UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

COMMON CAUSE
[redacted]

COMMON CAUSE EDUCATION FUND
[redacted]

ANTHONY NEL
c/o Citizens for Responsibility and Ethics in Washington
P.O. Box 14596
Washington, DC 20044,

HALEY SMITH
c/o Citizens for Responsibility and Ethics in Washington
P.O. Box 14596
Washington, DC 20044,

LINDA DUCKWORTH
c/o Citizens for Responsibility and Ethics in Washington
P.O. Box 14596
Washington, DC 20044,

RUTH NASRULLAH
c/o Citizens for Responsibility and Ethics in Washington
P.O. Box 14596
Washington, DC 20044,

Plaintiffs,

v.

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

TODD BLANCHE, in his official capacity as Acting U.S. Attorney General
950 Pennsylvania Ave., NW
Washington, DC 20530,

Defendants.

COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF

Case No. _____

INTRODUCTION

1. The U.S. Department of Justice ("DOJ") has launched an illegal and unprecedented quest to stockpile millions of Americans' confidential voter data in a system of records within its Civil Rights Division. DOJ has demanded that nearly every state and the District of Columbia turn over their unredacted statewide voter registration lists ("Confidential Voter Lists"), which vary among states but include sensitive personal information such as Social Security numbers, driver's license numbers, signatures, dates of birth, home addresses, places of birth, political party affiliation, and voter participation history. Never before has a federal agency centralized this volume of Americans' voting data in a single system of records. And in doing so, DOJ has flouted statutory safeguards designed to ensure transparency and public participation in the federal government's collection of Americans' personal information.

2. DOJ is using this highly sensitive data to build—without statutory authorization—a sprawling new voter surveillance and purging apparatus that endangers millions of Americans' fundamental voting and privacy rights.

3. Heeding the Administration's repeated calls to "take over" and "nationalize" elections,[1] DOJ has finalized and is now implementing its mandate to compile these state voter files in order to create a national voter registration system of records (the "Voter Registration Nationalization Policy" or "the Policy"). Pursuant to this Policy, DOJ seeks to federalize voter list maintenance, a responsibility that our Constitution and federal statutes entrust to the States.

4. DOJ is executing this unprecedented Policy by moving rapidly to usurp the States' lawful authority over elections and imposing its own secretive "verification procedures" for

[1] *E.g.*, *Trump urges Republicans to 'take over' and 'nationalize' voting*, ABC7 Chicago, YouTube (Feb. 3, 2026), https://tinyurl.com/4nfv2tdt.

identifying "ineligible voters" and then requiring states to remove those individuals from their voter rolls.[2]

5. In accordance with the Policy, DOJ has told federal courts and state officials that it will run states' entire Confidential Voter Lists through the Department of Homeland Security's ("DHS") flawed Systematic Alien Verification for Entitlements ("SAVE") system.[3]

6. In 2025, DHS haphazardly expanded SAVE—which was previously a limited tool that only queried certain immigration-related databases—to conduct mass "voter verification" citizenship checks using unreliable data. The faulty new system and flawed comparison methodology has already falsely identified significant numbers of U.S. citizens as non-citizens, imperiling their fundamental right to vote. And the system has proven especially unreliable for citizens born outside of the United States (e.g., naturalized, derived, and acquired citizens),[4] who are at a higher risk of being falsely identified as non-citizens.[5]

7. In addition to making bulk disclosures to DHS, DOJ plans to disclose Confidential Voter List data to unidentified private "contractors" to assist with its "list maintenance verification

---

[2] Alaska Memorandum of Understanding with DOJ Civil Rights Division, at 4-7, https://perma.cc/Q5CQ-LELB ("Alaska DOJ MOU"); Texas Memorandum of Understanding with DOJ Civil Rights Division, at 4-7, https://perma.cc/2EDA-RF7H ("Texas DOJ MOU").

[3] Hr'g Tr. at 50:22-23, *United States v. Amore*, No. 25-cv-639 (D.R.I. Mar. 27, 2026); Letter from Kris Warner, Sec'y of State of West Virginia, to Eric Neff, Acting Chief of the Civil Rights Division Voting Section at DOJ (Feb. 11, 2026), https://perma.cc/DCA2-U5Q2 ("West Virginia Letter").

[4] Derived citizenship is "[c]itizenship conveyed to children through the naturalization of their parents or, under certain circumstances, to foreign-born children adopted by U.S. citizen parents." USCIS, *Glossary of Terms*, https://perma.cc/7SXE-ZTYT. Acquired citizenship is "[c]itizenship conferred at birth on children born abroad to a U.S. citizen parent." USCIS, *Glossary of Terms*, https://perma.cc/8AB4-9LAX.

[5] *See* Jen Fifield and Zach Despart, *"Not Ready for Prime Time." A Federal Tool to Check Voter Citizenship Keeps Making Mistakes*, ProPublica & Texas Tribune (Feb. 13, 2026), https://perma.cc/PR4Q-67NR.

procedures."[6]

8. DOJ claims that its significant misuses of the Confidential Voter List data will allow it to identify voters with supposedly "problematic registrations" on state voter rolls, and claims for itself the power to conduct its own eligibility determinations and force the removal of any such voters from the rolls.[7]

9. No federal statute authorizes DOJ's sprawling new voter surveillance, data consolidation, and purging operation. In taking these actions, DOJ is usurping powers that the Constitution and federal statutes vest in the States. DOJ has also run roughshod over the Privacy Act, the Paperwork Reduction Act ("PRA"), and the Administrative Procedure Act ("APA"), threatening millions of Americans' fundamental rights in the process.

10. Centralizing hundreds of millions of Americans' state-level voter data in a single federal system also presents major cybersecurity risks, creating a new target for hackers and malign foreign actors who seek to undermine our elections and Americans' data security.

11. Compounding the problem, DOJ has carried out this illegal operation shrouded in secrecy, flouting statutory notice-and-comment requirements designed to ensure transparency and public participation in federal agencies' collection and use of Americans' sensitive personal data.

12. Most states have resisted DOJ's unprecedented data demands. DOJ has sued 30 states and the District of Columbia to force compliance with its requests. Federal courts have dismissed five of DOJ's suits for failure to state a claim, with two holding that the agency's data demands exceed its statutory authority and violate federal and state privacy laws.[8]

---

[6] Alaska and Texas DOJ MOUs, *supra* note 2, at 7.

[7] *E.g.*, Hr'g Tr. at 109:2-14., *United States v. Amore*, No. 25-cv-639 (D.R.I. Mar. 27, 2026); Alaska and Texas DOJ MOUs, *supra* note 2, at 4-5.

[8] *See United States v. Weber*, 2026 WL 118807 (C.D. Cal. Jan. 15, 2026); *United States v. Oregon*, 2026 WL 318402 (D. Or. Feb. 5, 2026); *United States v. Benson*, 2026 WL 362789 (W.D. Mich.

13. But at least 12 and, according to DOJ, as many as 19 states have acquiesced to DOJ's demands for their Confidential Voter Lists, including Alaska, Arkansas, Indiana, Kansas, Louisiana, Mississippi, Nebraska, Ohio, Oklahoma, South Dakota, Tennessee, Texas, and Wyoming. These states have disregarded the privacy and voting rights of millions of Americans who never consented to disclosing their sensitive personal data to the federal government for undefined purposes and without statutory authorization.

14. Plaintiffs include a voting rights organization whose members' sensitive personal data has been and will be illegally centralized, used, and disclosed by DOJ without their consent, and whose voter-services and educational programs are directly harmed by DOJ's unlawful actions. Plaintiffs also include registered voters whose Confidential Voter List data was disclosed without their consent to DOJ, and who are at heightened risk of being ensnared in DOJ's illegal and unreliable voter purge apparatus.

15. Plaintiffs request that the Court hold unlawful, stay, vacate, and set aside DOJ's Voter Registration Nationalization Policy, its decisions to compile the Confidential Voter List data in a system of records, and its policies and agreements to disclose that data. Plaintiffs further seek injunctive relief prohibiting DOJ's unlawful disclosure and use of the Confidential Voter List data.

PARTIES

16. Plaintiff **Common Cause** is a nonpartisan, grassroots organization organized under the laws of the District of Columbia that has a mission of upholding the core values of American democracy. Common Cause works to create open, honest, and accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all

Feb. 10, 2026); *United States v. Galvin*, 2026 WL 972129 (D. Mass. Apr. 9, 2026); *United States v. Amore*, 2026 WL 1040637 (D.R.I. Apr. 17, 2026).

people to make their voices heard in the political process. Common Cause has nearly one million members, twenty-two state offices, and a presence in all fifty states and the District of Columbia. It has members in every congressional district. Since its founding by John Gardner 50 years ago, Common Cause has been dedicated to making government at all levels more representative, open, and responsive to the interests of ordinary people.

17. Plaintiff **Common Cause Education Fund** (the "Education Fund") was formed in 2000 as a nonprofit under the laws of the State of Delaware. The Education Fund provides education, engagement, and research to Common Cause members, constituents, partner organizations, and the public about voter registration and the electoral process. The Education Fund works to create public engagement on democracy issues and promote effective citizen participation, which is critical for a healthy and robust democratic society. Common Cause and the Common Cause Education Fund (together "Common Cause") bring this action jointly.

18. Common Cause has members in each state whose Confidential Voter List data has been and will be illegally centralized, used, and disclosed by DOJ without their consent.

19. Plaintiff **Anthony Nel** is a derived U.S. citizen[9] and resident of Denton County, Texas. He is a member of Common Cause. He regularly votes and intends to continue doing so.

20. Plaintiff Nel was born in Port Elizabeth (Gqeberha), South Africa, in 1996. He immigrated to the United States with his parents in 2004, when he was eight years old. His parents became naturalized U.S. citizens in March 2013, when he was sixteen years old. He automatically became a U.S. citizen when his parents naturalized.

[9] As noted above, a derived U.S. citizen is a foreign-born child who automatically acquires U.S. citizenship through the naturalization of their parent(s), rather than through their own application. Under the Child Citizenship Act of 2000, children under 18 with at least one U.S. citizen parent (naturalized or birth) gain citizenship automatically if they reside in the U.S. as lawful permanent residents. 8 U.S.C. § 1431 (INA 320).

21. Plaintiff **Linda Duckworth** is a resident of Nebraska and a lifelong U.S. citizen. She is a member of Common Cause and engages in voter registration and activation for her community. She has been a registered voter in Nebraska since around 2004. She regularly votes and intends to continue to do so. Plaintiff Duckworth changed her name when she got married in 1976.

22. Plaintiff **Haley Smith** is a resident of Texas and a lifelong U.S. citizen. She is a member of Common Cause and Vice Chair of Common Cause Texas's Advisory Board. She engages in voter registration as a Volunteer Deputy Registrar for Hays County. She has been a registered voter in Texas since around 2022. She regularly votes and intends to continue to do so.

23. Plaintiff **Ruth Nasrullah** is a resident of Texas and a lifelong U.S. citizen. She is a member of Common Cause. She engages in voter registration as a Volunteer Deputy Registrar for Harris and Brazoria Counties. She has been a registered voter in Texas since around 2004. She regularly votes and intends to continue to do so. Plaintiff Nasrullah has changed her name three times due to marriage and divorce.

