How Federal Efforts to Access Voter Data Affect Our Privacy, Civil Liberties, and Democracy

A resource in collaboration between the Center for Democracy & Technology, The Leadership Conference's Center for Civil Rights and Technology, and Protect Democracy

Last updated December 12, 2025

Since taking office in January, the second Trump administration has launched a government-wide effort to access and aggregate an unprecedented amount of sensitive personal information on people nationwide. Following a March executive order directing federal agencies to expand their access to sensitive personal data held by other agencies and states, the administration has taken extraordinary steps to acquire Americans' personally identifiable information (PII). As part of this effort, the Department of Justice (DOJ) has demanded access to at least 40 states' voter files, which often contain sensitive personal information such as social security and driver's license numbers.

The DOJ's demands for access to state voter registration data are likely connected to the administration's efforts to investigate unfounded claims of widespread non-citizen voting by matching state voter registration data with federal immigration datasets using the Department of Homeland Security's (DHS) Systematic Alien Verification for Entitlements (SAVE) system. This attempt to collect state voter data has occurred in parallel with efforts to repurpose the SAVE system as a voter and citizenship verification tool by expanding the system to include additional personal data from other federal agencies. While framed as measures to enhance election integrity, these actions could infringe on states' constitutional authority to administer elections; perpetuate false narratives that erode trust in elections; facilitate the unjust targeting of immigrants; and raise urgent concerns about the privacy, legality, and the potential for misuse of the sensitive personal information contained in voting records.

At a time when trust in our democracy is eroding, the aggregation of voter data and other personal information threatens to undermine both electoral participation and civil liberties. This explainer is intended to inform stakeholders of the details and implications of the administration's latest privacy-invasive actions. It covers:

- **Background on voter registration data**, including past attempts by the federal government to access this information and the types of sensitive data in voter rolls;
- **The SAVE system**, including recent efforts to repurpose the system for voter and citizenship verification;

- **The legal landscape** surrounding federal attempts to access voter data; and
- **The impact to individuals** when voter registration data is misused, exposed, or exploited.

Background on Voter Registration Data

Every state is responsible for maintaining its own voter file, a digital database of information on all registered voters in that state. State voter files are highly sensitive and ripe for misuse, as they often contain PII, such as social security numbers (SSNs), driver's license numbers, dates of birth, and other private personal data.

What is the history of past attempts to collect voter data?

While the federal government has made previous attempts to collect sensitive state voter registration information, the administration's current effort is by far the largest and most sweeping in U.S. history — even surpassing the attempt made by President Trump's first administration. In 2017, the Presidential Advisory Commission on Election Integrity (also known as the Pence-Kobach commission) requested voter registration data from every state, including names, addresses, birthdates, partial SSNs, party affiliation, and history of incarceration.

The administration's efforts were later abandoned after significant legal pushback from a bipartisan group of states and fierce opposition from the civil rights and pro-democracy communities. In total, 44 states declined to provide the full list of requested information to the Commission, citing privacy and data security concerns — including Kansas and Maine, whose Secretaries of State were members of the Commission. Mississippi's Secretary of State famously responded to the request: "they can go jump in the Gulf of Mexico, and Mississippi is a great state to launch from."

What data is included in a state voter file?

State voter files are made up of information compiled by election administrators and collected from state voter registration applications, which vary by state.

All states collect:	**Some states collect additional information, such as:**
• Name • Residential address • Certain PII, such as full or partial SSN, driver's license number, and/or state ID number	• Political party affiliation • Phone number • Email address • Voting history (if a person voted, not how they voted) • Voting method (absentee, in-person, etc.)

Source: FAQs: Public Voter Registration Information and Security of State Voter Registration Databases

Background on Voter Registration Data (cont.)

How much of this information is publicly available?

Public access to voter registration data also varies by state. State laws and policies define who can request a public version of the voter file, how the data may be used, what information is kept confidential, and the cost for obtaining the file.

