



Explainer: Can the Federal Government Force States to Hand Over Citizens' Voter Information?

Derek Clinger, Senior Counsel

Published: December 19, 2025

Update: As of March 6, 2026, the Justice Department is suing 29 states and the District of Columbia for their sensitive voter data. Federal district courts have dismissed the Justice Department's lawsuits against California, Michigan, and Oregon, holding that federal law does not require states to turn over their sensitive voter data. The district court in the California case also found that the Justice Department's demands violate federal privacy laws. The Justice Department has appealed all three decisions. Read the [California](#), [Michigan](#), and [Oregon](#) opinions.

For more up-to-date information on the DOJ's lawsuits seeking states' sensitive voter data, [see our tracker here](#)

In late October 2025, Michigan Secretary of State Jocelyn Benson released an unusual video message “warning” the state’s residents that the U.S. Justice Department was “unlawfully demanding” their private voter information.¹ “Why do they want access to your personal information?” asked Benson.² “I’ve asked them that. Other secretaries of state— both Democrats and Republicans—have asked them that.³ They won’t tell us.” Her message was blunt: “Nobody—

¹ Press Release, Jocelyn Benson, Sec’y of State, State of Mich., *Secretary Benson Warns Michiganders: U.S. Department of Justice Is Unlawfully Demanding Your Private Voter Information* (Oct. 24, 2025), <https://www.michigan.gov/sos/resources/news/2025/10/24/benson-warns-us-doj-is-unlawfullydemanding-your-private-voter-information>.

² *Id.*

³ *Id.*

not the president, the DOJ or any other federal agency has the right to your sensitive, private voter information.”⁴

Benson’s warning was not unique. Elections officials from dozens of states—red and blue— have raised similar questions as the Justice Department has demanded complete voter registration lists from at least 40 states, including highly sensitive data like Social Security numbers and driver’s license numbers.⁵ The controversy reflects a deepening, and increasingly public, conflict between the federal government and the states over how elections are run and who has the power to administer them.

Since returning to office in January 2025, President Trump has pursued efforts to expand federal control over the country’s historically state-run election infrastructure. In March 2025, he issued a sweeping executive order that, among other provisions, sought to require documentary proof of citizenship to register to vote in federal elections—a requirement that has since been blocked by a federal court.⁶ Over the summer, reports indicated that the Justice Department was exploring ways to prosecute local election officials who the administration believes have not sufficiently followed certain security standards.⁷ President Trump also declared on social media that he would seek to eliminate mail voting and vote machines ahead of the 2026 midterm elections, inaccurately portraying states as “merely an ‘agent’ for the Federal Government” in the administration of federal elections.⁸

The Justice Department’s demands for state voter registration lists—which prompted Benson’s warning—came as part of letters sent to election administrators beginning in the spring of 2025.⁹ In addition to seeking details about how the state handles different aspects of election

⁴ *Id.*

⁵ See Kaylie Martinez-Ochoa, Eileen O’Connor & Patrick Berry, *Tracker of Justice Department Requests for Voter Information*, BRENNAN CTR. FOR JUST. (Dec. 12, 2025), <https://www.brennancenter.org/ourwork/research-reports/tracker-justice-department-requests-voter-information> (last visited Dec. 14, 2025).

⁶ Exec. Order No. 14248, 90 C.F.R. 14005 (2025); *League of United Latin Am. Citizens v. Exec. Off. of the President*, ___ F.Supp.3d ___, 2025 WL 3042704 (D.D.C. Oct. 31, 2025).

⁷ Devlin Barrett & Nick Corasaniti, *Justice Dept. Explores Using Criminal Charges Against Election Officials*, N.Y. TIMES (July 2, 2025), <https://www.nytimes.com/2025/07/02/us/politics/justice-department-electiondata.html>.

⁸ See, e.g., Ashley Lopez & Ari Shapiro, *Trump Announces on Truth Social that He’ll Ban Mail-In Voting and Voting Machines*, ALL THINGS CONSIDERED (Aug. 18, 2025, at 16:11 ET), <https://www.npr.org/2025/08/18/nxs1-5506137/trump-announces-on-truth-social-that-hell-ban-mail-in-voting-and-voting-machines>; John Yang & Harry Zahn, *Does Trump Have the Power To End Mail-In Voting? Legal Scholar Weighs In*, PBS NEWS WEEKEND (Aug. 23, 2025, at 17:40 EST), <https://www.pbs.org/newshour/show/does-trump-have-the-power-to-end-mail-in-voting-legal-scholar-weighs-in>.

⁹ See Martinez-Ochoa, O’Connor & Berry, *supra* note 5.

administration, these lengthy letters also sought each state’s complete, unredacted voter registration lists. These lists include basic identifying information, like each voter’s name and registration address, as well as more sensitive personal information, like birthdates, driver’s license numbers, and partial Social Security numbers¹⁰—information that laws in every state protect from public disclosure.

The Justice Department claims it needs complete voter registration lists to determine whether states are complying with their obligations under federal law to make “reasonable efforts” to maintain accurate voter rolls,¹¹ but legal experts and state officials have questioned this purported rationale. Media reports have indicated that the Justice Department has been sharing voter data with the Department of Homeland Security, potentially to run citizenship checks. The Justice Department and DHS have offered divergent statements about whether such data sharing is occurring, prompting state election officials to demand more clarity.^{12,13} Some observers have suggested that the Trump administration is attempting to create a national voter registration database,¹³ sparking privacy concerns.¹⁴ And many worry that these federal-level activities—which are largely spearheaded by individuals who participated in President Trump’s ill-fated efforts to challenge the results of the 2020 election—are part of a larger effort to sow distrust in the elections system ahead of the 2026 midterm elections.¹⁵

Whatever the Justice Department’s purpose, states have mostly declined to provide their full, unredacted voter registration lists, citing their privacy laws and instead offering publicly available versions that do not include more sensitive information.¹⁶ Indeed, of the more than 40 states

¹⁰ See *id.*

¹¹ See *infra* note 18.

¹² See Jonathan Shorman, *DOJ Is Sharing State Voter Roll Lists with Homeland Security*, STATELINE (Sept. 12, 2025, at 12:38 CT), <https://stateline.org/2025/09/12/doj-is-sharing-state-voter-roll-lists-withhomeland-security/>; Nick Corasaniti, *Election Officials Press Trump Administration Over Voter Data*, N.Y. TIMES (Nov. 18, 2025), <https://www.nytimes.com/2025/11/18/us/politics/election-officials-trump-voterdata.html>.

¹³ See Jonathan Shorman, *Some Republican States Resist DOJ Demand for Private Voter Data*, STATELINE (Sept. 18, 2025, at 05:00 CT), <https://stateline.org/2025/09/18/some-republican-states-resist-dojdemand-for-private-voter-data/>.

¹⁴ The first Trump administration unsuccessfully attempted to build a such a database in 2017. See Justin Levitt, *All Your Voter Data Are Belong to Us*, TAKE CARE BLOG (June 30, 2017), <https://takecareblog.com/blog/all-your-voter-data-are-belong-to-us>; Brennan Center for Justice, *Examples of Legal Risks to Providing Voter Information to Fraud Commission* (2017), https://www.brennancenter.org/sites/default/files/analysis/Legal_Implications_of_Kobach_Request.pdf?inline=1.