24. Defendant **DOJ** is a federal agency within the meaning of the APA, 5 U.S.C. § 551(1), the Privacy Act, 5 U.S.C. § 552a(a)(1), and the Paperwork Reduction Act, 44 U.S.C. § 3502, that is headquartered in Washington, D.C.

25. Defendant **Todd Blanche** is the Acting U.S. Attorney General and is sued in his official capacity.

JURISDICTION AND VENUE

26. 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 APA, 5 U.S.C. §§ 701 *et seq.*

27. 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 BACKGROUND

I. The Constitution and federal statutes charge the States, not the federal government, with voter list maintenance.

28. Election administration involves two essential functions: determining who is qualified to vote and conducting elections. The Constitution and federal statutes entrust the States with both tasks.

29. "Our Constitution provides that only the States—not Congress, and certainly not the President—may decide who is qualified to vote in federal elections." *League of United Latin Am. Citizens ("LULAC II") v. EOP*, 2026 WL 252420, *42 (D.D.C. Jan. 30, 2026); *see also* U.S. Const. art. I, § 2, cl. 1 (Voter Qualifications Clause); *id.* art. II, § 1, cl. 2 (Presidential Electors Clause); *id.* amend. XII; *id.* amend. XVII. Determining voter qualifications "forms no part of the power to be conferred upon the national government," aside from upholding the federal rights to vote and be free from discrimination. *See Arizona v. Inter Tribal Council of Ariz., Inc.*, 570 U.S. 1, 17 (2013).

30. "When it comes to the procedural conduct of federal elections," the Constitution's Elections Clause "grants broad regulatory authority to the States but reserves final, supervisory authority to Congress." *LULAC II*, 2026 WL 252420, at *6; *see also* U.S. Const. art. I, § 4, cl. 1.

31. "The Constitution assigns no direct role to the President in either" the "domain[s]" of "voter qualifications" or "election procedures." *LULAC II*, 2026 WL 252420, at *5.

32. To ensure certain uniform standards for states conducting voter registration and list maintenance, Congress has passed statutes such as the National Voter Registration Act of 1993 ("NVRA") and Help America Vote Act of 2002 ("HAVA"). The NVRA "erects a complex

superstructure of federal regulation atop state voter-registration systems." *Husted v. A. Philip Randolph Inst.*, 584 U.S. 756, 761 (2018) (cleaned up). And HAVA requires, among other things, "that each state maintains a computerized database for voter registrations." *Am. C.R. Union v. Phila. City Comm'rs*, 872 F.3d 175, 180-81 (3d Cir. 2017).

33. The overarching goal of these federal statutes, as articulated by the NVRA, is for all levels of government to "promote the exercise of" the "fundamental right" to vote and prevent the "discriminatory and unfair registration laws and procedures [that] can have a direct and damaging effect on voter participation." 52 U.S.C. § 20501(a) (Congress's findings). To achieve this goal, federal law seeks "to establish procedures that will increase the number of eligible citizens who register to vote," "enhance[] the participation of eligible citizens as voters," "protect the integrity of the electoral process," and provide structures for states to "ensure that accurate and current voter registration rolls are maintained." *Id.* § 20501(b) (Congress's purpose).

34. But nowhere does the NVRA, or any federal law, contemplate a *federal takeover* of the States' voter registration processes—let alone a takeover by the *Executive branch*—and certainly not in a manner that threatens to *decrease* lawful electoral participation and harms the voters that federal law seeks to protect.

35. While the NVRA and HAVA create federal requirements, both laws explicitly charge the States—not the federal government—with their implementation, including with respect to voter list maintenance, and provide flexibility for states to carry out these requirements. *See* 52 U.S.C. §§ 20506, 20507, 20509, 21085; *see also Arizona*, 570 U.S. at 15 (addressing NVRA); *Sandusky Cnty. Democratic Party v. Blackwell*, 387 F.3d 565, 576 (6th Cir. 2004) (addressing HAVA).

36. States have robust, transparent, and effective procedures to ensure their voter rolls are accurate and in compliance with state and federal law, including ensuring only U.S. citizens are on registration lists, monitoring voters' changes of address, removing deceased voters, removing voters for lack of voting activity, removing voters who are ineligible because of criminal convictions, and removing voters adjudicated mentally incompetent.[10]

37. State and local election officials use many resources for keeping voter rolls current. Thirty states require using the U.S. Postal Service's National Change of Address ("NCOA") program, and another 15 states have access to NCOA data.[11] Twenty-five states and the District of Columbia are members of the Electronic Registration Information Center, which allows states to share motor vehicle department data through fully encrypted means and access official death data from the Social Security Administration ("SSA").[12] And several states are members of the Alabama Voter Integrity Database, which provides similar resources.[13]

38. If the federal government believes that a state is not upholding its obligations under the NVRA or HAVA, those statutes allow DOJ to file a lawsuit and have that dispute adjudicated in court. But the statutes do not authorize what DOJ is presently doing: usurping the states' role of conducting list maintenance in the first instance. Congress has not authorized the DOJ to act in that manner.

---

[10] *Voter Registration List Maintenance*, Nat'l Conference of State Legislatures (updated Oct. 21, 2025), https://tinyurl.com/39hfssap.

[11] *Id.*

[12] *FAQs*, ERIC, https://perma.cc/KW4V-VPCJ.

[13] *Alabama Voter Integrity Database*, Alabama Secretary of State, https://perma.cc/Y65U-89JZ; *AVID MOU Agreements*, Alabama Secretary of State, https://perma.cc/4PVP-KD53; *see also Interstate voter registration data matching*, MIT Election Data + Science Lab (last updated Oct. 29, 2025), https://tinyurl.com/375dnt63.

II. The Privacy Act restricts the federal government's collection, use, and disclosure of Americans' private information.

39. "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." DOJ, *Overview of the Privacy Act of 1974*, at 1 (2020 ed.), https://perma.cc/6SB9-XAEK.

40. A key objective of the Privacy Act was to prevent the government from secretly 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. Legislative History of the Privacy Act of 1974, Source Book on Privacy, at 168, 217, 884 (1976), https://perma.cc/9W9F-R5ZL ("Privacy Act Leg. History"). 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 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." *Id.*

41. The Privacy Act fulfills that purpose through a series of substantive restrictions and procedural safeguards.

42. The Act establishes safeguards "against an invasion of personal privacy by requiring Federal agencies" to "collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is for a necessary and lawful purpose," and ensuring "that adequate safeguards are provided to prevent misuses of such information." Privacy Act of 1974 § 2(b), 2(b)(4), 88 Stat. 1896 (1974), *codified at* 5 U.S.C. § 552a note.

43. The Act generally prohibits agencies from disclosing records about individuals from a system of records without the individual's consent, subject to 13 exceptions. 5 U.S.C. § 552a(b). One of those exceptions permits disclosure to those employees of the agency "which maintains the record who have a need for the record in the performance of their duties." *Id.* § 552a(b)(1). Another exception permits disclosure pursuant to a properly noticed "routine use," *id.* § 552a(b)(3), which is defined as the use of a record "for a purpose which is compatible with the purpose for which it was collected," *id.* § 552a(a)(7).

44. The Privacy Act requires that each agency that maintains a system of records take certain steps to ensure the records it "maintains" on individuals are accurate, relevant, up-to-date, and secure, *see* 5 U.S.C. §§ 552a(e)(5), (6), (10), in order to prevent "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained," *id.* § 552(e)(10). The Act defines "maintain" to include "maintain, collect, use, or disseminate." *Id.* § 552a(a)(3).

45. The Act further prohibits an agency maintaining a system of records from "maintain[ing], collect[ing], us[ing], or disseminat[ing]" "record[s] describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." *Id.* §§ 552a(a)(3), (e)(7).

46. Additionally, 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" nine categories of

information concerning the system's contents, functions, uses, and procedures for individuals to access and correct records about themselves. *Id.*

47. At least 30 days *before* "any new use or intended use of the information in the system," an agency must "publish in the Federal Register notice" of the new use 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 & 12 (2016), https://perma.cc/N9QK-SDLE ("OMB Circular No. A-108"); *see also* 5 U.S.C. § 552a(v)(1) (authorizing OMB to issue binding Privacy Act guidelines).

48. Examples of "significant changes" to a system of records that require publication of a modified SORN include a "substantial increase in the number, type, or category of individuals about whom records are maintained in the system"; a "change that expands the types or categories of records maintained in the system"; a "change that modifies the purpose(s) for which the information in the system of records is maintained"; and a "new routine use or significant change to an existing routine use that has the effect of expanding the availability of the information in the system." OMB Circular No. A-108 at 5-6.

49. Agencies "shall" review and consider any "public comments on a published SORN." OMB Circular No. A-108 at 7.

50. To further ensure transparency and congressional oversight, any time an agency "proposes to establish or make a significant change in a system of records,' 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).

51. 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 the 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 Leg. History at 217.

III. The Paperwork Reduction Act further restricts the federal government's collection of Americans' private information.

52. The Paperwork Reduction Act was enacted in recognition of the federal government's "seemingly insatiable appetite for data." *Dole v. United Steelworkers of Am.*, 494 U.S. 26, 32 (1990). The PRA was intended to ensure that data collections serve a specific purpose, avoid duplicative or unnecessarily intrusive collections, "establish a Federal Information Locator System, and develop and implement procedures for guarding the privacy of those providing confidential information." *Id.* (emphasis added).

53. The legislative history of the PRA recognizes its interaction with the Privacy Act and notes that the PRA "reflects the careful consideration by the Committee for the protection of individual's [sic] privacy and confidentiality." S. Rep. 96-930, 60, 1980 U.S.C.C.A.N. 6241, 6300. The Senate Report emphasizes that the "collection, maintenance, use and dissemination of information by the federal government *shall* be consistent with applicable laws of confidentiality and the Privacy Act of 1974." *Id.* (emphasis added). This concern is reflected multiple times

throughout the text of the PRA, including in the Act's codified stated purposes: "The purposes of this subchapter are to— . . . (8) ensure that the creation, collection, maintenance, use, dissemination, and disposition of information by or for the Federal Government is consistent with applicable laws, including laws relating to—(A) *privacy and confidentiality, including section 552a of title 5 [The Privacy Act]*; (B) security of information, including section 11332 of title 40; and (C) access to information, including section 552 of title 5." 44 U.S.C. § 3501(8) (emphasis added).

54. This explicit embrace of the Privacy Act is further reflected in the PRA statutory text which requires that, "with respect to privacy and security," agencies collecting information must "assume responsibility and accountability for compliance with and coordinated management of sections 552 and 552a of title 5, subchapter II of this chapter [the Privacy Act], and related information management laws." *Id.* § 3506(g).

55. The PRA also requires federal agencies to comply with a number of steps *before* a "collection of information" can take place at all. A "collection of information" is defined as the "obtaining, causing to be obtained, soliciting, or requiring the disclosure to third parties or the public, of facts or opinions by or for an agency, regardless of form or format, calling for either [] answers to identical questions posed to . . . ten or more persons, other than agencies, instrumentalities, or employees of the United States." *Id.* § 3502(3).