The public version of the voter file does not contain all of the information in the state-held version. In most states, the publicly available file contains information about voter eligibility, including a voter's address, age, district, precinct, and polling location. No state makes available a voter's full SSN, driver's license number, or state ID number.

Illustrative State Laws Governing Public Access to State Voter Rolls

State	Who can request a copy?	How much does the copy of the file cost?	What data is included?	What is excluded?
Alabama	Anyone	~$37,000 (priced at one cent per record, estimated cost of purchasing full voter file containing records on all ~3.7 million registered voters in Alabama)	• Name • Voter status • Address • Phone number • Birth year • Voting history • Registration date • Race • Sex • Precinct • District • Last election voted in	• SSN
Minnesota	Any registered Minnesota voter	$46	• Name • Address • Birth year • Voting history • Phone number • Voting district	• SSN • Driver's license number • ID card number • Military ID number • Passport number • Day/month of birth
Vermont	Anyone	$0	• Name • Address • Birth year	• Last four digits of SSN • Driver's license number • Day/month of birth

Sources: 17 V.S.A. § 2154; 17 V.S.A. § 2141; Vermont SOS FAQs; Minn. Stat. § 201.091; Minnesota Registered Voters List Request Form; Ala. Code § 17-4-38; Alabama Public Inspection of Voter Registration Information.

Background on Voter Registration Data (cont.)

Why is the file public?

Public voter registration data is a critical tool for protecting democracy and the rights of voters in the U.S. It supports:

- **Trust in elections and government:** Transparency of state voter registration data is important for maintaining trust in the integrity of elections and the legitimacy of elected officials by allowing outside groups to provide oversight of the government's use of administrative resources and election processes.

- **Election security:** Public visibility into voter registration data can serve as a deterrent to hackers and foreign adversaries because it makes it harder for bad actors to alter or manipulate the data without detection.

- **Voting rights:** Publicly available voter rolls can help advocates, scholars, journalists, and other members of the public ensure election officials are complying with voting rights laws and are not taking actions to deny anyone their right to vote, especially those from marginalized groups.

- **Campaign equity:** Candidates, campaigns, and "get out the vote" initiatives rely on public voter registration data to identify and communicate with eligible voters. Limiting public access to this data could provide an advantage to incumbent or tenured candidates who have existing contact bases and could disadvantage challengers and referendum advocates.

Why does the Trump administration want this data?

The data that the DOJ is demanding from states in most instances is far more extensive than what is available in states' public files. The DOJ specifically requested access to all fields of states' voter registration databases, including driver's license numbers and partial SSNs.

The DOJ's demands for this data are likely related to its efforts to identify instances of alleged non-citizen voting by matching the requested state voter registration data with federal immigration datasets using the SAVE system. However, research consistently shows that non-citizen voting is exceedingly rare, and, as discussed below, the SAVE system is known to contain outdated information (including immigration status). These data quality issues could disenfranchise American citizens by incorrectly identifying ineligible voters.

The administration's effort to lay claim to this state voter data is also part of a larger government-wide effort to collect and aggregate unprecedented amounts of sensitive information on millions of people nationwide.

Background on Voter Registration Data (cont.)

In addition to state voter files, the administration has demanded that states share sensitive data from public benefit programs like the Supplemental Nutrition Assistance (SNAP) Program and Medicaid, and has demonstrated an unprecedented willingness to share and aggregate sensitive data across federal agencies like the Social Security Administration (SSA) and the Internal Revenue Service (IRS).

The SAVE System

The SAVE system, which is administered by DHS's U.S. Citizenship and Immigration Services (USCIS), was designed to help federal and state officials determine documented non-citizens' and recently naturalized citizens' eligibility for government benefits. DHS is now expanding and repurposing the SAVE system beyond benefits administration, specifically for voter verification and immigration enforcement, raising risks related to privacy, voter disenfranchisement, and improper immigration enforcement.

How is the SAVE system being changed and repurposed?