¹⁵ See Jasleen Singh, *The Trump Administration’s Campaign to Undermine the Next Election*, BRENNAN CTR. FOR JUST. (Aug. 3, 2025), <https://www.brennancenter.org/our-work/research-reports/trumpadministrations-campaign-undermine-next-election>.

¹⁶ See Martinez-Ochoa, O’Connor, and Berry, *supra* note 5.

known to have received such demands, as of the date of publication, the Justice Department has indicated that only 10 states—including Indiana, Louisiana, Mississippi, Tennessee, and Wyoming—have either provided their full voter registration lists or indicated they plan to do so.¹⁷

Faced with this widespread pushback, the Justice Department has escalated the dispute, filing lawsuits in federal court against 24 states (so far)—Arizona, California, Colorado, Connecticut, Delaware, Georgia, Hawaii, Illinois, Maine, Maryland, Michigan, Massachusetts, Minnesota, Nevada, New Hampshire, New Mexico, New York, Oregon, Pennsylvania, Rhode Island, Vermont, Virginia, Washington, and Wisconsin—plus D.C. in an effort to compel the states to turn over their complete voter registration lists.¹⁸ The Justice Department is also pursuing a similar case against Orange County, California,¹⁹ and Trump administration allies at the Republican National Committee have filed lawsuits under state public records laws against Hawaii and New Jersey, similarly seeking copies of the states’ voter registration data that they have been denied to date.²⁰

¹⁷ See Press Release, U.S. Dep’t of Just., *Justice Department Sues Four States for Failure to Produce Voter Rolls* (Dec. 18, 2025), <https://www.justice.gov/opa/pr/justice-department-sues-four-states-failure-produce-voter-rolls>; Martinez-Ochoa, O’Connor, and Berry, *supra* note 5.

¹⁸ See Press Release, U.S. Dep’t of Just., *Justice Department Sues Oregon and Maine for Failure to Provide Voter Registration Rolls* (Sept. 16, 2025), <https://www.justice.gov/opa/pr/justice-department-sues-oregon-and-maine-failure-provide-voter-registration-rolls>; Press Release, U.S. Dep’t of Just., *Justice Department Sues Six States for Failure to Provide Voter Registration Rolls* (Sept. 25, 2025), <https://www.justice.gov/opa/pr/justice-department-sues-six-states-failure-provide-voter-registration-rolls>; Press Release, U.S. Dep’t of Just., *Justice Department Sues Six Additional States for Failure to Provide Voter Registration Rolls* (Dec. 2, 2025), <https://www.justice.gov/opa/pr/justice-department-sues-six-additional-states-failure-provide-voter-registration-rolls>; Press Release, U.S. Dep’t of Just., *Justice Department Sues Four Additional States and One Locality for Failure to Comply with Federal Elections Laws* (Dec. 12, 2025), <https://www.justice.gov/opa/pr/justice-department-sues-four-additional-states-and-one-locality-failure-comply-federal>; Press Release, U.S. Dep’t of Just., *Justice Department Sues Four States for Failure to Produce Voter Rolls* (Dec. 18, 2025), <https://www.justice.gov/opa/pr/justice-department-sues-four-states-failure-produce-voter-rolls>; Press Release, U.S. Dep’t of Just., *Justice Department Sues Arizona and Connecticut for Failure to Produce Voter Rolls* (Jan. 6, 2026), <https://www.justice.gov/opa/pr/justice-department-sues-arizona-and-connecticut-failure-produce-voter-rolls>; Press Release, U.S. Dep’t of Just., *Justice Department Sues Virginia for Failure to Produce Voter Rolls* (Jan. 16, 2026), <https://www.justice.gov/opa/pr/justice-department-sues-virginia-failure-produce-voter-rolls>.

¹⁹ See Press Release, U.S. Dep’t of Just., *Justice Department Files Suit Against Orange County California Registrar of Voters for Refusing to Provide Non-Citizen Voter Removal Records in Violation of Federal Election Laws* (June 25, 2025), <https://www.justice.gov/opa/pr/justice-department-files-suit-againstorange-county-california-registrar-voters-refusing>.

²⁰ While these lawsuits seek similar information, they arise under state public records laws and are brought by private litigants rather than the Justice Department. As a result, they do not raise the same federalstate tensions that this explainer addresses. They do, however, underscore the breadth of efforts by the Trump administration and its allies to obtain voter registration data through any available means. See Richard

These standoffs implicate the long-established authority of states to administer elections and raise fundamental questions about the scope of the federal government’s role in the voter registration process. This explainer examines these issues. Part I provides background on voter registration in the United States, explaining how states are largely responsible for administering voter registration for federal elections, subject to certain federal requirements. Part II explores states’ obligations to protect the privacy of their citizens’ voter registration data. Part III discusses the key legal questions now reaching the courts: What information does federal voting law require states to disclose to the Justice Department? To what extent can states redact sensitive information like Social Security numbers and driver’s license numbers? And what limits exist on federal authority to access such information? Finally, Part IV examines potential legal options that citizens may have to protect their sensitive information when their states may be more willing to comply with federal demands.

I. State Administration of Voter Registration Under Federal Law

Since voter registration laws became common in the late nineteenth century, the administration of voter registration has primarily been the responsibility of state and local election officials, not the federal government. This arrangement stems from the Elections Clause of the U.S. Constitution, which directs states to administer elections for federal office by setting “the Times, Places and Manner” of such elections, while granting Congress the authority to “make or alter such Regulations.”²¹ As detailed below, Congress has imposed certain federal requirements on state voter registration systems—most notably through the National Voter Registration Act of 1993 (NVRA) and the Help America Vote Act of 2002 (HAVA)—but the tasks of registering voters and maintaining voter lists remain largely in the states’ hands.

A. The National Voter Registration Act

Although Congress enacted key voting rights legislation in the mid-twentieth century to curb discriminatory voting practices, the U.S. did not have a national voter registration law until 1993, when Congress passed the National Voter Registration Act (also known as the “Motor Voter”

Wiens, *Republican National Committee Sues Hawai’i Over Voter Rolls*, HONOLULU CIV. BEAT (Oct. 14, 2025), <https://www.civilbeat.org/2025/10/republican-national-committee-sues-hawaii-over-records-onvoter-rolls/>; Nicholas Malfitano, *Republican National Committee Sues State over Voter Maintenance Records* Access, LAW.COM (Nov. 19, 2025, at 15:19 ET), <https://www.law.com/njlawjournal/2025/11/19/republican-national-committee-sues-state-over-votermaintenance-records-access/?slreturn=20251120075906>.