56. Before a collection is initiated, an agency must conduct a review under Section 3506(c)(1), which includes "(i) an evaluation of the need for the collection of information; (ii) a functional description of the information to be collected; [and] (iii) a plan for the collection of the information." *Id.* § 3506(c).

57. The agency must also "provide 60-day notice in the Federal Register, and otherwise consult with members of the public and affected agencies concerning each proposed collection of information." *Id.*

58. In connection with such notice, the agency must solicit comments to, among other things, "evaluate whether the proposed collection of information is necessary for the proper performance of the functions of the agency, including whether the information shall have practical utility," and "enhance the quality, utility, and clarity of the information to be collected." *Id.* §§ 3506(c)(2)(A)(i), (iii).

59. Thus, the PRA *prohibits* a collection of information unless the agency has, in advance, (1) conducted the § 3506(c)(1) review (44 U.S.C. § 3507(a)(1)(A)); (2) published a 60-day notice in the Federal Register (*id.* at § 3506(c)(2)(A)); (3) evaluated the public comments received (*id.* § 3507(a)(1)(B)); (4) submitted the § 3506(c)(3) certification and a record (including public comments) supporting such certification to the Office of Information and Regulatory Affairs ("OIRA") within the Office of Management and Budget ("OMB")[14] (*id.* § 3507(a)(1)(C)); (5) published a second, 30-day notice in the Federal Register (*id.* § 3507(a)(1)(D), (b)); (6) obtained approval for the collection of information from OIRA (*id.* § 3507(a)(2)); and (7) obtained a control number issued by OIRA (*id.* § 3507(a)(3)).

60. Only if these requirements are met can the agency then commence the collection. In such a case, the PRA requires the agency to ensure that each information collection "is inventoried," "displays [the] control number" issued by OIRA, and includes a notice that "an

[14] OIRA handles PRA submissions, certifications, and approvals. *See* 44 U.S.C. § 3503(b). Most of the substantive PRA provisions, however, refer to decisions by the "Director." *See, e.g.,* 44 U.S.C. § 3507. For purposes of this Complaint, Plaintiffs shall refer to OIRA pursuant to 44 U.S.C. § 3503.

agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number." 44 U.S.C. § 3506(c)(1)(B)(iii)(V).

FACTUAL BACKGROUND

I. The Administration's ongoing attempt to federalize election administration

61. In his second term, President Trump has sought to "take over" and "nationalize" our elections.[15]

62. The President wrongly claims that "the States are merely an 'agent' [sic] for the Federal Government in counting and tabulating the votes. They must do what the Federal Government, as represented by the President of the United States, tells them, FOR THE GOOD OF OUR COUNTRY, to do."[16]

63. On March 25, 2025, President Trump signed an Executive Order directing federal agencies to take various actions related to the administration of federal elections. *See* Executive Order No. 14,248, *Preserving and Protecting the Integrity of American Elections*, 90 Fed. Reg. 14005 (Mar. 25, 2025) (the "2025 Elections EO").

64. The 2025 Elections EO directs the Attorney General to "take all appropriate action to enter into information-sharing agreements, to the maximum extent possible," with state election officials that "aim to provide the Department of Justice with detailed information on all suspected violations of State and Federal election laws discovered by State officials." *Id.* § 5(a). It also directs the Attorney General to "prioritize enforcement of Federal election integrity laws" in states that "are unwilling to enter into such an information sharing agreement or refuse to cooperate in

[15] *Trump urges Republicans to 'take over' and 'nationalize' voting*, ABC7 Chicago, YouTube (Feb. 3, 2026), https://tinyurl.com/4nfv2tdt.

[16] Donald J. Trump (@realDonaldTrump), Truth Social (Aug. 18, 2025, 7:17 AM), https://tinyurl.com/yckutpf.

investigations and prosecutions of election crimes," and to consider withholding federal "grants and other funds" from such states. *Id.* § 5(b). And it instructs that the "Attorney General shall take all appropriate action to align the Department of Justice's litigation positions with the purpose and policy of this order." *Id.* § 5(c).

65. Courts across the country—including in this District—have enjoined federal agencies from implementing key provisions of the 2025 Elections EO on the ground that they violate "the constitutional separation of powers." *LULAC II*, 2026 WL 252420, at *4; *see also League of United Latin Am. Citizens ("LULAC I") v. EOP*, 808 F. Supp. 3d 29, 80 (D.D.C. Oct. 31, 2025); *Washington v. Trump*, 2026 WL 73866 (W.D. Wash. Jan. 9, 2026); *California v. Trump*, 786 F. Supp. 3d 359, 396 (D. Mass. 2025).

66. On March 31, 2026, President Trump signed another Executive Order that, among other things, directs the Secretary of Homeland Security to compile a "list of individuals confirmed to be United States citizens who will be above the age of 18 at the time of an upcoming Federal election and who maintain a residence in the subject State," defined as the "State Citizenship List." *See* Executive Order No. 14,399, *Ensuring Citizenship Verification and Integrity in Federal Elections* 91 Fed. Reg. 17125 (Mar. 31, 2026) (the "2026 Elections EO"). The 2026 Elections EO directs that the "State Citizenship List shall be derived from Federal citizenship and naturalization records, SSA records, SAVE data, and other relevant Federal databases." *Id.*

67. The White House issued the 2026 Elections EO to work in tandem with the DOJ's Voter Registration Nationalization Policy, which is detailed below, to improperly use "citizenship and naturalization records, SSA records, SAVE data, and other relevant Federal databases" in violation of the Privacy Act, the PRA, the APA, and the Constitution.

II. DOJ's consolidation, use, and disclosure of Confidential Voter List data

68. DOJ has consummated its Voter Registration Nationalization Policy.

69. Pursuant to that Policy, DOJ is now collecting state voter files, compiling any state voter files it has or will obtain, and creating a national voter registration system of records in order to federalize voter registration list maintenance.

70. Since the President issued the 2025 Elections EO, DOJ's Civil Rights Division has contacted nearly every state and the District of Columbia to demand their complete Confidential Voter Lists, including sensitive personally identifiable information ("PII").[17]

71. DOJ's voter data demands are substantively identical: the agency is seeking "all fields" contained in each state's Confidential Voter List, including "the registrant's full name, date of birth, residential address, his or her state driver's license number, or the last four digits of the registrant's social security number."[18] In some states, the Confidential Voter List includes political data such as party affiliation and voter participation history.[19]

72. DOJ's Criminal Division also has sent its own emails and letters to election officials in at least 12 states,[20] requesting meetings to discuss an "information-sharing agreement" for the purpose of implementing the 2025 Elections EO.[21]

---

[17] Assistant Attorney General Harmeet Dhillon (@AAGDhillon), X (Dec. 5, 2025, 1:02 PM), https://perma.cc/M7EU-7MT9.

[18] *See*, *e.g.*, Collection of Letters from Harmeet K. Dhillon to State Secretaries of State, *United States v. Beals*, No. 3:26-cv-00042, ECF No. 16-4 (E.D. Va. Jan. 30, 2026).

[19] *Access to and Use of Voter Registration Lists*, Nat'l Conference of State Legislatures (updated July 17, 2025), https://tinyurl.com/3jr9w6a3.

[20] *See, e.g.*, Email from Scott Laragy, Principal Deputy Director of the Executive Office for U.S. Att'ys, and Paul Hayden, Senior Counsel at the Dept. of Justice Criminal Division, to Stephanie Thomas, Sec'y of State of Conn. (July 10, 2025), https://perma.cc/5ZC9-AD6P.

[21] Kaylie Martinez Ochoa, Eileen O'Conner, & Patrick Berry, *Tracker of Justice Department Requests for Voter Information*, Brennan Ctr. for Just. (last updated April 9, 2025), https://tinyurl.com/ypf63y95.

73. DOJ's letters claim its "purpose" for demanding the states' full voter rolls, including PII, is "to ascertain [the states'] compliance with the list maintenance requirements of the NVRA and HAVA."[22]

74. As part of implementing the Voter Registration Nationalization Policy, DOJ has requested that states execute a "Memorandum of Understanding" ("MOU") that requires states to cede their voter list maintenance responsibilities to the federal government.[23]

75. Specifically, DOJ's MOU provides that:

> After analysis and assessment of your state's [voter registration list ("VRL")], the Justice Department will securely notify you or your state of any voter list maintenance issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, the Justice Department found when testing, assessing, and analyzing your state's VRL for NVRA and HAVA compliance, i.e., that your state's VRL only includes eligible voters.
>
> You agree therefore that within forty-five (45) days of receiving that notice from the Justice Department of any issues, insufficiencies, inadequacies, deficiencies, anomalies, or concerns, your state will clean its VRL/Data by removing ineligible voters and resubmit the updated VRL/Data to the Civil Rights Division of the Justice Department to verify proper list maintenance has occurred by your state pursuant to the NVRA and HAVA.[24]

76. The MOU further says that DOJ may disclose Confidential Voter List data to "a contractor with the Department of Justice who needs access to the VRL/Data information in order to perform duties related to the Department's list maintenance verification procedures."[25]

77. The MOU does not specify any data security safeguards applicable to the contractor or any standards for vetting contractors. DOJ has not publicly disclosed which contractor, if any, it has retained to perform these functions. But DOJ's internal communications, released in

---

[22] *Id.*

[23] *See* Alaska and Texas DOJ MOUs, *supra* note 2.

[24] *Id.* at 5.

[25] *Id.* at 4, 6-7.

response to a Freedom of Information Act ("FOIA") lawsuit, show that when DOJ receives data from states, it may "require processing information in new ways," including "[p]otential analysis of ingested data by [a] litigative consultant."[26]

78. Other internal communications show that DOJ's view is that "HAVA, NVRA, CRA - none of them require to give the states information about what we are going to do with the data. No judge will have authority to limit us beyond a promise of Federal law compliance."[27]

79. DOJ has described its efforts implementing the Policy as "[i]ngestion of bulk confidential Voter Registration Data from multiple states" and "[s]torage of bulk confidential Voter Registration Data from multiple states."[28]

80. DOJ claims that, "as of February 27, 2026, thirteen states have provided their" full statewide voter registration lists ("SVRLs") "without any MOU; two states have agreed to provide their SVRL under the terms of the MOU; and three states have indicated their intention to provide the SVRLs in the near future."[29]

81. At least two states, Alaska and Texas, have provided their Confidential Voter Lists to DOJ after executing the MOU.[30]

82. On information and belief, DOJ has no formal MOUs with the other states that have acquiesced to DOJ's demands for Confidential Voter Lists.

83. After DOJ sued Oklahoma to force disclosure of its voter data, the parties executed a settlement agreement on March 24, 2026, under which Oklahoma agreed to provide its

[26] January 12, 2026, email from John Watson to Kilian Kagle, https://perma.cc/RQG4-E5EB.
[27] November 18, 2025, email from Eric Neff to Jesus Osete, https://perma.cc/A25E-GWKA.
[28] January 12, 2026, email from John Watson to Kilian Kagle, *supra*.
[29] Neff Decl. ¶ 16, *United States v. Galvin*, No. 25-cv-13816, ECF No. 70-2 (D. Mass. Feb. 27, 2026), https://tinyurl.com/3mwdbwzr.
[30] *See* Alaska and Texas DOJ MOUs, *supra* note 2.