DHS filed a system of records notice (SORN) on October 31, 2025 that outlined changes to the SAVE system. Many of these changes had been previously made public, including an agreement between DHS and the SSA to merge SSA data with the SAVE system, a move that raises cybersecurity and privacy concerns and could lead to matching errors resulting in the improper disenfranchisement of eligible voters. Key changes include:

- **Expanding the system to include U.S. citizens by birth, and using it to verify their voter eligibility and citizenship status.** This fundamentally repurposes the system from a more modest immigration status look-up tool used in some public benefits administration processes to what effectively functions as a national citizenship database, which has never previously existed or been sanctioned. On the contrary, the U.S. government attempted to prevent the creation of an official or de facto national data bank by passing the Privacy Act of 1974. Including U.S. citizens by birth in the system raises the risk of disenfranchisement or erroneous immigration enforcement.

- **Adding additional categories of records in the system to include full and partial SSN, U.S. passport number, driver's license number, and information from SSA.** The database was previously searchable using a DHS immigration identifier number, consistent with the purpose of verifying immigration status. The SORN outlines using state data sources including via inter-governmental data-sharing networks (e.g. the National Law Enforcement Telecommunications System). Linking records across databases by state driver-license numbers is far afield from immigration status verification, and reflects the sudden expansion of SAVE from a specific tool for citizenship verification in specific contexts into a national identity verification tool.

The SAVE System (cont.)

- **Expanding the uses of the data** to include sharing with SSA and with other federal agencies, including to "support auditing of federal programs administered by state, local, and tribal governments (e.g. Medicaid)."

- **Allowing bulk searches.** Verification was previously executed by manually entering information for individual cases. Allowing bulk searches may increase the risk that states will not undertake the necessary but time-consuming steps of verifying incomplete or negative findings, which the system depends on to limit the risk of the system producing inaccurate results.

Many of these changes appear to have been put in place before the SORN was published, in violation of the Privacy Act of 1974, which requires agencies to provide the public with 30 days' advanced notice and the opportunity to provide public comment before implementing new routine uses (5 U.S.C. § 552a(e)(11)). The belated SORN does not undo the harms created by that delay or the rapid rollout of changes that could exacerbate data matching issues.

How is SAVE related to voter verification?

While the SAVE system was originally intended for benefits eligibility verification, states and election officials have used it for voter verification in recent years. For example, a 2023 Mississippi law requires election officials to use the SAVE database in voter registration verification processes. In August, the Trump administration began pressuring states to use the SAVE system for voter verification in order to receive federal election security grants. In November of this year, USCIS announced that 26 states have signed or are in the process of signing agreements with DHS to use the SAVE system to verify voter eligibility.

However, the data quality issues in the SAVE system have hampered efforts to use the tool for voter verification. When Texas tested using the SAVE system for voter verification earlier this year, nearly 300 out of 1,657 searches (or approximately 18 percent) returned errors due to duplicate data or incompatible data formats.

Efforts to expand access to voter registration data and repurpose the SAVE system for broader uses must be understood in the context of unfounded narratives about voter fraud and the recent push to require proof of citizenship to register to vote. Non-citizen voting is illegal in federal elections and is exceedingly rare. Yet there have been multiple efforts at the state and federal level to require proof of citizenship to vote. In March, President Trump signed an executive order requiring registrants to provide proof of citizenship when filling out the federal voter registration form, and in April the House passed the SAVE Act in an attempt to impose a similar requirement. The executive order's citizenship provision was preliminarily enjoined by a Washington, D.C. federal district court in April 2025, then permanently enjoined in October.

The SAVE System (cont.)

Moreover, the changes to SAVE outlined above are not necessary for voter verification. Election officials already have clear, well-established processes for verifying eligible voters and conducting voter list maintenance. ERIC (Electronic Registration Information Center), for example, is a tool created by bipartisan election officials to enable private, secure interstate data sharing for the purpose of identifying voters who have died, moved, or become otherwise ineligible to vote. While some states have withdrawn from ERIC after it became the target of unfounded conspiracy theories, a development that potentially makes the repurposed SAVE system more appealing, relying on an expanded SAVE system is a less efficient option that introduces serious privacy, security, and accuracy issues.