²¹ U.S. Const. art. I, § 4.

law).²² The NVRA aimed to increase voter registration rates by requiring states to provide at least three specified opportunities for registration: registration when applying for a driver’s license; registration by mail; and registration at designated public agencies.²³ (A small number of states—Idaho, Minnesota, New Hampshire, North Dakota, Wisconsin, and Wyoming—are exempt from the NVRA’s requirements because they either had no registration requirement or allowed election-day registration when the law took effect.²⁴) The law also led to the creation of a standardized federal voter registration form (although states can and do continue to use their own state-specific forms as well).²⁵

Beyond seeking to increase voter registration, the NVRA imposed obligations on state and local election officials to maintain accurate voter registration lists.²⁶ Specifically, it requires officials to “conduct a general program that makes a reasonable effort” to identify and remove ineligible voters who have died or moved.²⁷ Federal courts have interpreted this standard as modest. As the Sixth Circuit recently noted in upholding Michigan’s compliance, the NVRA “does not require a perfect effort, nor does it require the most optimal effort, nor does it even require a very good effort,” but instead “only requires a reasonable effort.”²⁸ In other words, the law gives states significant discretion in how they conduct their list maintenance programs.²⁹

The NVRA also includes two provisions to promote state implementation. First, it requires states to keep records of their list maintenance programs and “make [them] available for public inspection,” enabling the public to assess whether states are meeting their obligations under the law.³⁰ Second, the NVRA authorizes both the U.S. Attorney General and private litigants to bring civil lawsuits against states to enforce compliance.³¹ But as these provisions themselves indicate, responsibility to administer voter registration continues to rest chiefly with state and local elections officials, rather than federal officials.

²² Alexander Keyssar, *THE RIGHT TO VOTE* 253–57 (2d ed. 2009); see also Michael Morse, *Democracy’s Bureaucracy: The Complicated Case of Voter Registration Lists*, 103 B.U. L. REV. 2123 (2023) (analyzing the history and provisions of the NVRA and HAVA).

²³ Cf. 52 U.S.C. § 20501; 52 U.S.C. § 20506.

²⁴ 52 U.S.C. § 20503(b). See also U.S. DEP’T OF JUST., *The National Voter Registration Act of 1993 (NVRA)*, <https://www.justice.gov/crt/national-voter-registration-act-1993-nvra> (last visited Nov. 20, 2025).

²⁵ See 52 U.S.C. § 20508.

²⁶ See 52 U.S.C. § 20501(b)(4).

²⁷ 52 U.S.C. § 20507(a)(4).

²⁸ *Pub. Int. Legal Found., Inc. v. Benson*, 136 F.4th 613, 628 (6th Cir. 2025).

²⁹ See Morse, *supra* note 22 at 2140–41.

³⁰ 52 U.S.C. § 20507(i).

³¹ 52 U.S.C. § 20510.

B. The Help America Vote Act

Congress enacted another significant federal voter registration requirement in 2002 with the Help America Vote Act, which responded to problems exposed during the razor-thin 2000 presidential election. Among its many provisions, HAVA required states to create and maintain a computerized, *statewide* voter registration list³²—a major shift from the prior system in which voter rolls were managed primarily at the local level.³³

Building on the NVRA, HAVA also established “minimum standards” to maintain the accuracy of these statewide lists. These include requirements for a “system of file maintenance that makes a reasonable effort to remove registrants who are ineligible to vote from the official list of eligible voters” and “[s]afeguards to ensure that eligible voters are not removed in error from the official list of eligible voters.”³⁴ Still, HAVA expressly left the details of implementation to the states, providing broad discretion over how to meet these federal requirements.³⁵

HAVA’s enforcement mechanisms are limited. In contrast to the NVRA, HAVA does not include language requiring states to make records of their list maintenance programs public³⁶—an omission that may prove significant in the Justice Department’s lawsuits, discussed below in Part III.B. And while HAVA authorizes the U.S. Attorney General to bring enforcement actions, it does not permit private lawsuits.³⁷ Instead, states must establish an administrative complaint procedure to address grievances.³⁸

II. State Privacy Protections for Voter Registration Data

States’ voter registration lists contain highly sensitive personal information, including birthdates, driver’s license numbers and partial Social Security numbers—data that creates significant risks of identity theft and misuse. These risks are not theoretical: In 2016 and 2017, an advocacy organization published lists of Virginia voters whom the organization accused of illegally registering to vote and included the voters’ names,

³² 52 U.S.C. § 21083.

³³ See Morse, *supra* note 22 at 2140, 2144–45.

³⁴ 52 U.S.C. § 21083(a)(4).

³⁵ 52 U.S.C. § 21085.

³⁶ Cf. 52 U.S.C. §§ 21081–21085.

³⁷ 52 U.S.C. § 21111.

³⁸ 52 U.S.C. § 21112.



addresses, and sometimes even complete Social Security numbers.³⁹ The organization later removed the data and apologized as part of a legal settlement,⁴⁰ but the incident underscored the need to protect private voter data.

To safeguard the personal details they collect from voters, states offer a range of privacy protections. Many of these laws are specific to voter lists, while others more generally shield private information from state public records laws. In addition, states may have obligations to protect their citizens' data under federal law, such as the Privacy Act of 1974. This Part explores these different privacy protections.

A. State laws specific to voter registration information

States take varied approaches to protecting voter registration information. Among other things, states commonly limit what data is publicly available, restrict who may access voter lists, and impose conditions on how voter information can be used.

Most states have laws that restrict disclosure of highly sensitive voter data, such as full birthdates, driver's license numbers and partial Social Security numbers.⁴¹ Minnesota, for example, maintains a "master" voter list for official use and a separate "public information" list.⁴² The master list includes all voter data, including highly sensitive information, but access is limited to purposes

³⁹ Jane C. Timm, *Vote Fraud Crusader J. Christian Adams Sparks Outrage*, NBC NEWS (Aug. 27, 2017, at 05:13 CDT), <https://www.nbcnews.com/politics/donald-trump/vote-fraud-crusader-j-christian-adamssparks-outrage-n796026>. The conservative organization describes itself as "exist[ing] to assist states and others to aid the cause of election integrity and fight against lawlessness in American elections." PUB. INT. LEGAL FOUND., INC., About page, <https://publicinterestlegal.org/about/> (last visited Dec. 14, 2025).

⁴⁰ See Jerry Lambe, *Fmr Trump Voting Commission Official Forced To Apologize for Falsely Accusing People of Voter Fraud*, LAW & CRIME (July 17, 2019, at 15:28 CT), <https://lawandcrime.com/high-profile/fmr-trumpvoting-commission-official-forced-to-apologize-for-falsely-accusing-people-of-voter-fraud/>.

⁴¹ See, e.g., Alaska Stat. § 15.07.195(a); Ala. Code § 17-4-38(c); Ariz. Rev. Stat. § 16-168(C); Cal. Elec. Code § 2194(b); Colo. Rev. Stat. § 1-2-302(8); Conn. Gen. Stat. § 9-50d; Fla. Stat. § 97.0585(1); Ga. Code § 212-225(b); Haw. Rev. Stat. § 11-97; 10 Ill. Comp. Stat. 5/1A-25(c); Ind. Code § 3-7-26.4-8(c); Iowa Code § 48A.38(1)(f); Kan. Stat. § 25-2305; Ky. Rev. Stat. § 116.095; La. Stat. § 18:154(C), (F); Me. Rev. Stat. tit. 21A, § 196-A(1)(K)(2); Mass. Gen. Laws ch. 51, § 47C; Mich. Comp. Laws § 168.509gg; Minn. Stat. § 201.091, subdiv. 9; Miss. Code § 23-15-165(6); Mo. Stat. § 115.157(3); Neb. Rev. Stat. § 32-330(3)(b); Neb. Rev. Stat. § 32-301(3); Nev. Rev. Stat. § 293.558(2), (4); N.H. Rev. Stat. § 654:45, VII; N.J. Stat. § 19:31-18; N.M. Stat. § 1-4-5.5; N.M. Stat. § 1-4-50; N.C. Gen. Stat. § 163-82.10(a1)-(a2), (c); N.D. Cent. Code § 16.1-02-15; Ohio Rev. Code § 3503.13(A)(2)(a); Okla. Stat. tit. 26, § 7-103.2(B)(2)-(3); Or. Rev. Stat. § 247.948(2); 25 Pa. Cons. Stat. § 1404(a); 4 Pa. Code § 183.14(c); S.C. Code § 7-5-170(1); S.D. Codified Laws § 12-4-9; S.D. Codified Laws § 12-4-371; Tenn. Code § 2-2-127(a); Tex. Elec. Code § 18.066(b); Va. Code § 24.2-405(C); Va. Code § 24.2-406(C); Vt. Stat. tit. 17, § 2154(b)(1); Wash. Rev. Code § 29A.08.710; W. Va. Code § 3-230(b)-(c); Wis. Stat. § 6.36(1)(b)1.a; Wyo. Stat. § 22-2-113(d).