Confidential Voter List to DOJ within five business days, and DOJ stated it would only use the data to assess Oklahoma's compliance with the NVRA, HAVA, and "other purposes" outlined in DOJ regulations.[31]

84. DOJ has sued 30 states and the District of Columbia for refusing to turn over their Confidential Voter Lists. So far, courts have dismissed five of DOJ's suits for failure to state a claim.[32]

III. DOJ fails to comply with federal data protection laws before engaging in its bulk collection of Confidential Voter List data

85. In both its MOU and in recent litigation, DOJ has confirmed that it is compiling the voter data in a system of records at the Civil Rights Division titled "JUSTICE/CRT – 001, Central Civil Rights Division Index File and Associated Records" ("Central CRT Index File"). DOJ has cited three pertinent SORNs for that system: 68 Fed. Reg. 47610, 611 (August 11, 2003), 70 Fed. Reg. 43904 (July 29, 2005), and 82 Fed. Reg. 24147 (May 25, 2017).[33]

86. However, none of the published SORNs for the Central CRT Index File contemplate or provide the public notice, as required by the Privacy Act, that the system will contain hundreds of millions of Americans' Confidential Voter List data from states across the country, that DOJ plans to disclose this highly sensitive data in bulk to other agencies and private contractors, and that DOJ plans to send the results of its "verification procedures" to states with instructions to remove purportedly "ineligible voters" DOJ identifies. *See* 5 U.S.C. § 552a(e)(4)

---

[31] Settlement Agreement at 3-4, *United States v. Ziriax*, No. 26-cv-361 (W.D. Okla. March 24, 2026), https://perma.cc/9D82-QFHF.

[32] *See Weber*, 2026 WL 118807; *Oregon*, 2026 WL 318402; *Benson*, 2026 WL 362789; *Galvin*, 2026 WL 972129; *Amore*, 2026 WL 1040637.

[33] *See, e.g.*, Alaska and Texas DOJ MOUs, *supra* note 2 at 4; Br. of United States as Appellant at 39-40, *United States v. Weber*, No. 26-1232 (9th Cir. Mar. 18, 2026), https://bit.ly/4cnF6Xb; United States MTD Opp. at 29-30, *United States v. Hanzas*, Case No. 2:25-cv-903-MKL, ECF No. 58 (D. Vt. Feb. 17, 2026), https://bit.ly/4tRghZo.

(requiring that SORNs disclose, among other things, "the categories of individuals on whom records are maintained in the system," the "categories of records maintained in the system," and "the categories of sources of records in the system").

87. The primary SORN for the Central CRT Index File, published in 2003, describes the system as consisting of "case files, matters, memoranda, correspondence, studies, and reports relating to enforcement of civil rights laws and other various duties of the Civil Rights Division." 68 Fed. Reg. at 47611. Nothing in this SORN puts the American public on notice that the system will be used to retain, analyze, and disclose their state-level voter registration data en masse for DOJ's secretive "list maintenance verification procedures." For example, the SORN does not include registered voters in the "categories of individuals covered by the system," it does not include state voter registration data (let alone states' entire Confidential Voter Lists) in the "categories of records in the system," and it does not identify "list maintenance verification" as one of the system's "purposes." *See id.*

88. The other two SORNs cited by DOJ in the MOUs modified the 2003 SORN and likewise do not include any of these details. *See* 70 Fed. Reg. 43904 (July 29, 2005) (adding a routine use allowing disclosure of certain information about closed criminal cases); 82 Fed. Reg. 24147 (May 25, 2017) (adding, per governmentwide OMB guidelines, new routine uses relating to data "breach response").

89. DOJ has not published a modified SORN or solicited public comment for the Central CRT Index File despite amassing, using, and disclosing millions of Americans' sensitive voter data in that system since May 2025.

90. DOJ has not published PRA notices, solicited public comment, or otherwise followed the PRA's requirements for its new collection of millions of Americans' Confidential Voter List data.

91. On information and belief, DOJ is also failing to use basic security precautions with respect to the Confidential Voter Lists it has already obtained and seeks to obtain in the future.

92. Never before has the personal data contained in the Confidential Voter Lists been centralized in a federal system of records at this scale. Prior to DOJ's Voter Registration Nationalization Policy, the data was generally maintained separately by the states, in a decentralized manner.

93. Centralizing this data in a single system of records could facilitate data breaches, identity theft, and other economic crimes, with potentially devastating consequences for the victims, if safeguards are not followed. As election experts have observed, the "data the DOJ [is compiling]—Social Security numbers, drivers license numbers, and dates of birth— comprise the holy trinity of identity theft. If this data were leaked, the financial well-being of millions of Americans would be put at risk."[34] For that reason, best practices demand that DOJ store this sensitive information in a hashed format,[35] so that if a malign actor successfully obtained such files from DOJ's systems, the retrieved data would not be able to be read or understood.

[34] Testimony Before the Alaska State Senate Judiciary and State Affairs Committee, David J. Becker, Executive Director and Founder, Center for Election Innovation & Research (March 4, 2026), https://perma.cc/W4AS-PSXP.

[35] Hashing data is a form of one-way encryption that ensures that, even if the system in which the data is stored is breached, the underlying data cannot be read or used. *See, e.g.,* National Institute of Standards and Technology ("NIST"), Glossary entry for "hashing," https://csrc.nist.gov/glossary/term/hashing. Banks, for example, almost universally store customers' passwords in a hashed (rather than plain text) format for purposes of protecting them even in the event of a data breach.

94. But correspondence with various states demonstrates that DOJ is not following such safeguards.

95. For example, DOJ is instructing states to upload unredacted and unhashed copies of the Confidential Voter Lists directly to DOJ's Justice Enterprise File Sharing System ("JEFS"), and states are complying with these instructions.

96. Files uploaded to DOJ's JEFS system are not hashed before they are transmitted. Nor are they hashed after they are received.

97. DOJ also maintains web-based access to the JEFS system housing the Confidential Voter Lists. *See, e.g.,* Department of Justice Privacy Impact Assessment JMD/Justice Enterprise File Sharing (JEFS) System, available at https://www.justice.gov/media/1169496/, at 3 ("JEFS enables users to upload up to 15 gigabytes of most file types—documents, videos, photos, etc.—from a phone, tablet or computer. Users can then access those files for up to 60 days from anywhere through the DOJ network or over the Internet.")

98. Once in JEFS, this data is accessible to a wide number of DOJ employees and private contractors. These employees and private contractors do not have a need for these records in the performance of their duties.

99. In DOJ's own words, it is "collecting voter registration list data from various states that contains PII," which is stored on DOJ's "P Drive with Lit Support and the attorneys who are working with the data having access to those folders for their investigations."[36]

[36] August 7, 2025, email from Timothy Mellett to Allan Percival, https://perma.cc/9WZK-9P2K.

IV. DOJ plans to disclose Confidential Voter List data to DHS to use its SAVE system for unreliable, mass citizenship checks without authority to do so

100. In addition to sharing Confidential Voter List data with unknown third-party contractors, DOJ is also disclosing and will imminently disclose Confidential Voter List data en masse to DHS so it can run the data through its unreliable SAVE system, which DHS haphazardly expanded in 2025 as a tool for mass "voter verification" citizenship checks.

101. SAVE is an "online inter-governmental service" designed to help government entities "determine citizenship and immigration status of individuals within their jurisdiction for the purpose of granting benefits, licenses, as well as for other lawful purposes."[37] To use SAVE, federal agencies "must execute a Memorandum of Agreement [("MOA")] or Computer Matching Agreement with the U.S. Citizenship and Immigration Services that includes terms that the SAVE Program will be used in accordance with the law."[38]

102. SAVE was not designed for mass voter eligibility checks. As its name reflects, Congress established the "Systematic Alien Verification for Entitlements" system to verify whether *non-citizens* ("aliens") are entitled to certain government *benefits* ("entitlements"). *See* Immigration Reform Control Act of 1986, Pub. L. No. 99-603, title I, §121(c)(1), 100 Stat. 3359, 3391 (1986), *codified at* 42 U.S.C. § 1320b-7 note; *id.* § 121(a)(1)(C), 100 Stat. at 3384-86 (1986), *codified at* 42 U.S.C. § 1320b-7(d) (section titled "Verification of Immigration Status of Aliens Applying for Benefits under Certain Programs").

[37] DHS, *Privacy Impact Assessment for the Systematic Alien Verification Entitlements "SAVE" Program*, DHS Ref. No. DHS/USCIS/PIA-006(d), at 1 (Oct. 31, 2025), https://perma.cc/G92U-LYPM ("2025 SAVE PIA").

[38] *Id.* at 21.

103. But in 2025, DHS dramatically "overhaul[ed]" SAVE,[39] transforming what was previously a limited tool that only conducted individualized searches of immigration-related databases into a massive new national citizenship data bank that conducts bulk searches of millions of Americans' sensitive data stored across multiple federal and state agencies.[40] Working with the Department of Government Efficiency ("DOGE") to implement the 2025 Elections EO, DHS hastily expanded SAVE to allow states to bulk upload their entire voter registration lists—including full names, dates of birth, and SSNs—to identify potential non-citizens.[41] DHS took these actions without advance testing, validation, or statutorily required notice and comment.

104. Overhauled SAVE utilizes unreliable data and search methods that the government itself acknowledges risks falsely identifying U.S. citizens as non-citizens, especially citizens born outside of the United States (e.g., naturalized, derived, and acquired citizens). In privacy assessments conducted throughout 2025, DHS acknowledged that "[s]hortfalls in data accuracy in the [SAVE] system could cause incomplete or false results."[42]

105. Most notably, SAVE now incorporates data collected by the Social Security Administration that SSA has long recognized is incomplete and unreliable for verifying citizenship, especially for citizens born outside of the United States. That is because SSA captures this data from an individual at a single moment in time: when they apply for an SSN and the

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

[40] *See* Privacy Act Notice of Modified System of Records, 90 Fed. Reg. 48948, 48949-50 (Oct. 31, 2025) ("2025 SAVE SORN").

[41] *See id.*

[42] DHS, *Privacy Threshold Analysis for the SAVE Program*, at 17 (approved July 17, 2025), https://perma.cc/9AXY-WCLU; DHS, *Privacy Threshold Analysis for the SAVE Program*, at 17 (approved Sept. 11, 2025), https://perma.cc/A44N-4729; *see also* 2025 SAVE PIA at 19 ("[D]ue to misspelling of names, transposed numbers, or incomplete information, the SAVE Program may produce inaccurate results.").

corresponding card. If an individual becomes a citizen after obtaining their SSN, SSA does not automatically update their citizenship status.[43] SSA has cautioned against repurposing its citizenship data for other uses, explaining that while "citizenship information is accurate for SSA's program purposes, if used later for other purposes, it may not be current" because "SSA is not the custodian of U.S. citizenship records."[44]

106. DHS admits that overhauled SAVE's data gaps are especially likely to impact citizens born outside of the United States, stating in recent guidance that "if an individual with acquired citizenship has not received a Certificate of Citizenship from USCIS (e.g., some foreign-born children of U.S. citizens) or is not designated as a U.S. citizen in SSA records, SAVE may not be able to confirm that individual's U.S. citizenship," and that, "[i]n these circumstances, SAVE returns the case to the user agency for review of their information for data entry errors or to seek additional information from the individual."[45]

107. Despite the known problems with overhauled SAVE, several states are—at the Administration's urging—rapidly deploying the system for mass voter citizenship checks. Early results are damning: they show that, in states such as Texas, the overhauled SAVE process has falsely identified eligible U.S. citizen voters as non-citizens, forced them to needlessly provide documentary proof of citizenship to state and federal authorities, and caused eligible voters to be wrongfully removed from voter rolls, even disenfranchising some.[46] SAVE has also created

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

[44] *Id.*

[45] USCIS, *Voter Registration and Voter List Maintenance Fact Sheet* (Aug. 27, 2025), https://perma.cc/Q5F7-YBCA.

