The overhauled SAVE system's outdated and unreliable citizenship data risks impairing eligible naturalized citizens' ability and willingness to register and vote, frustrating LWV's mission-critical functions of educating, empowering, and encouraging them to register and vote, and providing services to facilitate their registration and voting. Additionally, the U.S.-born citizens that LWV assists with voter registration face similar risks, due to SSA's admitted gap in citizenship data for those born before 1981.

192. The League Plaintiffs are further harmed by the lack of SORN and matching-agreement information for the overhauled SAVE interagency system, and by the denial of notice-and-comment required by the Privacy Act. This vital information and opportunity for public comment would help the League Plaintiffs fulfill their core mission of protecting voters, including their own members, nationwide.

193. For example, the League Plaintiffs lack SORN information on the exact parameters of the overhauled SAVE system's uses for voter roll verification; the sources of the data pooled in that system; the policies and practices for records retrieval; the procedures for voters to access records contained in the system and contest or correct their contents; and other steps voters can take to ensure their government records are accurate, up-to-date, and secure. Without this basic information, the League Plaintiffs are kept in the dark about exactly how voters' information has been pooled across agencies and the magnitude of the risks to eligible naturalized and U.S.-born citizen registrants and voters, and the League Plaintiffs cannot properly educate the public or their members about these risks and how to mitigate them.

194. Likewise, without notice and the opportunity to comment, the League Plaintiffs cannot raise critical concerns about the accuracy of the SSA data now being pooled into the overhauled SAVE system and offer recommendations to ensure eligible voters are not wrongfully purged from voter rolls or investigated based on stale and inaccurate SSA data.

CLASS ACTION ALLEGATIONS

195. Proposed Class Representatives—Plaintiffs J. Does 1, 2, 3, 4, and 5—bring this action under Federal Rules of Civil Procedure 23(a) and 23(b)(2) on behalf of themselves and all other persons similarly situated.

196. Plaintiffs seek to represent the following class: All United States citizens and lawful

permanent residents whose records containing their Personally Identifiable Information are contained in the Interagency Data Systems, whose PII originated from a federal agency other than DHS or its subcomponents, and who did not consent to that PII being shared with DHS (the "Proposed Class.").

197. Plaintiffs J. Does 1, 4, and 5 also seek to represent, including for purposes of a forthcoming motion seeking preliminary relief, a subclass of the Proposed Class, consisting of: All naturalized citizens whose records within Social Security Administration databases do not accurately reflect their U.S. citizenship status, and who reside in jurisdictions using DHS's overhauled SAVE system for activities relating to voter registration and voter roll list maintenance (the "Proposed Preliminary Relief Subclass").

198. The Proposed Class is so numerous that joinder of all members is impracticable. *See* Fed. R. Civ. P. 23(a)(1). On information and belief, Defendants have unlawfully transferred records, copied, or otherwise incorporated records containing the PII of millions of U.S. citizens and lawful permanent residents into new Interagency Data Systems housed at DHS.

199. The Proposed Class's claims turn on common questions of fact or law that are capable of class-wide resolution. *See* Fed. R. Civ. P. 23(a)(2). The legality of Defendants' hasty consolidation of cross-government records, without statutory authority and without complying with the Privacy Act's protections, is a common question that is the same for all Class members.

200. The Proposed Class Representatives' claims are typical of the claims of the Proposed Class. *See* Fed. R. Civ. P. 23(a)(3). Each Class member's claims arise from the same course of events: Defendants' consolidation of cross-government records into Interagency Data Systems housed at DHS. And each class member will experience the same injuries (injuries to their privacy, deprivation of information and the opportunity to weigh in about how their personal information is used, and a breach of confidence by government stewards) if relief is denied.

201. The Proposed Class Representatives will fairly and adequately represent the Proposed Class. *See* Fed. R. Civ. P. 23(a)(4). The Proposed Class Representatives are committed to seeking declaratory and injunctive relief that will benefit all members of the Proposed Class equally, removing their data from unlawful Interagency Data Systems and ensuring transparency concerning the use of their data. They are aware of their obligations as Proposed Class Representatives and willing to dedicate time and effort to pursuing the interests of the Proposed Class.

202. The Proposed Class Representatives are represented by counsel with extensive experience in administrative law and class actions, who are committed to zealously representing the Proposed Class. *See* Fed. R. Civ. P. 23(a)(4), 23(g).