⁴² Cf. Minn. Stat. § 201.091.

related to election administration, jury selection, and certain law enforcement inquiries.⁴³ By contrast, the publicly available list contains only names, addresses, years of birth, and voting history; state law expressly prohibits the public list from including full birthdates, any part of a Social Security number, driver's license numbers, and other unique identification numbers.⁴⁴ This approach is common among other states.

Beyond limiting what data is publicly available, many states also restrict who may obtain copies of their public-facing voter registration lists and/or restrict permissible uses of voter information.⁴⁵ California law, for instance, limits access to candidates for public office, political parties, ballot measure committees, and individuals seeking the data for a handful of specified purposes.⁴⁶ Maine law similarly limits access to its voter list to political parties, organizations engaged in "get out the vote" efforts, current officeholders, governmental entities, and law enforcement agencies.⁴⁷ Outside these categories, even this more limited voter information remains confidential.

States employ additional safeguards as well. Most maintain special confidentiality programs for certain groups, such as minors who pre-register to vote before turning 18;⁴⁸ certain public officials or employees;⁴⁹ or victims of domestic violence, sexual assault, stalking, or similar crimes.⁵⁰ Many impose fees for access to their voter registration lists.⁵¹ Others restrict third-party sharing by

⁴³ Minn. Stat. § 201.091, subdiv. 1.

⁴⁴ Minn. Stat. § 201.091, subdivs. 4, 9.

⁴⁵ See, e.g., Ariz. Rev. Stat. § 16-168(E); Cal. Elec. Code § 2191(c); Cal. Elec. Code § 2194(a)(3); Fla. Stat. § 97.0585(3); Ga. Code § 21-2-601; Haw. Code R. 3-177-160(g); Idaho Code § 34-437A; 10 Ill. Comp. Stat. 5/1A-25(c); Ind. Code § 3-7-26.3-4(b); Ind. Code § 3-7-26.4-10; Iowa Code § 48A.39; Kan. Stat. § 25-2320a; Ky. Rev. Stat. § 117.025(3)(i); Me. Stat. tit. 21-A, § 196-A(4), (6); Md. Code, Elec. Law § 3-506(a)(1); Mass. Gen. Laws ch. 51, § 47C; Minn. Stat. § 201.091, subdiv. 4; Mo. Rev. Stat. § 115.157(3); Mont. Code § 13-2-122(1); Neb. Rev. Stat. § 32-330(2), (4); Nev. Rev. Stat. § 293.440(6); N.H. Rev. Stat. § 654:31, VI; N.J. Stat. § 19:31-18.1(c); N.J. Stat. § 47:1B-3(a)(1); N.M. Stat. § 1-4-5.5(C); N.Y. Elec. Law § 3-103; N.D. Cent. Code § 16.1-02-15; Or. Rev. Stat. § 247.955; 25 Pa. Cons. Stat. § 1404(b), (c)(2); 17 R.I. Gen. Laws § 17-6-5; S.D. Codified Laws § 12-4-41; Tenn. Code § 2-2-138(b), (d); Tex. Elec. Code § 18.009(a); Utah Code § 20A2-104(4); Va. Code § 24.2-407; Vt. Stat. tit. 17, § 2154(c)(1); W. Va. Code § 3-2-30(c), (f); Wyo. Stat. § 22-2-113(a).

⁴⁶ See Cal. Elec. Code § 2191(c); Cal. Elec. Code § 2194(a)(3).

⁴⁷ See Me. Stat. tit. 21-A, § 196-A(1).

⁴⁸ See, e.g., Colo. Rev. Stat. § 1-2-227(2); Fla. Stat. § 97.0585(1)(d); Wash. Rev. Code § 29A.08.725.

⁴⁹ See, e.g., Ariz. Rev. Stat. § 16-153; Cal. Elec. Code § 2166.7; 8 Colo. Code Regs. § 1505-1:2(2.10); Haw. Rev. Stat. § 11-14.5(a); Mo. Rev. Stat. § 115.157(6); Mont. Code § 13-2-115(6); Ohio Rev. Code § 3503.13(A)(2)(c); Okla. Stat. tit. 26, § 4-115.2; Or. Rev. Stat. § 247.965.

⁵⁰ See, e.g., Nat'l Ass'n of Sec'ys of State, WHITE PAPER: VOTING AND STATE ADDRESS CONFIDENTIALITY PROGRAMS, (2022), <https://www.nass.org/sites/default/files/reports/NASS-White-Paper-Voters-ACPPPrograms-Oct22.pdf> (identifying states with address confidentiality programs).

⁵¹ See, e.g., Ariz. Rev. Stat. § 16-168(E)-(F); Ark. Code § 7-5-109(c); Ga. Code § 21-2-225(b); 10 Ill. Comp. Stat. 5/1A-25(b)-(c); La. Admin Code. tit. 31, pt II, § 105; Me. Stat. tit. 21-A, § 196-A(2); Mo. Rev. Stat. §

allowing voters to opt out or by requiring election officials to obtain voter consent before releasing information.⁵² And to enforce these various protections, many states impose civil or criminal penalties—sometimes even on election officials—for impermissibly disclosing or misusing voter data.⁵³

B. State laws applicable to public records

Beyond their voter-specific laws, states also protect sensitive personal information through public records laws. Most states have “freedom of information” or “open records” laws that make government records publicly accessible,⁵⁴ but these laws typically include privacy exemptions requiring agencies to redact sensitive data before disclosure.⁵⁵ Such exemptions commonly cover Social Security numbers, driver’s license numbers, financial account information, and other identifiers that could facilitate identity theft or invasion of privacy.⁵⁶ When voter registration lists fall under these laws, these exemptions generally require election officials to remove highly sensitive data before release.

115.157(3)–(4); Mont. Code § 13-2-122; N.Y. Elec. Law § 5-602; Or. Rev. Stat. § 247.945(4); Tenn. Code § 22-138; Tex. Elec. Code § 18.066(e)–(f); Utah Code § 20A-2-104(3)(d); Vt. Stat. tit. 17, § 2141.

⁵² See, e.g., Alaska Stat. § 15.07.195(c)(4); Del. Code tit. 15, § 1303; Nev. Rev. Stat. § 293.558(3); N.C. Gen. Stat. § 163-82.10B; Utah Code § 20A-2-108(1)(b); 002-0005-17 Wyo. Admin. Code § 4; see also Ohio Rev. Code § 149.45(C) (creating an opt-out process through the state’s open records law).