[46] *See, e.g.*, *League of Women Voters v. Dep't of Homeland Security*, No. 25-3501 (D.D..C), Nel Decl. (ECF No. 66-3) ¶¶ 12-26; B. Doe Decl. (ECF No. 66-5) ¶¶ 28-31; C. Doe (ECF No. 66-6) Decl. ¶¶ 17-18.

significant confusion and problems for election administrators, and jeopardized millions of Americans' privacy and data security.[47]

108. As one recent investigation found, overhauled SAVE "is making persistent mistakes, particularly in assessing citizenship for people born outside the U.S."[48]

109. For example, in Missouri, 70 county clerks in December 2025 signed a letter to the state legislature stating that SAVE results they were provided were "outdated, inaccurate, and include individuals we know to be U.S. citizens—our neighbors, colleagues, and even voters we have personally registered at naturalization ceremonies."[49] The election director for St. Louis County "found that around 35 percent of roughly 690 people initially flagged by the SAVE tool were registered at naturalization ceremonies."[50]

110. The results from one Texas county reveal a SAVE error rate of "at least 14%," but the "real rate is probably higher, since some of those sent [SAVE non-citizenship] notices to prove their citizenship might not respond in time to meet the deadline."[51]

111. Despite the known problems with overhauled SAVE, since the day DHS announced the overhauled SAVE system was operational, DOJ has been pushing forward with its plans to use the flawed system to conduct mass citizenship checks of the Confidential Voter List data it is obtaining from states.[52]

---

[47] *See* Fifield and Despart, *supra*.

[48] *Id.*

[49] Letter from 70 Missouri County Clerks to Rep. Jonathan Patterson (Dec. 3, 2025), https://tinyurl.com/4nz7nkst

[50] Alexandra Berzon and Nick Corasaniti, *Initial Review Finds No Widespread Illegal Voting by Migrants, Puncturing a Trump Claim*, N.Y. Times (Jan 14, 2026), https://tinyurl.com/36kfzc7u.

[51] Fifield and Despart, *supra*.

[52] May 13, 2025, email from Maureen Riordan to Mac Warner, https://perma.cc/FEN6-U7T6.

112. DOJ has been working on obtaining access to SAVE ever since.[53] DOJ's internal communications suggest that while the Civil Rights Division is leading its efforts to gain access to SAVE for voter list maintenance purposes, DOJ also intends to share access with the Criminal Division.[54]

113. According to a February 11, 2026, letter from the West Virginia Secretary of State, DOJ confirmed to state officials that "the alleged purpose of the DOJ's request is to run West Virginia's entire voter list through [SAVE]."[55]

114. At a March 19, 2026, court hearing in DOJ's voter data suit against Connecticut, DOJ counsel represented that DOJ has not yet executed an MOA with DHS to use SAVE, and that "none of the private" voter data "that's been produced to [DOJ] has been run through [the] SAVE database."[56]

115. At a March 26, 2026, hearing in DOJ's voter data suit against Rhode Island, however, DOJ counsel stated that "we are certainly going to be proceeding with running" Confidential Voter List data "against DHS's SAVE database," which counsel describes as essentially "a fetching system that seeks information from other databases to cross-check whether the data set on a [voter] roll is either a deceased person or a noncitizen."[57]

[53] *See*, *e.g.*, June 5, 2025, email from Maureen Riordan to Michael Gates, https://perma.cc/M6L6-VRM6; December 23, 2025, email from Eric Neff to Chris Hayes, https://perma.cc/MFV6-AH2M.
[54] January 13, 2026, email from Andrew Braniff to Jesus Osete, https://perma.cc/QVK6-XHGA.
[55] West Virginia Letter, *supra*.
[56] Hr'g Tr. at 52-53, 78, *United States v. Thomas,* No. 26-21 (D. Conn. March 19, 2026).
[57] Hr'g Tr. at 50-51, *United States v. Amore*, No. 25-639 (D.R.I. March 26, 2026).

116. While DOJ counsel at the Rhode Island hearing initially stated, incorrectly, that SAVE's "accuracy rate" is "in effect 100 percent," counsel went on to acknowledge the data "holes" in the system with respect to naturalized and derived citizens.[58]

117. Even though DOJ is not currently an authorized SAVE user, the Civil Rights Division has been closely monitoring and amplifying the results of the states' use of SAVE's new bulk "voter verification" functionality.

118. DHS touted that, as of December 2025, more than 47 million voters have had their personal data run through the flawed SAVE system in an attempt to identify non-citizens.[59] Echoing this figure, Assistant Attorney General for Civil Rights Harmeet Dhillon claimed in December 2025 that the Administration had "checked 47.5 million voter records"—apparently through SAVE—and has "found 260,000 plus dead people" and "several thousand noncitizens enrolled to vote in federal elections."[60]

119. As of March 2026, Assistant Attorney General Dhillon has claimed that the Administration's review of "50–60 million voter records has revealed there are thousands of ineligible and outdated registrations—including non-citizens."[61]

120. In sum, DOJ is rapidly amassing, analyzing, matching, and disclosing inside and outside of the agency millions of Americans' Confidential Voter data, with the stated purpose of identifying purportedly "ineligible voters" using concededly unreliable means and methodology,

---

[58] *See id.* at 51-53.

[59] Jude Joffe-Block, *Trump's SAVE tool is looking for noncitizen voters. But its flagging U.S. citizens too*, NPR (Dec. 10, 2025), https://www.npr.org/2025/12/10/nx-s1-5588384/save-voting-data-us-citizens.

[60] Assistant Attorney General Harmeet Dhillon (@AAGDhillon), X (Dec. 5, 2025, 1:02 PM), https://perma.cc/M7EU-7MT9.

[61] Assistant Attorney General Harmeet Dhillon (@AAGDhillon), X (Mar. 17, 2025, 2:43 PM), https://perma.cc/Y5DT-UNGA.

and then requiring states to cancel those voters' registrations. For at least two states, DOJ has executed formal MOUs that purport to cede the states' voter list maintenance responsibilities to the federal government. For the remaining states that have acquiesced to DOJ's data demands, no formal agreement restricts how DOJ uses and discloses the states' Confidential Voter List data. And DOJ has taken these actions in secret, without statutorily required transparency, consent, or input from the impacted American people.

V. Plaintiff Anthony Nel's wrongful removal from the voter rolls as a result of overhauled SAVE's unreliable data and methods

121. After turning 18, Plaintiff Nel registered to vote and began voting in state and federal elections in Texas. He first voted in the 2016 election and intends to continue voting.

122. After voting in the November 2025 election (during early voting), Plaintiff Nel received a letter from the Denton County Voter Registrar, dated October 21, 2025, titled "Notice to Registered Voter for Proof of Citizenship (USCIS Verification)." The letter states in part that a "comparison of the information in your voter registration records with the United States Citizenship and Immigration Services SAVE records show that you were not a United States citizen at the time of the comparative process." It then instructs: "[t]o maintain your active voter registration status, please provide proof that you are a United States citizen." The letter lists several types of documents that will be accepted as proof of U.S. citizenship, and notes that copies of the documents can be delivered by hand, mail, fax, email, or any other method of transmission.

123. The letter further states: "Please provide proof of U.S. citizenship within (30) days from the date of this letter. If we do not receive a response from you within thirty (30) days, your voter registration will be cancelled."

124. Of the documents sufficient to prove citizenship listed in the letter, the only document Plaintiff Nel had was a U.S. passport. However, his passport expired on July 17, 2023.

Due primarily to the threat of his voter registration being cancelled unless he provided proof of citizenship, he applied to renew his passport and paid the required fee. He obtained a renewed passport on December 10, 2025. In early December 2025, he checked Denton County's voter lookup system and saw that it no longer listed him as a registered voter.

125. After Plaintiff Nel emailed the Denton County Voter Registrar asking why his voter registration was cancelled, the Elections Administrator responded that Plaintiff Nel's "name appeared on a list of potential non-citizens that was sent to us from the Secretary of State's office. On 10/22/2025 we mailed a letter to you asking for proof of citizenship. … When you did not reply to the letter within the 30-day period, your registration was cancelled." Later in December, Plaintiff Nel received another letter from the Denton County Voter Registrar, postmarked December 3, 2025, titled "Notice of Cancellation," confirming that his voter registration had been cancelled.

126. Ultimately, Plaintiff Nel was able to provide the Denton County Voter Registrar with a copy of his renewed passport and, as a result, his voter registration was reinstated. However, Plaintiff Nel is concerned that he will continue to be wrongly identified as a non-citizen if the DOJ runs his information through the SAVE system, and that he will again be forced to prove his citizenship status in order to retain his voter registration. Being caught in such a cycle, with his voting rights on the line, is distressing to him. He feels compelled to continue regularly checking his voter registration status to ensure it is not wrongly cancelled again.

INJURIES TO PLAINTIFFS

I. Injuries to the Voter Plaintiffs and Common Cause Members

127. Plaintiffs Nel, Smith, Duckworth, and Nasrullah ("the Voter Plaintiffs") and other members of Common Cause who are registered to vote in the states that have supplied Confidential Voter List data to DOJ have suffered and will suffer violations of their privacy rights through DOJ

and other agencies' improper access to and misuse of their sensitive personal data, including driver's license numbers, partial social security numbers, birth dates, and other information.

128. The Voter Plaintiffs and other Common Cause members who are registered to vote in the states that have supplied Confidential Voter List data to DOJ have a right to keep this sensitive data private. When each of them registered to vote, they provided sensitive personal information with the expectation that it would be used only for the purpose of registering to vote. Each expected this information to be kept private when they supplied it to state officials as part of the registration process, based on assurances in state privacy laws and the limits of what states typically provide in public versions of the voter file. They did not consent to it to being obtained, stored, and used by the DOJ, or shared with and then stored and used by other federal agencies such as DHS, or shared with and then stored and used by private contractors and third parties.

129. Yet DOJ has done this and/or is imminently planning to do so. This intrusion upon the voters' sensitive private information, and the unauthorized and unconsented sharing, aggregation, and combination of their data without their consent, is alarming and offensive—all the more so because the Voter Plaintiffs and others like them were given no advance notice or opportunity to comment on DOJ's novel misuse of their private information, as the law requires.

130. This intrusion will cause the Voter Plaintiffs and other Common Cause members who are registered to vote in the states that have supplied Confidential Voter List data to DOJ to fear providing information to their own governments and accessing public services in the future, diminish their trust in government, and disrupt their expectation that they may live their private lives without unconsented monitoring by agents of the federal government and its undisclosed contractor(s).