Legal Landscape

Since the DOJ began its campaign to access state voter registration data in May, state officials from across the political spectrum have challenged the legality of these requests and taken steps to protect the privacy and security of their voters' sensitive personal information.

Of the 40 states that have received demands for copies of their statewide voter registration files, only two — Indiana and Wyoming — have provided their full, unredacted statewide voter registration data. Instead, most states have only provided the publicly available version of their voter file or not provided the file at all. As of the date of publication of this explainer, the DOJ has sued 18 states over their refusal to provide the full data, and in two other states registered voters have sued to prevent state election officials from disclosing their data. The states that have challenged the DOJ's requests have pointed to a number of legal principles, including constitutional principles, federal voting rights laws, federal privacy statutes, and state privacy laws.

Constitutional Principles and States' Authority

In their challenges to the DOJ's demands, states have argued that federal intrusion into state voter data undermines states' constitutional authority to run their own elections and threatens the decentralized nature of U.S. elections. Article 1, Section 4 of the Constitution, commonly referred to as the Elections Clause, gives states the power to determine "The Times, Places and Manner" of federal elections, which has historically included responsibility for administering the voter registration process and conducting voter registration list maintenance. The decentralization of elections is an important feature of American democracy that protects against federal interference in election results, enhances the security of election data, and empowers state and local election officials to set election policies that are directly responsive to the needs of their communities. The DOJ demands and threats of sanctions risk undermining that deliberately decentralized system.

Legal Landscape (cont.)

Federal Voting Rights Laws

The DOJ has demanded access to states' voter rolls under the auspices of ensuring state compliance with three varying federal voting rights laws: the Help America Vote Act (HAVA), the National Voter Registration Act (NVRA), and the Civil Rights Act of 1960 (CRA). In ongoing litigation, states have challenged the DOJ's authority to access voters' sensitive personal data under these statutes.

HAVA and the NVRA each have provisions requiring states to conduct voter list maintenance (52 U.S.C. § 20507(c)–(g); 52 U.S.C. § 21083(a)(2)). In its demands to states, the DOJ has asserted that in order to evaluate states' compliance with these provisions, it must review not only states' processes for voter registration list maintenance, but also each state's list itself, including sensitive personal information beyond what is typically available. However, this reasoning falls short, as the unredacted lists that DOJ is after likely are not needed for the DOJ to evaluate NVRA and HAVA compliance. Full information about every individual registered to vote, including, for example, SSNs or driver's license numbers, is not relevant to determining whether a state has proper list maintenance procedures as required by these statutes.

The CRA permits the DOJ to request certain election-related records; however, all record requests must be accompanied by a written "statement of the basis and the purpose" of the request, a requirement that states have alleged the DOJ has failed to fully comply with (52 U.S.C. § 20703). States have also argued that the DOJ's attempts to use the CRA to access and aggregate sensitive personal information on registered voters run counter to the purpose of the statute, which was enacted with a specific purpose: to protect against the unconstitutional disenfranchisement of voters based on race and expand voting access (H.R. Rep. 86-956 at 1944 (1959)).

Federal Privacy Statutes

The Privacy Act regulates the federal government's custody of individual's personal information, requiring federal agencies initiating a new data collection to publish a SORN, or a public notice, in the Federal Register, in which the agency identifies the purpose for which information about an individual is collected, from whom it is being collected, what type of information is collected, and how that information will be shared with other agencies (5 U.S.C. § 552(a)). Some states, including Maine and Michigan, have noted the DOJ's failure to comply with the procedural requirements under the Privacy Act as further grounds for denying the DOJ's request for their voters' sensitive personal data. Seemingly in response to legal pressure, DHS belatedly published a SORN months after DOJ's initial demands for the information and the expansion of the SAVE system for voter verification.

Legal Landscape (cont.)