⁵³ See, e.g., Ariz. Rev. Stat. § 16-168(F); Del. Code tit. 15, § 1303(d); Fla. Stat. § 104.051; Ga. Code § 21-2601; Ga. Code § 21-2-561(4); Haw. Rev. Stat. § 11-14(d); Kan. Stat. § 25-2320a; Me. Stat. tit. 21-A, § 196A(6); Md. Code, Elec. Law § 3-506(a)(1); Neb. Rev. Stat. § 32-330(4); N.H. Rev. Stat. § 654:31, VI; N.H. Rev. Stat. § 654:45; N.J. Stat. § 19:31-18.1(c); N.M. Stat. § 1-4-5.6; N.C. Gen. Stat. § 163-82.10(a1); N.D. Cent. Code § 16.1-02-16(3); 65 Pa. Stat. and Cons. Stat. § 67.708; 17 R.I. Gen. Laws § 17-6-7; S.D. Codified Laws § 12-4-41; Tenn. Code § 2-2-138(d)(2); Tex. Elec. Code § 18.009(b); Tex. Elec. Code § 18.067; Utah Code § 20A-2-104(3)(g), (j); Vt. Stat. tit. 17, § 2154(c)(1); Wash. Rev. Code § 29A.08.740; W. Va. Code § 3-2-33; Wyo. Stat. § 22-26-112(a)(viii).

⁵⁴ See, e.g., *Public Records Law and State Legislatures*, Nat’l Conf. of State Legislatures, (Apr. 16, 2025), <https://www.ncsl.org/center-for-legislative-strengthening/public-records-law-and-state-legislatures>; Reps. Comm. for Freedom of the Press, *Open Government Guide*, <https://www.rcfp.org/opengovernment-guide/> (last visited Dec. 15, 2025).

⁵⁵ See, e.g., Cal. Gov’t Code § 7924.000; Colo. Rev. Stat. § 24-72-204; Conn. Gen. Stat. § 1-210; Fla. Stat. § 119.071; Haw. Stat. § 92F-13; Kan. Stat. § 45-221; Iowa Code § 22.7; Me. Stat. tit. 1, § 402(3); Mich. Comp. Laws § 15.243; Miss. Code § 23-15-165(6); Neb. Rev. Stat. § 84-712.05; N.M. Stat. § 14-2-1.1; N.Y. Pub. Off. Law § 89; N.D. Cent. Code § 44-04-18.10; Ohio Rev. Code § 149.45; Okla. Stat. tit. 51, § 24A.5; Or. Rev. Stat. § 192.345; 38 R.I. Gen. Laws § 38-2-21; S.C. Code § 30-4-40; S.D. Codified Laws § 1-27-1.5; Tenn. Code § 2-2-112(c); Tex. Gov’t Code § 552.101; Utah Code § 63G-2-210; Vt. Stat. tit. 17, § 2154.

⁵⁶ *Cf. id.*

C. Federal privacy obligations for states

Federal and state actors may also have obligations under federal law to safeguard voter data. Election law scholar and former Justice Department official Justin Levitt has pointed to the federal Privacy Act of 1974 as one such source.⁵⁷ The Act requires federal agencies seeking to collect data from other governmental entities, including states, to notify specific Congressional committees, publish notice in the Federal Register, and allow for public comment.⁵⁸ Underscoring the importance of this requirement, the Act specifies that the penalty for “willful” noncompliance is a federal misdemeanor and can result in a fine of up to \$5,000.⁵⁹ The Act also authorizes individuals harmed by the federal government’s failure to comply with any of the Act’s provisions to bring civil lawsuits to recover monetary damages.⁶⁰ In September 2025, for example, a class-action lawsuit was filed against the Trump administration alleging, in part, Privacy Act violations for collecting Americans’ personal information to investigate voter eligibility without providing the required notice.⁶¹

Importantly, the Privacy Act prohibits the source of requested information—such as a state—from disclosing the data if the source believes the Act’s notice requirements have not been met.⁶² According to Levitt, the Justice Department likely has not complied with these obligations, meaning states may be legally barred from providing the requested information under the Privacy Act.⁶³ Indeed, in early court filings, some states have urged dismissal of the Justice Department’s lawsuits on the grounds that the Department has not complied with the Act’s notice requirements.⁶⁴

* * *

In the voting context and beyond, these privacy protections reflect efforts to balance transparency commitments with the need to safeguard sensitive personal information. As the Virginia incident described above illustrates, disclosure without adequate safeguards can put voters’ information at risk. Yet, as discussed in the next Part, the Justice Department argues that

⁵⁷ Justin Levitt, *The Recent Rash of DOJ Voter File “Requests,”* Election Law Blog (July 18, 2025, at 07:44 CT), <https://electionlawblog.org/?p=151010>.

⁵⁸ See 5 U.S.C. § 552a(e)(4) (notice in Federal Register); 5 U.S.C. § 552a(r) (notice to Congressional committees).

⁵⁹ 5 U.S.C. § 552a(i)(2).

⁶⁰ 5 U.S.C. § 552a(g)(1)(D), (g)(4).

⁶¹ See Complaint, *League of Women Voters v. U.S. Department of Homeland Security*, Case 1:25-cv-03501 (D. D.C. Sep. 30, 2025).

⁶² 5 U.S.C. § 552a(q).

⁶³ Levitt, *supra* note 57.

⁶⁴ See Motion to Dismiss filed by Shirley Weber, *United States v. Weber*, Case No. 2:25-cv-09149 (C.D. Cal. Nov. 07, 2025); Motion to Dismiss filed by State of Oregon, *United States v. Oregon*, Case No. 6:25-cv01666 (D. Or. Nov. 14, 2025).

these privacy rules should not stand as barriers to their efforts to obtain states' complete, unredacted voter registration lists.

III. Balancing Federal Enforcement Authority and State Privacy Protections

The central issue in the Justice Department's demands and lawsuits is what, if any, information federal voting laws require states to disclose to the federal government despite state laws designed to protect voters' sensitive personal information. The Justice Department has invoked different combinations of the NVRA, HAVA, and the Civil Rights Act of 1960 (discussed below) across its lawsuits. Notably, while it alleges violations of all three federal laws in most of its initial eight lawsuits (two of these initial states are exempt from the NVRA),⁶⁵ it relies solely on the Civil Rights Act of 1960 in its more recently lawsuits.⁶⁶ None of these laws directly addresses whether or when the Justice Department's authority extends to requiring disclosure of voters' highly sensitive personal information, like Social Security numbers and driver's license numbers. This Part examines each of these federal statutes and considers how they interact with state and federal privacy protections.

A. Disclosure under the NVRA

The NVRA does not explicitly require states to provide full, unredacted copies of their voter registration lists to the federal government. As discussed in Part I.A., the statute requires states to make list maintenance records available for public inspection and more generally authorizes

⁶⁵ Cf. Complaint, *United States v. Weber*, Case No. 2:25-cv-09149 (C.D. Cal. Sep. 25, 2025); Complaint, *United States v. Bellows*, Case No. 1:25-cv-00468 (D. Me. Sep. 16, 2025); Complaint, *United States v. Benson*, Case No. 1:25-cv-01148 (W.D. Mich. Sep. 25, 2025); Complaint, *United States v. Board of Elections of the State of N.Y.*, Case No. 1:25-cv-01338 (N.D. N.Y. Sep. 25, 2025); Complaint, *United States v. Pennsylvania*, Case No. 2:25-cv-01481 (W.D. Pa. Sep. 25, 2025); Complaint, *United States v. Oregon*, Case No. 6:25-cv-01666 (D. Or. Sep. 16, 2025).