131. In addition, the improper disclosure of these voters' sensitive personal information to various government agencies and private contractors is likely to cause financial harm and other forms of pocketbook harm. The improper use of this data, including its use or storage subject to undisclosed security protocols, including to private contractors and potentially across multiple federal agencies, dramatically heightens the risk that the Voter Plaintiffs' and other Common Cause members' data will be misused or else obtained by hackers or other unauthorized third parties, who upon information and belief frequently test government databases for vulnerabilities and seek to obtain government data and use it for fraud, theft, and similar purposes.

132. DOJ's unauthorized access to their information has intruded upon the right to privacy of the Voter Plaintiffs' and other Common Cause members who are registered to vote in the states that have supplied Confidential Voter List data. Their safety and security may be at risk. If this information is further disseminated, used, or shared, their right to privacy will be further invaded and their security will be at additional heightened risk.

133. The privacy intrusion is heightened for the Voter Plaintiffs, including Plaintiffs Nasrullah, Nel, and Smith, and other Common Cause members who live in Texas, Alaska, and other states that have signed the MOU with DOJ indicating that the DOJ may share their information with external third parties of unknown qualification and bias.

134. Some of the Voter Plaintiffs and other Common Cause members who are registered to vote in the states that have supplied Confidential Voter List data have particular concerns about their personal privacy, safety, and security due to their life experiences. For example, Plaintiff Nasrullah has heightened concerns about her personal privacy due to her life experiences, including her experience as an activist and journalist. Due to her heightened privacy concerns, she intentionally protects her personal information and limits the personal information she shares.

135. In addition to these privacy-related and pocketbook harms, the Voter Plaintiffs and other members of Common Cause who are registered to vote in the states that have supplied Confidential Voter List data to DOJ are also at grave risk of suffering harms to their voting rights and right to participate in politics as a result of the challenged misuse of the Confidential Voter List data. In particular, DOJ claims the authority to use the Confidential Voter List data to determine who is eligible to vote, but its unauthorized and ill-considered attempts to use the data for those purposes has led and will lead to numerous false positives—that is, faulty indications that qualified, registered voters on a state's voter rolls are ineligible. As stated in DOJ's MOU, DOJ nevertheless will use these "verification procedures" to identify purported "ineligible voters" and then require states to remove those individuals from their voter rolls.

136. The Voter Plaintiffs and certain other Common Cause members who are registered to vote in the states that have supplied Confidential Voter List data to DOJ are especially likely to be ensnared and have their voting rights targeted in DOJ-led voter purges based on misuse of the Confidential Voter List data. In particular, DOJ has specifically indicated that it intends to use processes that are disproportionally likely to ensnare citizens born outside of the U.S. (*i.e.*, naturalized, derived, and acquired citizens); people who were formerly incarcerated; students or others who change addresses; and seniors or those whose data may be missing from the SSA databases that DHS's overhauled SAVE system now queries. Further, using NCOA or its data may systematically flag college students as ineligible based on residency.[62] And the SSA databases are missing citizenship data for individuals born before 1981.[63]

[62] Sweeney, Latanya, and Josh Visnaw, *Measuring Mistakes: A Data-Driven Assessment of Voter List Maintenance and Erroneous Deletions in Ohio's 2024 Election*, Technology Science (April 22, 2025).

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

137. All of the named Voter Plaintiffs and numerous additional Common Cause members who are registered to vote in the states that have supplied Confidential Voter List data to DOJ fall within one or more of these high-risk categories.

138. For example, Plaintiff Nel is a derived citizen and one of many Texas voters whose voter registration was already wrongly cancelled by local election officials in Texas because of their use of the overhauled SAVE system. Both Plaintiff Duckworth and Plaintiff Nasrullah were born before 1981 and have changed their names due to marriage. Plaintiff Smith is a college student who has moved frequently. All are concerned that additional use or disclosure of their personal information by DOJ will result in being wrongly flagged for removal from the voter rolls (Mr. Nel for the second time) or mislabeled an illegal voter.

139. In addition, the Voter Plaintiffs and other members of Common Cause who are registered to vote in the states that have supplied Confidential Voter List data to DOJ have also suffered and will continue to suffer ongoing harm by virtue of being deprived of information concerning the collection, aggregation, and sharing of their data that DOJ was statutorily required to disclose in advance. For instance, they do not know the purposes for which the DOJ is aggregating their data; the policies and practices the DOJ or other agencies such as DHS are following (if any) to store, control access to, retain, and dispose of the data being consolidated in the Central CRT Index File; the policies and practices the DOJ is following (if any) when conducting "list maintenance verification procedures;" the steps taken to ensure that these "procedures" are technically secure and results in accurate records; the procedures to contest, correct, or update the result of these "procedures;" or the policies and practices the DOJ is following (if any) in the disclosure of the results of these "procedures" to states.

140. All of this information, and other related information, should have been provided to the Voter Plaintiffs and other members of Common Cause who are registered to vote in the states that have supplied Confidential Voter List data through SORNs and Federal Register notices *before* the DOJ began demanding Confidential Voter Lists.

141. Without this information guaranteed by law, the Voter Plaintiffs and other members of Common Cause who are registered to vote in the states that have supplied Confidential Voter List data to DOJ cannot adequately understand how their personal data is being consolidated, disclosed, or utilized as part of the DOJ's "list maintenance verification procedures," take steps to safeguard their data and their voting rights, or protect themselves from any related consequences. They also lack the necessary information to be able to submit a request for an accounting of the disclosures of their records under §552(c) or a request to review and, if necessary, amend their personal records under § 552(d).

142. This lack of information is concerning and distressing to the Voter Plaintiffs, and each seeks this information so that they can determine the additional steps needed to protect themselves and their right to vote, such as establishing credit monitoring and/or closely monitoring their voter registration and preparing to respond to efforts to remove them from the rolls.

143. The Voter Plaintiffs and other members of Common Cause who are registered to vote in the states that have supplied Confidential Voter List data to DOJ have also been deprived of advance notice and the opportunity to participate in the process for determining how their personal data is being collected and used, including the right to comment in advance on DOJ's compilation of data in the Central CRT Index File and the right to have those comments considered.

144. Three of the Voter Plaintiffs have submitted comments and provided testimony to the government on many issues and would have liked to provide comment on DOJ's Policy had they been given an opportunity. In fact, Plaintiff Duckworth wrote a comment to the Nebraska Secretary of State to request that her personal voter file data not be provided to the federal government. She received no response. She also would have submitted comments on any SORN or PRA notice DOJ published regarding its collection and new uses of voter data—had DOJ complied with the Privacy Act and PRA—and intends to do so if DOJ complies in the future.

II. Organizational injuries to Common Cause

145. Common Cause as an organization is also independently injured by DOJ's unlawful misuse of the Confidential Voter List data and the ensuing privacy and informational violations.

146. Common Cause is a national, nonpartisan organization with nearly one million members across all 50 states. Its mission is to create open, honest, and accountable government that serves the public interest; promote equal rights, opportunity, and representation for all; and empower all people to make their voices heard in the political process. Common Cause endeavors to encourage voters to get involved in the electoral process because of its belief that voters' robust and fair ability to vote is crucial to the health of our democracy and deciding the future of the country.

147. As part of its mission, Common Cause devotes significant resources to promoting political participation and voter turnout in the states that have supplied Confidential Voter List data to DOJ. Common Cause expends resources deploying and supporting staff based on the ground in the states, including in states that have supplied Confidential Voter List data to DOJ such as Texas, Ohio, Nebraska, and Indiana, in order to carry out that mission. Common Cause's efforts in those and other states that have supplied Confidential Voter List data to DOJ include

monitoring changes in voter registration and election procedures and administration at the state and local level; educating the public about changes in voting and election procedures through in-person events, social media, and other campaigns; conducting direct outreach to encourage people to register and vote; assisting, training and supporting partner organizations that conduct voter registration in the relevant states; and conducting or facilitating poll observation and other election protection programs to ensure that election procedures are followed and that eligible voters are able to vote and to assist voters who are having trouble at the polls. Common Cause devotes resources, including money, staff and volunteer time, and strategic bandwidth to planning and executing these voting- and election-related programs at the state level. And Common Cause typically serves a key role in leading statewide election protection programs and educating civil society groups about state rules regarding democracy, elections, and open government.

148. For example, in Nebraska, Common Cause staff regularly train and mobilize approximately 200 people to conduct statewide poll-monitoring programs, covering about 300 polling locations and reporting issues that arise on Election Day, including voters who are turned away from the polls. Common Cause in Texas devotes significant time and resources to create and disseminate materials to help raise public awareness about voting procedures, increase voter engagement, and train volunteers involved in voter registration. Common Cause Ohio has been conducting election protection work since 2012; it helps to recruit and train volunteers to monitor the polls and attend Boards of Elections meetings to ensure that election procedures, including the counting of provisional ballots, are followed; and it helps educate partner organizations on changes in election administration, including the purging of voters from the rolls and mass challenges to voters' eligibility. In Indiana, Common Cause conducts voter registration efforts, particularly in under-served communities, creates and distributes know-your-rights materials for voters, and

manages a poll-monitoring program across the state—with special attention to communities that have experienced obstacles to voting in the past, such as those with higher rates of naturalized citizenship. These examples are representative of Common Cause's work nationally and across the states impacted by DOJ's data collection efforts.

149. Among other impacts, DOJ's unlawful misuse of the Confidential Voter List data and the ensuing privacy violations will disrupt Common Cause's existing voter education and protection efforts, hampering Common Cause's ability to serve this vital mission and causing it to expend additional resources to accomplish its goal of increasing political engagement and participation. In Common Cause's experience, willingness to participate in elections and other aspects of civic life depends in significant part on trust in government. As a result of DOJ's actions to collect and share data with DHS, members of the public have expressed concern about how the federal government will use their personal data, including for purposes of retaliation against them or their family members. That is particularly true of naturalized and derived citizens, as well as those whose family members may not be citizens and may be targets of immigration enforcement.

150. Since the highly publicized effort by DOJ to collect and centralize state voter data, Common Cause has observed a significant increase in inquiries about DOJ's efforts and the potential impacts on voters in the states that have supplied Confidential Voter List data to DOJ. For example, in Nebraska, Common Cause has seen an approximate tenfold increase in questions about voter data and privacy. Because of the increased attention and concern about these issues, Common Cause has spent and will continue being forced to expend additional resources, including financial resources and staff and volunteer time, to update training and public education materials relating to voter registration and voter privacy, to answer questions and concerns from voters, potential registrants, and civil society groups regarding the misuse of voter data, and to persuade

citizens to register to vote and to participate in the political process despite the alarming privacy violations and data risks that may result. Common Cause has seen similar trends in the other states that have voluntarily turned over their Confidential Voter List data. Thus, DOJ's unlawful efforts to obtain private voter data and its secretive and impermissible misuses of that data make Common Cause's mission of promoting political participation more difficult and costly to achieve. Indeed, research shows that "privacy or security" concerns are among the top reasons why eligible unregistered voters do not want to register to vote.[64]

151. DOJ's misuse of the Confidential Voter List data and the resulting risk it poses to voters' ability to participate in elections will also interfere with and harm Common Cause's efforts to conduct and facilitate nonpartisan election protection and poll monitoring programs. As part of its mission to protect voters and promote political participation, Common Cause provides its members, partner organizations, and the public with authoritative, deeply researched resources and tools to facilitate the registration and voting process. To ensure that election procedures are followed and that voters who encounter obstacles receive help and assistance, Common Cause facilitates statewide poll monitoring programs, creates materials to train volunteers to observe and report issues that occur on Election Day, recruits and trains volunteers, connects voters with election protection hotlines, and conducts post-election debriefs to identify and address problems.