203. Defendants have acted or refused to act on grounds that apply generally to the Proposed Class, creating Interagency Data Systems using the same unlawful procedures and without legal basis. Injunctive relief and a corresponding declaratory judgment regarding the legality and enforceability of that decision is therefore appropriate with respect to the Proposed Class as a whole. *See* Fed. R. Civ. P. 23(b)(2).

CLAIMS FOR RELIEF

COUNT ONE
Violation of the APA (Privacy Act)
Agency Action Contrary to Law and Required Procedure, 5 U.S.C. § 706(2)

204. Plaintiffs repeat and incorporate by reference each of the foregoing allegations as if fully set forth herein.

205. The APA requires courts to "hold unlawful and set aside agency action" that is "not in accordance with law," 5 U.S.C. § 706(2)(A), "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right," *id.* § 706(2)(C), or "without observance of procedure required by law," *id.* § 706(2)(D).

206. Defendants' establishment and operation of the Interagency Data Systems are "final agency action[s] for which there is no other adequate remedy in a court," within the meaning of the APA. *Id.* § 704.

207. By establishing and operating the Interagency Data Systems, Defendants have established and significantly changed "system[s] of records" containing information about individuals that is retrieved by unique identifier. *Id.* § 552a(a)(5).

208. The Interagency Data Systems are prohibited by the Privacy Act. They constitute prohibited "national data bank[s] that combine[], merge[], or link[] information on individuals maintained in systems of records by other Federal agencies"; prohibited mechanisms that "direct[ly] link … computerized systems of records maintained by Federal agencies"; and/or prohibited "computer matching[s] of records not otherwise authorized by law." Pub. L. 100-503, § 9, 102 Stat. at 2514.

209. Defendants also established and are operating the Interagency Data Systems without complying with any of the Privacy Act's basic protections, including its non-discretionary "[r]equirements" for "system[s] of records." 5 U.S.C. §§ 552a(e)(1)-(12).

210. Defendants established and are operating the Interagency Data Systems without first publishing a SORN or soliciting public comment on any new use or intended use of information pooled in the Interagency Data Systems, in violation of the Privacy Act. *See id.* § 552a(e)(4), (e)(11).

211. By establishing and operating the Interagency Data Systems, Defendants have established and significantly changed "computer matching program[s]" without first executing, notifying the public about, and soliciting public comment on any "matching agreements" for the Interagency Data Systems, in violation of the Privacy Act. *See id.* §§ 552a(o)(1), (e)(12).

212. On information and belief, Defendants have failed to create accurate "accounting[s]" of disclosures relating to the Interagency Data Systems in accordance with the Privacy Act. *See id.* § 552a(c).

213. Defendants have failed to establish "appropriate … safeguards" for the Interagency Data Systems "to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained" in accordance with the Privacy Act. *See id.* § 552a(e)(10); *see also id.* §§ 552(e)(5)-(6).

214. Accordingly, Defendants' establishment and operation of the Interagency Data Systems are "not in accordance with law," 5 U.S.C. § 706(2)(A), "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right," *id.* § 706(2)(C), and "without observance of procedure required by law," *id.* § 706(2)(D).

COUNT TWO
Violation of the APA (Privacy Act)
Agency Action Unlawfully Withheld or Unreasonably Delayed, 5 U.S.C. § 706(1)

215. Plaintiffs repeat and incorporate by reference each of the foregoing allegations as if fully set forth herein.

216. The APA requires courts to "compel agency action unlawfully withheld or unreasonably delayed." 5 U.S.C. § 706(1).

217. Prior to establishing and operating the Interagency Data Systems, the Privacy Act required Defendants to publish SORNs and matching agreement notices in the Federal Register and provide opportunity for public comment, *id*. §§ 552a(e)(4), (11), (12), 552a(o); create accurate "accounting[s]" of disclosures relating to the Interagency Data Systems, *id.* § 552a(c); and "establish appropriate … safeguards" for the systems, *id.* § 552a(e)(10); *see id.* §§ (e)(5)-(6).

218. By failing to take any of these actions, Defendants have "unlawfully withheld or unreasonably delayed" agency action. 5 U.S.C. § 706(1).