⁶⁶ Cf. Complaint, *United States v. Griswold*, Case No. 1:25-cv-03967 (D. Colo. Dec. 11, 2025); Complaint, *United States v. Albence*, Case No. 1:25-cv-01453 (D. Del. Dec. 2, 2025); Complaint, *United States v. Nago*, Case No. 1:25-cv-00522 (D. Haw. Dec. 11, 2025); Complaint, *United States v. DeMarinis*, Case No. 1:25-cv-03934 (D. Md. Dec. 1, 2025); Complaint, *United States v. Galvin*, Case No. 1:25-cv-13816 (D. Mass. Dec. 11, 2025); Complaint, *United States v. Aguilar*, Case No. 3:25-cv-00728 (D. Nev. Dec. 11, 2025); Complaint, *United States v. Toulouse Oliver*, Case No. 1:25-cv-01193 (D. N.M. Dec. 2, 2025); Complaint, *United States v. Amore*, Case No. 1:25-cv-00639 (D. R.I. Dec. 2, 2025); Complaint, *United States v. Copeland Hanzas*, Case No. 2:25-cv-00903 (D. Vt. Dec. 1 2025); Complaint, *United States v. Hobbs*, Case No. 3:25-cv-06078 (W.D. Wash. Dec. 2, 2025); Complaint, *United States v. District of Columbia Board of Elections*, Case No. 1:25-cv-04403 (D. D.C. Dec. 18, 2025); Complaint, *United States v. Raffensperger*, Case No. 5:25-cv-00548 (M.D. Ga. Dec. 18, 2025); Complaint, *United States v. Matthews*, Case No. 3:25-cv-03398 (C.D. Ill. Dec. 18, 2025); Complaint, *United States v. Wisconsin Elections Commission*, Case No. 3:25-cv-1036 (W.D. Wis. Dec. 18, 2025).

the Attorney General to bring enforcement actions against noncompliant states. But no federal court has ever squarely considered whether these provisions compel disclosure to the federal government of voters' most sensitive information, such as Social Security numbers and driver's license numbers. Instead, the most pertinent existing case law suggests that states should not readily turn over this information.

In actions brought by private organizations seeking similar information to that now demanded by the Justice Department, federal courts have articulated three key principles that may guide resolution of the Department's claims. (The NVRA does not distinguish between demands for voter information made by private organizations and the federal government.) First, courts have generally held that the NVRA's disclosure provision does require states to make records related to list maintenance activities available to third parties notwithstanding state privacy laws. *But*, second, these same courts have uniformly held that states can redact highly sensitive data, such as Social Security numbers or driver's license numbers, and have specifically noted that the NVRA does not preclude such redactions. Third, at least one federal circuit has held that the NVRA requires states to offer only in-person inspection or physical copying of the records, not electronic production.

A leading example of the first two principles is the First Circuit's 2024 decision in *Public*

Interest Legal Foundation v. Bellows.⁶⁷ There, Maine had flatly refused to provide its statewide voter registration list to a private organization, citing state privacy laws.⁶⁸ The court held that the NVRA did require Maine to disclose the list, but affirmed that Maine could redact "uniquely or highly sensitive personal information," like Social Security numbers and full birthdates.⁶⁹ The court explained that "nothing in the text of the NVRA" forbids such redactions and emphasized that doing so can "further assuage" the "potential privacy risks implicated by the public release" of voter lists.⁷⁰ It also noted that several other federal courts had reached similar conclusions about states' ability to redact sensitive data.⁷¹ Thus, even if courts were to compel some disclosure to the Justice Department pursuant to the NVRA, states would presumably be allowed to redact their citizens' highly sensitive information, preserving the privacy protections provided for in state law.

The third principle—that the NVRA does not require states to provide electronic copies of records—comes from the Eleventh Circuit's 2024 decision in *Greater Birmingham Ministries v. Secretary of State for Alabama*, which concerned a private organization's request under the NVRA

⁶⁷ *Pub. Int. Legal Found., Inc. v. Bellows*, 92 F.4th 36 (1st Cir. 2024).

⁶⁸ See *id.* at 41.

⁶⁹ *Id.* at 51–56.

⁷⁰ *Id.* at 56.

⁷¹ *Id.* (collecting cases); see also *Sullivan v. Strauch*, 769 F.Supp.3d 455 (D. Md. 2025); *Voter Reference Foundation, LLC v. Torrez*, 727 F.Supp.3d 1014 (D. N.M. 2024).

for records of Alabama’s list maintenance efforts.⁷² The court held that the NVRA requires only that states make records available for “public inspection” or “photocopying at a reasonable cost.”⁷³ The court noted that while Congress has amended similarly worded statutes—such as the Freedom of Information Act—to require electronic production, it has never done so with the NVRA.⁷⁴ Given this precedent, states could presumably restrict Justice Department access to in-person review of paper or physically copied records sought pursuant to NVRA—a restriction that could limit the federal government’s ability to aggregate and analyze voter data across multiple states or to share it with other federal agencies.

Taken together, this case law suggests that states can fulfill their NVRA disclosure obligations while still protecting their citizens’ most sensitive information in accordance with state law. It is worth noting that many of the states now being sued by the Justice Department took exactly this position in response to the initial letters they received. Some offered to provide a redacted version of the voter registration list, while others provided instructions for how the Justice Department could properly seek to obtain the voter registration list in accordance with state law.⁷⁵

Given that the case law cited above involved requests from private organizations, rather than the federal government, the Justice Department may contend that it is differently situated (although the NVRA offers no clear textual basis for such an argument). But the Justice Department’s recent litigation choices may signal a retreat on this point: as noted above, while the Justice Department pursued NVRA claims in its first batch of lawsuits, it did not include them in any of the cases it filed in December.

B. Disclosure under HAVA

HAVA presents a different question than the NVRA because it lacks any public disclosure provision. Unlike the NVRA, which requires states to “make available for public inspection” records related to voting list maintenance, HAVA contains no comparable language. This omission may be dispositive. In the NVRA litigation discussed above, the statute’s explicit public disclosure provision was essential to the courts’ analyses. Courts reasoned that this disclosure requirement obligated states to provide their voter registration lists (albeit redacted) and accompanying records, despite state privacy laws.⁷⁶ Without comparable language in HAVA, the legal basis for requiring disclosure is unclear.

Further, even if a court were to conclude that HAVA implicitly requires some disclosure to enable federal enforcement, the question would remain whether states could redact highly sensitive

⁷² *Greater Birmingham Ministries v. Secretary of State for Alabama*, 105 F.4th 1324 (11th Cir. 2024).

⁷³ *Id.* at 1332-34.

⁷⁴ *Id.*

⁷⁵ See Martinez-Ochoa, O’Connor & Berry, *supra* note 5.

⁷⁶ See cases cited in note 71.

personal information, as courts have permitted under the NVRA. Given the lack of an express disclosure requirement under HAVA, courts would presumably not require states to disclose the sort of private voter information that they have been allowed to shield from NVRA disclosure requests. Ultimately, the Justice Department's claims under HAVA appear even more tenuous than its NVRA claims, which help to explain the Justice Department's decision not to pursue HAVA claims in its most recently filed lawsuits.