152. Because of DOJ's unlawful efforts to impermissibly collect and maintain the Confidential Voter List data, transmit such data to DHS and/or other federal agencies without consent or authorization, and ultimately to use the Confidential Voter List data to question voters' eligibility using error-prone processes, Common Cause has had to and must continue to expend

[64] *Why Are Millions of Citizens Not Registered to Vote?* The Pew Charitable Trusts (June 2017), https://perma.cc/FL78-7GZN.

staff and volunteer time and financial resources to ensure that eligible voters are not erroneously removed from the state's voter rolls or otherwise prevented from voting. Those steps include investigating the processes that each jurisdiction will use to purge voters identified by DOJ; updating its training materials; and spending time and resources training volunteers, partners, and staff working on its election protection and poll monitoring programs to be able to assist voters who may be erroneously purged and to answer voters' questions and address voters' concerns relating to the misuse of Confidential Voter List data. Common Cause will also need to continue updating existing materials and developing new educational materials, web materials, FAQ materials, and other resources to support and educate voters who are already on the rolls and are concerned about the violation of their privacy and/or DOJ's contemplated voter purges. As it has done in response to past voter purges, and in response to DOJ's misuse of the Confidential Voter List data, Common Cause also intends to devote resources to conduct public education campaigns reminding voters to double-check their registration status to ensure that they have not been erroneously purged.

153. These new or expanded efforts to mitigate the effects of DOJ's unlawful actions will require Common Cause to divert its resources, including the time and efforts of volunteers and staff, away from existing priorities and programs, and will be a drain on Common Cause's existing election protection and voter engagement programs. Common Cause has a limited number of staff responsible for its work in each state, and its staff must choose priorities to abandon or postpone when a new threat to political participation, like DOJ's unlawful actions here, arises. Common Cause's other organizational priorities in the states that have acquiesced to the DOJ's data demands include legislative advocacy, protecting access to ballot initiatives, guarding against public corruption, reforming campaign finance, and administrative reforms to improve election

administration. For instance, in Texas, Common Cause serves as a watchdog for public corruption, conducts awareness campaigns about new electoral districts, and advocates for local reforms before city councils and county commissions, among other programs. Common Cause Ohio's other priorities include working to strengthen ethics and accountability in government, ensure fair electoral districts, and reduce the influence of money in politics. Expending greater resources to protect voters and elections will detract from those and other programs aimed at protecting America's democratic institutions.

154. DOJ's unlawful misuse of the Confidential Voter List data will thus thwart Common Cause's mission, make its organizational mission more difficult to achieve, and undermine its core activities. Common Cause has been and will be forced to expend more of its limited resources to educate potential registrants, voters, volunteers, and civil society partner organizations in the states that have supplied Confidential Voter List data to DOJ about the uses and misuses of voters' private data and to address the public's legitimate fears about whether their personal data is secure and whether their political participation will come at the price of their privacy and data security and other misuses of their data. Common Cause also has been and will be forced to allocate greater resources in those states to train volunteers and educate partner groups and the public about the risk of being purged as a result of DOJ's actions and to assist voters who are unable to vote on Election Day due to being erroneously purged from the voter rolls. Common Cause will accordingly have fewer resources to devote to its existing core organizational activities, including, without limitation, registering voters in historically marginalized communities, increasing voter turnout, educating voters about the electoral process, and staffing and directing election-protection efforts to ensure that all voters' ballots are counted. This resource drain will also diminish the organization's work in other areas, such as advocating for or against specific

legislation, educating members of the public about that legislation, and engaging with civil rights advocacy.

155. Common Cause has also suffered and will continue to suffer ongoing harm by virtue of being deprived of the information that DOJ was required to disclose under the mandatory provisions of the PRA and the Privacy Act. Common Cause depends on these disclosures to inform its research, advocacy, public education, and education of its members concerning changes in voting and election procedures. Common Cause's ability to perform its mission-critical functions, including monitoring changes in voting and election procedures, conducting direct outreach, training and supporting partner organizations, educating civil society groups and voters, and executing voting- and election-related programs, are directly impaired by the DOJ's failure to publish SORNs, Federal Register notices, and other information concerning the collection and consolidation of Confidential Voter List data in the Central CRT Index File in advance of collection.

156. Common Cause has also been denied the statutorily guaranteed opportunity to comment in advance on the DOJ's collection, compilation, and sharing of Confidential Voter List data, including raising concerns about the impact of DOJ's actions on voter willingness to participate in elections and other aspects of civil life and offering potential solutions that would support Common Cause's mission of promotion political participation.

157. Common Cause has also had to and will expend resources, diverted from its usual programs, to attempt to obtain more information about DOJ's consolidation and use of Confidential Voter List data in an effort to overcome DOJ's failure to follow the relevant mandatory informational disclosure and procedural requirements.

CLAIMS FOR RELIEF

COUNT I
Violation of the APA
(Agency Action in Excess of Statutory Authority)

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

159. The APA requires courts to "hold unlawful and set aside agency action" that is "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(A), (C).

160. DOJ's Voter Registration Nationalization Policy and decisions to compile, consolidate, use, and disclose both within and outside of the agency Confidential Voter List data, as well as the associated policies and agreements, are "final agency action[s] for which there is no other adequate remedy in a court," within the meaning of the APA. 5 U.S.C. § 704.

161. An "agency . . . literally has no power to act . . . unless and until Congress authorizes it to do so by statute." *FEC v. Cruz*, 596 U.S. 289, 301 (2022); *accord Marin Audubon Soc'y v. FAA*, 121 F.4th 902, 911 (D.C. Cir. 2024).

162. No statute authorizes DOJ to federalize voter list maintenance by (1) consolidating millions of voters' sensitive personal data in a centralized system of records, (2) disclosing data from that system internally within DOJ or outside of DOJ, including to DHS, and private contractors, (3) matching that data against other datasets for purposes of conducting "list maintenance verification procedures," and (4) disclosing the results of those "procedures" to states with instructions that they "remov[e] ineligible voters" identified by DOJ. *See* Alaska and Texas DOJ MOUs, *supra* note 2, at 7.

163. Congress has enacted statutes to regulate elections such as the NVRA and HAVA. Those laws do not authorize DOJ to conduct or intervene in voter list maintenance, or to consolidate hundreds of millions of Americans' sensitive voter data in a centralized system of records. Rather, the NVRA and HAVA explicitly charge *the States* with maintaining their voter rolls. *See* 52 U.S.C. §§ 20506, 20507, 20509, 21085; *see also Arizona,* 570 U.S. at 15 (addressing NVRA); *Sandusky Cnty. Democratic Party*, 387 F.3d at 576 (addressing HAVA).

164. If Congress had intended for these statutes to confer the extraordinary authority DOJ now claims—*i.e.*, the power to usurp the States' authority to maintain their voter rolls—it would have said so clearly and expressly. *See West Virginia v. EPA*, 597 U.S. 697, 724 (2022); *Ala. Ass'n of Realtors v. HHS*, 594 U.S. 758, 764 (2021). Congress did no such thing.

165. Defendants' Policy and associated actions are therefore "in excess of statutory jurisdiction, authority, or limitations, or short of statutory right." 5 U.S.C. § 706(2)(A), (C).

COUNT II
Violation of the APA
(Agency Action Contrary to Constitutional Power)

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

167. The APA requires courts to "hold unlawful and set aside agency action … found to be … contrary to constitutional right, power, privilege, or immunity." 5 U.S.C. § 706(2)(B).

168. The Constitution presumes coequal branches, and the "doctrine of separation of powers" lies "at the heart of our Constitution." *Buckley v. Valeo*, 424 U.S. 1, 119 (1976).

169. The Executive cannot usurp Congress's legislative authority by fiat. *See Youngstown Sheet & Tube Co. v. Sawyer*, 343 U.S. 579, 585 (1952). The Executive has no

constitutional power to enact, amend, or repeal parts of duly enacted statutes. *See Clinton v. City of New York*, 524 U.S. 417, 438-39 (1998).

170. An agency violates the separation of powers where it acts in the total absence of authority from Congress in a domain that the Constitution assigns to Congress and the States. *See Minnesota v. Mille Lacs Band of Chippewa Indians*, 526 U.S. 172, 189 (1999) (it is "black letter law" that the Executive's "'power, if any, . . . must stem either from an act of Congress or from the Constitution itself.'" (quoting *Youngstown*, 343 U.S. at 585)).

171. As detailed above, DOJ lacks any statutory authority to establish a national voter registration system and federalize or otherwise take over the States' responsibilities for voter list maintenance.

172. DOJ also lacks any constitutional authority to federalize voter list maintenance. Rather, the Constitution vests "the power to determine who is qualified to vote" in the States and "the power to regulate federal election procedures" in the States and Congress; the Constitution "assigns no direct role to the President in either domain." *LULAC II*, 2026 WL 252420, *5; *see* U.S. Const. art. I, § 2, cl. 1 (Voter Qualifications Clause); *id.* amend. XVII; *id.* art. I, § 4, cl. 1 (Elections Clause); *see also Arizona*, 570 U.S. at 17.

173. By acting with a "total absence of authority from Congress in a domain that the Constitution assigns to Congress and the States," *LULAC II*, 2026 WL 252420, *51, DOJ has violated the separation of powers.

174. Defendants' Policy and associated actions therefore "contrary to constitutional right, power, privilege, or immunity." 5 U.S.C. § 706(2)(B).

COUNT III
Violation of the Separation of Powers

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

176. This Court has inherent equitable power to enjoin unconstitutional Executive conduct. *See Free Enter. Fund v. Pub. Co. Acct. Oversight Bd.*, 561 U.S. 477, 491 n.2 (2010); *Armstrong v. Exceptional Child Ctr., Inc.*, 575 U.S. 320, 327 (2015).

177. For the same reasons set forth above in Count II, Defendants' actions violate the separation of powers and must therefore be enjoined and declared unlawful.

COUNT IV
Violation of the APA
(Agency Action Contrary to Federalism Principles, the Elections Clause, the Voter Qualifications Clause, and the 17th Amendment)

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

179. Under principles of federalism and the Constitution's Elections Clause, the Voter Qualifications Clause, and the 17th Amendment, states have the presumed primary responsibility and duty to decide who is eligible to vote in both state and federal elections and how to administer the election. This includes deciding how to administer voter registration, maintain voter registration lists, and perform voter list maintenance.

180. The federal government can intrude on that presumed primary authority of state and local election administration only under the circumstances Congress has authorized by statute.

181. Congress has not authorized any part of the federal Executive branch to finalize or implement DOJ's Voter Registration Nationalization Policy by compiling state voter files and

creating a national voter registration system of records in order to federalize the core tasks of voter list maintenance.