COUNT THREE
Violation of the APA
Arbitrary and Capricious Agency Action, 5 U.S.C. § 706(2)

219. Plaintiffs repeat and incorporate by reference each of the foregoing allegations as if fully set forth herein.

220. The APA requires courts to "hold unlawful and set aside agency action" that is "arbitrary" and "capricious." 5 U.S.C. § 706(2)(A).

221. Defendants' establishment and operation of the Interagency Data Systems are arbitrary and capricious because, among other things, Defendants failed to engage in reasoned decisionmaking or reasonably explain their actions; failed to conduct a PIA or otherwise consider the privacy implications of their actions; failed to conduct a FISMA assessment or otherwise consider the data security risks of their actions; failed to consider the reliance interests and

reasonable privacy expectations of the millions of Americans who never consented to their personal data being pooled and repurposed as Defendants have; failed to consider whether the data they are pooling is sufficiently reliable to fulfill the new purposes for which it is being used and the attendant risks of error; failed to consider reasonable alternatives; and failed to acknowledge or explain their departure from longstanding executive branch policies.

COUNT FOUR
Violation of Non-Discretionary Official Duties
Mandamus, 28 U.S.C. § 1361

222. Plaintiffs repeat and incorporate by reference each of the foregoing allegations as if fully set forth herein.

223. "The district courts shall have original jurisdiction of any action in the nature of mandamus to compel an officer or employee of the United States or an agency thereof to perform a duty owed to the plaintiff." 28 U.S.C. § 1361.

224. As alleged above in paragraphs 204 through 218, the Privacy Act imposes non-discretionary, official duties on Defendants with respect to the establishment and operation of systems of records.

225. As alleged above in paragraphs 204 through 218, Defendants have violated each of these non-discretionary, official duties under the Privacy Act through their establishment and operation of the Interagency Data Systems.

226. As alleged above in paragraphs 204 through 218, Plaintiffs have a clear and indisputable right to relief from Defendants' Privacy Act violations.

227. If the Court finds that the APA does not authorize any of the relief sought herein, mandamus is Plaintiffs' only adequate remedy, and there are compelling equitable grounds for issuing the writ.

228. Plaintiffs are therefore entitled to a writ of mandamus compelling Defendants to comply with their non-discretionary duties under the Privacy Act.

COUNT FIVE
Ultra Vires

229. Plaintiffs repeat and incorporate by reference each of the foregoing allegations as if fully set forth herein.

230. Non-statutory *ultra vires* review is available when an agency takes action "entirely in excess of its delegated powers and contrary to a specific prohibition in a statute," unless a statutory review scheme "provides aggrieved persons with a meaningful and adequate opportunity for judicial review" or "forecloses all other forms of judicial review." *Nuclear Regul. Comm'n v. Texas*, 605 U.S. 665, 681 (2025) (cleaned up).

231. To the extent any statutes arguably authorize Defendants to combine certain specific data systems for particular purposes, they do not authorize Defendants to combine, consolidate, link, and analyze highly sensitive personal data stored in disparate agency systems of records across the government for new purposes unrelated to the reasons for the data's collection.

232. Quite the opposite, the Privacy Act explicitly *prohibits* interagency national data banks. *See* 5 U.S.C. § 552a note. And the other provisions of the Privacy Act establish specific prerequisites to creating any system of records—which Defendants have defied.

233. By establishing and operating the Interagency Data Systems, Defendants are acting "entirely in excess" of whatever powers have been delegated to them by Congress, and "contrary to [] specific prohibition[s]" in multiple statutes, including the Privacy Act, E-Government Act, and FISMA. *See Nuclear Regul. Comm'n*, 605 U.S. at 681.

234. Defendants' actions are therefore *ultra vires* and unlawful.

COUNT SIX
Violation of the Separation of Powers

235. Plaintiffs repeat and incorporate by reference each of the foregoing allegations as if fully set forth herein.

236. The Constitution authorizes private Plaintiffs "to sue to enjoin unconstitutional actions by state and federal officers." *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320, 327 (2015).

237. "Federal agencies are creatures of statute. They possess only those powers that Congress confers upon them. If no statute confers authority to a federal agency, it has none." *Judge Rotenberg Educ. Ctr., Inc. v. FDA*, 3 F.4th 390, 399 (D.C. Cir. 2021).

238. No statute gives Defendants authority to establish an interagency national data bank, let alone one for determining the citizenship of voters and voter registrants. *See* 5 U.S.C. § 552a note.