C. Disclosure under the Civil Rights Act of 1960

Finally, the Justice Department contends in all of its lawsuits to date that the Civil Rights Act of 1960 requires states to disclose their complete, unredacted voter registration lists. Overshadowed by later civil rights legislation, the 1960 Act expanded the enforcement powers of an earlier civil rights bill, the Civil Rights Act of 1957, which aimed to combat racially discriminatory voting practices, particularly in the South.⁷⁷ Title III of the 1960 Act requires election officials to retain "all records and papers which come into [their] possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election."⁷⁸ It also authorizes the Attorney General to inspect and copy such records upon written demand stating its "basis and purpose," and it provides a mechanism to compel disclosure in federal court.⁷⁹

Title III was designed to help the Justice Department investigate discriminatory registration practices, and it played a critical role in early voting rights litigation.⁸⁰ Today, however, the statute's application is less clear. The Justice Department contends that modern statewide voter registration lists fall within Title III's preservation and disclosure requirements. To date, however, no federal court has squarely addressed Title III's applicability to such materials.⁸¹

⁷⁷ William Sturkey, *The Hidden History of the Civil Rights Act of 1960*, Afr. Am. Intell. Hist. Soc'y: Black Persps. (Feb. 18, 2018), <https://www.aaihs.org/the-hidden-history-of-the-civil-rights-act-of-1960/>.

⁷⁸ 52 U.S.C. § 20701.

⁷⁹ 52 U.S.C. § 20703; 52 U.S.C. § 20705.

⁸⁰ See Sturkey, *supra* note 77.

⁸¹ The closest example appears to be a 2006 consent decree resolving a Title III enforcement action brought by the Justice Department against Georgia. See Consent Judgment and Decree, *United States v. Georgia*, No. 1:06-cv-2442 (N.D. Ga. Oct. 27, 2006). As part of the resolution, Georgia agreed to provide the federal government with its "full" statewide voter registration list, "including each registered voter's full name, address, birth date, and all additional voter identification information, including social security numbers or driver's license numbers as collected by the State for voter application and registration purposes." *Id.* at 3. Meanwhile, the Justice Department agreed to limit data sharing to Congress or for use before a court or grand jury (not with other federal agencies), destroy the shared information upon conclusion of the consent decree, and give Georgia the opportunity to address and correct any list maintenance compliance issues before taking further legal action. *Id.* at 3-4. While not binding precedent, the consent decree offers some insight into how the Justice Department has historically viewed the scope of its Title III authority and the type of data protections it has previously accepted.

Courts reviewing these claims will likely need to resolve some procedural questions first, including whether the Justice Department's written demands satisfied Title III's requirement to state the "basis and purpose" and whether the lawsuits were filed in the proper courts. On the latter point, Title III requires the Justice Department to bring any enforcement action in the federal judicial district where the written demand was made or where the relevant records are located.⁸² California has argued that the Justice Department's lawsuit fails to meet this requirement, contending that the demand was made, and the records are located, in Sacramento, which is in the Eastern District of California, but the Department sued in the Central District of California.⁸³

If the courts find that the Justice Department complied with Title III's procedural requirements, they will then face several substantive questions. These include whether Title III applies only to investigations of discriminatory practices or extends to other registration-related inquiries; whether states must produce digital copies or merely permit in-person inspection; and whether states may redact sensitive personal information, as courts have allowed under the NVRA. With little precedent to guide them, courts will be working from a relatively blank canvas, creating uncertainty about what they may ultimately conclude.

IV. Citizen Lawsuits to Prevent State Disclosure

While states have so far mostly resisted the Justice Department's demands for complete voter registration lists, not all have maintained that stance. Indiana and Wyoming have already provided their full, unredacted voter registration lists, and media reports indicate that officials in several other states are negotiating with the Justice Department about doing the same. This has prompted citizens in at least two states (South Carolina and Nebraska) to take legal action themselves, filing lawsuits to enforce state privacy protections and prevent their state governments from disclosing sensitive voter data. The results have been mixed, illustrating both the promise and limits of this strategy for individuals in other states concerned about the potential disclosure of their data.

The South Carolina lawsuit was filed shortly before an early September deadline the Justice Department gave the state election commission to turn over its voter registration records. A voter sought to block any data transfer, alleging that disclosure would violate state privacy laws, including one that requires the commission to keep voter data confidential and a state constitutional provision guaranteeing a right to privacy.⁸⁴ The lawsuit initially went the voter's

⁸² 52 U.S.C. § 20705.

⁸³ See Memorandum of Points & Authorities in Support of Defendants' Motion to Dismiss, *United States v. Weber*, No. 2:25-cv-09149 (C.D. Cal. Nov. 7, 2025).

⁸⁴ Complaint, *Crook v. South Carolina Election Commission*, Calhoun C.P. No. 2025-CP-09-00195 (S.C. Common Pleas Aug. 29, 2025), available at <https://clearinghouse.net/doc/163756/>.

way, with the trial court issuing a temporary restraining order and preliminary injunction, finding a “likelihood that immediate irreparable damage

will result to Plaintiff if her personal information data is released in violation of her right to privacy.”⁸⁵ However, the state supreme court quickly reversed the trial court’s order, holding that the court had not sufficiently explained its reasoning.⁸⁶

After the state supreme court’s reversal, the matter was transferred to another state court, which denied the plaintiff’s request for injunctive relief in October.⁸⁷ The court rejected the plaintiff’s legal arguments, concluding that state law authorizes the commission to enter data-sharing agreements to disclose voter registration data securely and that the state constitution’s right to privacy does not encompass sharing data between the state and federal government.⁸⁸ The court also expressed the view that Title III “likely” required the commission to turn over its voter registration records to the Justice Department.⁸⁹

Rather than appealing this decision, the plaintiff filed an amended lawsuit seeking a court order prohibiting release of her data unless the state reaches an agreement with the Justice Department that includes specific security measures, such as data-use restrictions, safeguards against third-party sharing, secure transmission protocols, and confidentiality procedures for storage and destruction.⁹⁰ The commission had previously told the court that it would not release the data without security safeguards,⁹¹ and in a November response, the commission indicated that it was still waiting for a proposed agreement from the Justice Department.⁹²

A similar lawsuit was filed in Nebraska state court in late September. There, a voter and a government watchdog organization sued the secretary of state to prevent him from turning over

⁸⁵ Temporary Restraining Order, *Crook v. South Carolina Election Commission*, Calhoun C.P. No. 2025-CP-09-00195 (S.C. Common Pleas Sep. 2, 2025), available at <https://clearinghouse.net/doc/163755/>.

⁸⁶ *Crook v. South Carolina Election Commission*, No. 2025-001777, 2025 WL 2630725 (S.C. Sep. 11, 2025).

⁸⁷ Order, *Crook v. South Carolina Election Commission*, Richland C.P. No. 2025-CP-40-06539 (S.C. Common Pleas Oct. 1, 2025), available at <https://scdailygazette.com/wp-content/uploads/2025/10/Coble-ruling-Oct.-1.pdf>.

⁸⁸ *Id.* at *5-10.

⁸⁹ *Id.* at *10-11.