182. The federal government has only limited authority under the Constitution concerning a state's voter eligibility decisions. DOJ's effort to implement its Voter Registration Nationalization Policy unlawfully inserts the federal government into making voter eligibility decisions.

183. "An individual has a direct interest in objecting to laws that upset the constitutional balance between the National Government and the States when the enforcement of those laws causes injury that is concrete, particular, and redressable. Fidelity to principles of federalism is not for the States alone to vindicate." *Bond v. United* States, 564 U.S. 211, 222 (2011).

184. Defendants' Policy and associated actions are therefore "contrary to constitutional right, power, privilege, or immunity" and should be enjoined and vacated. 5 U.S.C. § 706(2)(B).

COUNT V
Violation of Federalism Principles, the Elections Clause, the Voter Qualifications Clause, and the 17th Amendment

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

186. This Court has inherent equitable power to enjoin unconstitutional Executive conduct. *See Free Enter. Fund*, 561 U.S. at 491 n.2; *Armstrong*, 575 U.S. at 327.

187. For the same reasons set forth above in Count IV, Defendants' actions violate principles of federalism, the Elections Clause, the Voter Qualifications Clause, and the 17th Amendment and must therefore be enjoined and declared unlawful.

COUNT VI
Violation of the APA
(Agency Action Contrary to the Privacy Act)

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

189. The APA requires courts to "hold unlawful and set aside" agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law," or "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

190. The Privacy Act requires agencies to publish a SORN in the Federal Register whenever they "establish or revise" a "system of records." 5 U.S.C. § 552a(e)(4). And at least 30 days *before* "any new use or intended use of the information in the system," the agency must "publish in the Federal Register notice" of the new use and "provide an opportunity for interested persons to submit written data, views, or arguments to the agency." *Id.* § 552a(e)(11).

191. "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." OMB Circular No. A-108 at 7 & 12. And agencies "shall" review and consider any "public comments on a published SORN." *Id.* at 7.

192. Since May 2025, DOJ has compiled tens of millions of Americans' Confidential Voter List data in the Central CRT Index File, a system of records housed at the Civil Rights Division, and is disclosing that data en masse to DHS and private contractors, performing unreliable list maintenance "verification procedures," and then reporting the unreliable results to the states with instructions to remove purportedly "ineligible voters."

193. Despite substantially modifying the system of records and its usage of the system, DOJ failed to publish a SORN in the Federal Register regarding its use of Confidential Voter List data from the Central CRT File Index as required by 5 U.S.C. § 552a(e)(4).

194. DOJ also failed to publish in the Federal Register notice of "any new use or intended use of the information in the system" at least 30 days before such new use or intended use as required by 5 U.S.C. § 552a(e)(11).

195. DOJ also failed to "provide an opportunity for interested persons to submit written data, views, or arguments to the agency" regarding its use of the Confidential Voter List data as required by 5 U.S.C. § 552a(e)(11).

196. The Privacy Act generally prohibits disclosure of an individual's records from a system of records without their consent unless it fits one of 13 exceptions. *See* 5 U.S.C. § 552a(b)(1)-(13).

197. As part of its Voter Registration Nationalization Policy, DOJ has executed agreements and policies that allow for mass disclosure of Confidential Voter List data from the Central CRT File Index, in bulk, to persons within the agency, to other federal agencies, to private contractors, as well as DOJ's analysis back to states, all in violation of numerous provisions of the Privacy Act.

198. These disclosures, and the policies and agreements authorizing them, violate 5 U.S.C. § 552a(b). They were made without the consent of the individuals whose information DOJ is disclosing, and they fall within no statutory exception or any properly noticed "routine use."

199. The Privacy Act requires that each agency that maintains a system of records take certain steps to ensure the records it "maintains" on individuals are accurate, relevant, up-to-date, and secure, *see* 5 U.S.C. §§ 552a(e)(5), (6), (10), in order to prevent "substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained," *id.* § 552(e)(10). The Act defines "maintain" to include "maintain, collect, use, or disseminate." *Id.* § 552a(a)(3).

200. The Act further prohibits an agency maintaining a system of records from "maintain[ing], collect[ing], us[ing], or disseminat[ing]" "record[s] describing how any individual exercises rights guaranteed by the First Amendment unless expressly authorized by statute or by the individual about whom the record is maintained or unless pertinent to and within the scope of an authorized law enforcement activity." *Id.* §§ 552a(a)(3), (e)(7).

201. By maintaining, collecting, using, and disseminating the Confidential Voter List data, DOJ has violated the Privacy Act by: failing to "maintain all records which are used by the agency in making any determination about any individual with such accuracy, relevance, timeliness, and completeness as is reasonably necessary to assure fairness to the individual in the determination," *id.* § 552a(e)(5); failing to "make reasonable efforts to assure that such records are accurate, complete, timely, and relevant for agency purposes" before "disseminating" the records to persons other than agencies, *id.* § 552a(e)(6); unlawfully maintaining records that "describe[e] how any individual exercises rights guaranteed by the First Amendment," *id.* § 552a(e)(7); and failing to establish "appropriate . . . safeguards" 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," *id.* § 552a(e)(10).

202. Defendants' Policy and associated actions therefore violate the Privacy Act and are "not in accordance with law" and "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

COUNT VII
Violation of the APA
(Agency Action Contrary to the Paperwork Reduction Act)

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

204. The APA requires courts to "hold unlawful and set aside" agency action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law," or "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

205. DOJ's actions, including its prior and ongoing demands for Confidential Voter Lists, as more fully described herein, qualify as a "collection of information" under 44 U.S.C. § 3502(3) (the "Collection of Information").

206. The PRA prohibits a collection of information unless and until an agency (DOJ in this case) complies with its requirements. These requirements include (1) conducting a § 3506(c)(1) review; (2) publishing a 60-day notice in the Federal Register; (3) soliciting and evaluating public comments; (4) submitting a § 3506(c)(3) certification and supporting record to OIRA; (5) publishing a second, 30-day notice in the Federal Register; (6) obtaining approval for the collection of information from OIRA; (7) obtaining a control number issued by OIRA; and (8) displaying the control number as well as a notice that the "agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number" in the collection of information. 44 U.S.C. § 3506(c)(1)(B)(i).

207. DOJ failed to conduct the § 3506(c)(1) review required by 44 U.S.C. § 3507(a)(1)(A)) before initiating the Collection of Information.

208. DOJ failed to publish a 60-day notice in the Federal Register required by 44 U.S.C. § 3506(c)(2)(A)) before initiating the Collection of Information.

209. DOJ failed to solicit public comments as required by 44 U.S.C. § 3507(a)(1)(B) before initiating the Collection of Information.

210. DOJ failed to evaluate public comments as required by 44 U.S.C. § 3507(a)(1)(B) before initiating the Collection of Information.

211. DOJ failed to submit a § 3506(c)(3) certification or record supporting such certification to OIRA as required by 44 U.S.C. § 3507(a)(1)(C) before initiating the Collection of Information.

212. DOJ failed to publish a 30-day notice in the Federal Register as required by 44 U.S.C. § 3507(a)(1)(D) and (b) before initiating the Collection of Information.

213. DOJ failed to obtain approval for the collection of information from OIRA as required by 44 U.S.C. § 3507(a)(2) before initiating the Collection of Information.

214. DOJ failed to obtain a control number issued by OIRA as required by 44 U.S.C. § 3507(a)(3) before initiating the Collection of Information.

215. DOJ failed to display a control number issued by OIRA in its Collection of Information as required by 44 U.S.C. § 3506(c)(1)(B)(i).

216. DOJ failed to display a notice that the "agency may not conduct or sponsor, and a person is not required to respond to, a collection of information unless it displays a valid control number" in its Collection of Information as required by 44 U.S.C. § 3506(c)(1)(B)(i).

217. Defendants' Policy and associated actions therefore violated the PRA and were "not in accordance with law" and "without observance of procedure required by law." 5 U.S.C. §§ 706(2)(A), (D).

COUNT VIII
Violation of the APA
(Arbitrary and Capricious Agency Action)

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

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

220. DOJ's Policy and associated actions to consolidate, use, and disclose the Confidential Voter List data were arbitrary and capricious because, among other things, the agency failed to consider the privacy and data-security risks of its actions, the robust procedures states already have in place to ensure compliance with the NVRA and HAVA, the PRA's requirements for new information collections, the Federal Information Security Modernization Act's requirements for data security, the chilling effect its actions would have on Americans' voting rights, and the reliance interests and reasonable privacy expectations of the millions of Americans who never consented to their voter data being compiled in a centralized federal database housed at DOJ.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs respectfully request that this Court:

1) Declare that DOJ's Voter Registration Nationalization Policy and actions to compile, consolidate, use, and disclose Confidential Voter List data, as well as the associated policies and agreements, are unlawful, *ultra vires*, unconstitutional, and arbitrary and capricious;
2) Hold unlawful, stay, vacate, and set aside DOJ's Voter Registration Nationalization Policy and actions to compile, consolidate, use, and disclose Confidential Voter List data, as well as the associated policies and agreements;

3) Order DOJ to delete, disentangle, and unlink any Confidential Voter List data in its possession, custody, or control;
4) Order DOJ to instruct any party it has provided Confidential Voter List data delete, disentangle, and unlink that data;
5) Order DOJ to publish all information and comply with all procedures mandated by the Privacy Act and PRA for the Confidential Voter List data it has already collected;
6) Enjoin DOJ from disclosing any Confidential Voter List data internally and to non-DOJ personnel, including to other federal agencies, state agencies, or private contractors (of DOJ or any other agency);
7) Grant any temporary, preliminary, or permanent injunctive relief necessary to prevent Defendants' actions from irreparably harming Plaintiffs;
8) Retain jurisdiction to ensure compliance with this Court's orders;
9) Award Plaintiffs their costs and reasonable attorneys' fees incurred in this action; and
10) Grant any other relief this Court deems just and proper.

Dated: April 21, 2026

Respectfully submitted,

/s/ Nikhel S. Sus

Nikhel S. Sus (D.C. Bar No. 1017937)
John B. Hill (N.Y. Bar No. 5505508)*
CITIZENS FOR RESPONSIBILITY
AND ETHICS IN WASHINGTON
P.O. Box 14596
Washington, DC 20044
[redacted]

Sara Chimene-Weiss*
PROTECT DEMOCRACY PROJECT
[redacted]

Jane Bentrott (D.C. Bar No. 1029681)
Naomi Gilens (D.C. Bar No. 90037831)
PROTECT DEMOCRACY PROJECT
[redacted]

Jared Fletcher Davidson*
PROTECT DEMOCRACY PROJECT
[redacted]

John Haubenreich*
PROTECT DEMOCRACY PROJECT
[redacted]

Ming Cheung*
Ari J. Savitzky*
Theresa J. Lee*
Sophia Lin Lakin*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
[redacted]

Laura K. Follansbee (D.C. Bar No. 1782046)
Arthur B. Spitzer (D.C. Bar No. 235960)
AMERICAN CIVIL LIBERTIES UNION
FOUNDATION OF THE DISTRICT OF COLUMBIA
[redacted]

* *Pro hac vice* motion forthcoming

Counsel for Plaintiffs