239. Nor does the Executive Branch possess any constitutional authority over elections. The Constitution's "Elections Clause provides that Congress—not the President—is the check on States' authority to regulate federal elections." *League of United Latin Am. Citizens v. Exec. Off. of the President*, 780 F. Supp. 3d 135, 194 (D.D.C. 2025); *see* U.S. Const. art. I, § 4, cl. 1.

240. Defendants have therefore violated the separation of powers by establishing and operating the Interagency Data Systems.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

1) Declare Defendants' decisions to establish and operate the Interagency Data Systems unlawful, arbitrary and capricious, *ultra vires*, and unconstitutional;

2) Stay and vacate Defendants' decisions to establish and operate the Interagency Data Systems;

3) Enter a preliminary and/or permanent injunction against Defendants and all others within the scope of Federal Rule of Civil Procedure 65(d)(2), or alternatively issue a writ of mandamus:

   a) requiring them to return the Interagency Data Systems to their prior operational state before Defendants unlawfully established and significantly changed them;

   b) prohibiting them from operating the Interagency Data Systems beyond the scope and functionality authorized by the Privacy Act and their operative SORNs;

   c) prohibiting them from pooling interagency records into or through the Interagency Data Systems without statutory authorization;

   d) prohibiting them from using data unlawfully pooled into or made available through the Interagency Data Systems;

   e) requiring them to delete, disentangle, and unlink non-DHS Defendant agencies' data unlawfully pooled into or made available through the Interagency Data Systems;

   f) requiring them to publish systems of records notices in the Federal Register disclosing what data was pooled into the Interagency Data Systems, for what purpose, and all other details for which the Privacy Act mandates disclosure; and

   g) granting any other temporary, preliminary, or permanent injunctive relief necessary to prevent Defendants' actions from irreparably harming Plaintiffs.

4) Award Plaintiffs their costs and reasonable attorneys' fees incurred in this action; and

5) Grant any other relief this Court deems just and proper.

Dated: September 30, 2025

Respectfully Submitted,

/s/ Nikhel S. Sus
Nikhel S. Sus (D.C. Bar No. 1017937)
John B. Hill (N.Y. Bar No. 5505508)*
Lauren C. Bingham (Fl. Bar No. 105745)*
Yoseph T. Desta (DC Bar No. 90002042)
CITIZENS FOR RESPONSIBILITY AND ETHICS IN WASHINGTON
P.O. Box 14596
Washington, D.C. 20044
Telephone: (202) 408-5565
Fax: (202) 588-5020
nsus@citizensforethics.org
jhill@citizensforethics.org
lbingham@citizensforethics.org
ydesta@citizensforethics.org

Aman T. George (D.C. Bar No. 1028446)
Jennifer Fountain Connolly (D.C. Bar No. 1019148)
Johanna M. Hickman (D.C. Bar No. 981770)
Mark B. Samburg (D.C. Bar No. 1018533)
Robin Thurston (D.C. Bar No. 1531399)
DEMOCRACY FORWARD FOUNDATION
P.O. Box 34553
Washington, D.C. 20043
(202) 448-9090
ageorge@democracyforward.org
jconnolly@democracyforward.org
hhickman@democracyforward.org
msamburg@democracyforward.org
rthurston@democracyforward.org

Jon Sherman (D.C. Bar No. 998271)*
Michelle Kanter Cohen (D.C. Bar No. 989164)
Emily Davis (D.C. Bar No. 90020129)
FAIR ELECTIONS CENTER
1825 K St. NW, Suite 701
Washington, DC 20006
202-331-0114
jsherman@fairelectionscenter.org
mkantercohen@fairelectionscenter.org
edavis@fairelectionscenter.org

*application for *pro hac vice* admission forthcoming

Counsel for All Plaintiffs

John L. Davisson (D.C. Bar No. 1531914)
Enid Zhou (D.C. Bar No. 1632392)
Abigail Kunkler (D.C. Bar No. 90030868)
ELECTRONIC PRIVACY INFORMATION CENTER
1519 New Hampshire Ave NW
Washington, D.C. 20036
Telephone: 202-483-1140
Fax: 202-483-1248
davisson@epic.org
zhou@epic.org
kunkler@epic.org

Counsel for Plaintiff Electronic Privacy Information Center