⁹⁰ Amended Complaint for Injunctive Relief, *Crook v. South Carolina Election Commission*, Richland C.P. No. 2025-CP-40-06539 (S.C. Common Pleas Oct. 24, 2025), available at <https://publicindex.sccourts.org/Richland/PublicIndex/PIImageDisplay.aspx?ctagency=40002&doctype=D&docid=1761326468166->

⁹¹ See Order at *4, *Crook v. South Carolina Election Commission*, Richland C.P. No. 2025-CP-40-06539 (S.C. Common Pleas Oct. 1, 2025), available at <https://scdailygazette.com/wp-content/uploads/2025/10/Coble-ruling-Oct.-1.pdf>.

⁹² Answer to Amended Complaint for Injunctive Relief, *Crook v. South Carolina Election Commission*, Richland C.P. No. 2025-CP-40-06539 (S.C. Common Pleas Nov. 10, 2025), available at

the state’s voter registration data to the Justice Department.⁹³ The plaintiffs alleged that Nebraska law prohibits disclosure of voters’ birthdates, driver’s license information, and Social Security numbers, and bars third parties—including the federal government—from making or receiving copies of the state’s voter list.⁹⁴ They sought multiple declarations that state law prohibits such disclosure and an injunction to prevent any data transfer during the litigation.⁹⁵

The Nebraska case has proceeded differently than South Carolina’s. In response to the lawsuit, the secretary, who previously said he was “fine” handing over the state’s data,⁹⁶ agreed not to provide voter records to the Justice Department while the litigation is pending.⁹⁷ As a result, no court has yet ruled on the merits of the plaintiffs’ claims. Meanwhile, the secretary has reportedly continued negotiations with the Justice Department about how the federal government would protect the privacy of any information ultimately disclosed.⁹⁸ The case remains ongoing, and its eventual resolution may offer guidance to citizens in other states considering similar legal challenges.

These cases offer some insight into how citizen-led litigation could unfold in other states where officials are more inclined to turn over their voters’ data to the federal government.

Both lawsuits at least temporarily paused a potential disclosure and perhaps prompted state officials to give more consideration to safeguarding sensitive voter data. But the South Carolina court’s rejection of the plaintiff’s core privacy arguments suggests that favorable rulings are by no means guaranteed. Much will depend on the specifics of each state’s privacy laws and how state officials choose to respond if sued.

In states like Indiana and Wyoming that have already provided voter data to the federal government, the viability of citizen-led litigation is even more uncertain. Once that information has been turned over, there may be little a state court can do to unwind the disclosure. Still,

⁹³ Complaint, *Common Cause v. Evnen*, Lancaster Case No. D02CI250003301 (Neb. Dist. Ct. Sep. 22, 2025), available at <https://www.commoncause.org/nebraska/wp-content/uploads/2025/09/CommonCause-and-Dawn-Essink-V.-Evnen-Complaint.pdf>.

⁹⁴ *Id.*

⁹⁵ *Id.*

⁹⁶ See Juan Salinas II, *Nebraska Secretary of State Wants to Hand Over Voter Data to Feds, But Says Lawsuit Blocks It*, Nebraska Examiner (Oct. 7, 2025), <https://nebraskaexaminer.com/2025/10/07/nebraskasecretary-of-state-wants-to-hand-over-voter-data-to-feds-but-says-lawsuit-blocks-it/>.

⁹⁷ See Josie Golka, *Lawsuit Suspends Secretary of State’s Response to DOJ Request for Voter Information*, Nebraska News Service (Oct. 5, 2025), https://www.nebraskanewsservice.net/news/lawsuit-suspendssecretary-of-state-s-response-to-doj-request-for-voter-information/article_ab84aa1b-b355-4906994a-ed4a475eab47.html.

⁹⁸ Zach Wendling, *Lawsuit Over Sending Nebraska Voter Data to Feds Paused for Shutdown*, Nebraska Examiner (Oct. 20, 2025), <https://nebraskaexaminer.com/briefs/lawsuit-over-sending-nebraska-voterdata-to-feds-paused-for-shutdown/>.

citizens could potentially seek a declaration that the disclosure violated state privacy laws, an injunction blocking further data sharing, or perhaps even an order requiring state officials to request the return or deletion of data already shared. Citizens may even be able to pursue actions for monetary damages if they suffer harm from the disclosure—either through state-specific data privacy statutes, where they exist,⁹⁹ or through general tort claims, such as invasion of privacy or public disclosure of private facts, in states that have waived immunity.¹⁰⁰ In some states, moreover, privacy statutes include criminal penalties for the improper disclosure of sensitive voter data, conceivably creating an avenue for state or local officials with prosecutorial authority to investigate potential violations.¹⁰¹

Conclusion

The legal battle over the Justice Department’s demands for complete voter registration lists remains in its early stages and is unlikely to conclude before the 2026 midterm elections.¹⁰² For states invoking their privacy laws to push back against these demands, existing case law provides some support. While federal courts have held that the NVRA requires disclosure of voter registration records, they have consistently allowed states to redact highly sensitive information like Social Security numbers and driver’s license numbers. Moreover, one federal circuit has held that the NVRA requires only in-person inspection or physical copying of records. Together, these principles suggest the NVRA’s disclosure requirements can be harmonized with state privacy protections, requiring states to disclose list maintenance records while allowing them to protect voters’ most sensitive information. Whether these principles remain fully operative when the federal government requests records, or whether HAVA or the Civil Rights Act of 1960 independently require disclosure, are questions the courts must now resolve.

⁹⁹ See, e.g., Minn. Stat. § 13.08, subdiv. 1 (creating a cause of action for damages when a person is harmed by a state or local governmental entity’s violation of the state’s data privacy provisions); Wash. Rev. Code § 29A.08.740(2) (creating civil liability against any recipient of voter data whose failure to exercise due care results in the data being used for commercial purposes); see also N.C. Gen. Stat. § 163-82.10(a1) (generally precluding civil causes of action for unauthorized disclosure of voters’ personal data except when the disclosure resulted from “gross negligence, wanton conduct, or intentional wrongdoing that would otherwise be actionable.”)

¹⁰⁰ See, e.g., Matthiesen, Wickert & Lehrer, S.C., *State Sovereign Immunity and Tort Liability in All 50 States* (January 2022), <https://www.mwl-law.com/wp-content/uploads/2018/02/STATE-SOVEREIGNIMMUNITY-AND-TORT-LIABILITY-CHART.pdf#:~:text=These%20acts%20sometimes%20establish%20a%20special%20court,North%20Carolina%2C%20and%20Ohio%20use%20this%20approach.>

¹⁰¹ See *supra* note 53.

¹⁰² To date, the Justice Department has not sought expedited consideration of the cases it has brought. To the extent this litigation remains pending during the 2026 midterm elections, it is conceivable that federal officials could seek to use states’ refusal to share complete vote data to propagate unsupported claims of wrongdoing and sow mistrust about the results. Cf. Singh, *supra* note 15.

Meanwhile, in states where officials may be more willing to comply with the Justice Department's demands, individual citizens may be able to pursue litigation to prevent—or at least delay—disclosure or force negotiations over data security measures. Still, the long-term effectiveness of such lawsuits, even in states with robust privacy laws, will likely depend on how federal courts interpret the scope of federal disclosure requirements.

The answer to these questions will not only determine whether millions of Americans' sensitive personal information must be turned over to federal authorities but will also help define the balance between federal enforcement authority and state control over election administration in the United States.