The Paperwork Reduction Act requires that agencies collecting certain information, or modifying an existing collection of information, must obtain approval from the Office of Management and Budget (OMB) following a series of procedural steps, including providing the public with notice and the opportunity to comment (44 U.S.C. § 3507(h)(3)). The DOJ's demands for state voter data and DHS's recent modifications of the SAVE system — for example, to collect social security numbers — appear to have been executed without regard for the Paperwork Reduction Act's requirements.

State Privacy Laws

Many states have laws that protect the personal information in voter rolls from disclosure. These vary from state to state but are commonly in place to protect private sensitive information such as SSNs and driver's license numbers. Some states have noted that complying with the DOJ's demands would force them to violate their own state laws. Multiple federal courts have held that states may redact uniquely sensitive personal information when providing access to voter roll information in compliance with the NVRA (*Project Vote/Voting for Am., Inc. v. Long*, 682 F.3d 331 (4th Cir. 2012); *Pub. Int. Legal Found., Inc. v. N. Carolina State Bd. of Elections*, 996 F.3d 257 (4th Cir. 2021); *Pub. Int. Legal Found., Inc. v. Bellows*, 92 F.4th 36 (1st Cir. 2024)).

Impacts

The administration's efforts to access and aggregate voter registration data and attempts to match that information against outdated data in the hastily expanded SAVE system threaten our privacy and undermine core democratic protections. These moves are part of a larger effort to collect and aggregate an unprecedented amount of sensitive information on people nationwide, the impacts of which include:

- **Putting our personal data at risk.** The expanded SAVE system connects and centralizes highly sensitive data from a number of sources making it a prime target for hackers. Inappropriate access to personal data exposes individuals to fraud as well as political retaliation or harassment, like doxxing. This threat is especially concerning given the administration's track record of poor cybersecurity practices.

- **Further eroding privacy rights.** Federal access to state voter registration data, especially when matched with other government data, fundamentally threatens the privacy of all people living in the U.S. The administration's efforts to create a single federal source of citizenship and voting data far exceeds the reason why the underlying data was originally collected and provides access beyond Americans' consent.

Impacts (cont.)

- **Unjustly targeting immigrants.** The expanded SAVE system could be abused as a tool for stepped-up immigration enforcement. Outdated, missing, incomplete, or incorrect information within the SAVE system could lead to errors that result in wrongful immigration enforcement. Furthermore, the increased collection of government data also has chilling effects on the speech of non-citizens, advocates for non-citizens, and those who fear they could be profiled for immigration enforcement, especially when data is augmented by private data from data brokers. The unwarranted focus on non-citizen voting may also lead to false accusations or even charges of illegal voting and other intimidation tactics among communities with high immigrant populations, all of which could deter voting by naturalized citizens in mixed-status families.

- **Disenfranchising eligible voters.** The way the administration is planning to use this data may dissuade citizens (both citizens by birth and naturalized or derived citizens) from exercising their right to vote over fears about how their data will be used. The use of the SAVE system may result in data matching errors that could prevent eligible voters from registering to vote or voting, or lead to wrongful referral for criminal prosecution of citizens who have lawfully voted in the past.

- **Eroding trust in elections.** Raising baseless doubts about voter fraud and voter roll integrity will unnecessarily erode trust in our elections and make it seem like future election results are unknowable, paving the way for election denial. In particular, a focus on voter data and the SAVE system may contribute to existing false narratives about election fraud, especially regarding widespread non-citizen voting, and could bolster any potential election subversion attempts during the upcoming 2026 and 2028 elections.

The Trump administration's efforts to access and repurpose voter registration data are alarming. By combining voter rolls with sensitive data from across the government, this administration is seeking to build the functional equivalent of a massive, centralized repository of our PII. This unprecedented consolidation of data not only threatens our privacy and opens the door to misuse, surveillance, and discrimination — it threatens to undermine the democratic process itself.

Questions? Contact elections@cdt.org, techcenter@civilrights.org, or techanddata@protectdemocracy.org.