

No. 26-1232

**IN THE UNITED STATES COURT OF APPEALS
FOR THE NINTH CIRCUIT**

UNITED STATES OF AMERICA,
Plaintiff and Appellant,

v.

SHIRLEY WEBER, IN HER OFFICIAL CAPACITY AS THE SECRETARY OF STATE OF
CALIFORNIA, ET AL.,

Defendants and Appellees,

NAACP, ET AL.,

Defendants-Intervenor and Appellees.

**On Appeal from the United States District Court
for the Central District of California**

No. 2:25-cv-09149-DOC-ADS

DEFENDANTS-APPELLEES' ANSWERING BRIEF

ROB BONTA

Attorney General of California

SAMUEL T. HARBOUR

Solicitor General

R. MATTHEW WISE

SETH E. GOLDSTEIN

Supervising Deputy

Attorneys General

ANDRA LIM

IAN FEIN

Deputy Solicitors General

ROBERT WILLIAM SETRAKIAN

ANNE P. BELLOWS

LISA C. EHRLICH

MICHAEL S. COHEN

KEVIN L. QUADE

WILLIAM BELLAMY

MALCOLM A. BRUDIGAM

Deputy Attorneys General

CALIFORNIA DEPARTMENT OF JUSTICE

1300 I Street, Suite 125

Sacramento, CA 95814

(916) 210-6004

Andra.Lim@doj.ca.gov

Attorneys for Defendants and Appellees

April 17, 2026

TABLE OF CONTENTS

	Page
Introduction.....	1
Statement of jurisdiction.....	5
Statement of the issues.....	6
Addendum of statutory and regulatory provisions.....	6
Statement of the case.....	6
A. Statutory background.....	6
B. Factual background.....	13
C. Proceedings below.....	17
Summary of argument.....	21
Standard of review.....	23
Argument.....	24
I. The federal government is not entitled to the unredacted voter registration list under Title III.....	24
A. The federal government has not plausibly alleged that it is entitled to voters’ sensitive information.....	24
B. The federal government’s demand falls outside Title III’s scope.....	37
C. Title III does not preempt California privacy laws.....	44
II. The federal government’s records demand also violates federal privacy laws.....	48
A. The federal government’s demand violates the Privacy Act.....	48
B. The federal government’s demand violates the E-Government Act.....	55
C. The federal government’s demand violates DPPA.....	57
Conclusion.....	60

TABLE OF AUTHORITIES

	Page
CASES	
<i>Abagninin v. AMVAC Chemical Corp.</i> 545 F.3d 733 (9th Cir. 2008)	35
<i>Alabama ex rel. Gallion v. Rogers</i> 187 F. Supp. 848 (M.D. Ala. 1960)	10
<i>Arizona v. Inter Tribal Council of Ariz., Inc. (“ITCA”)</i> 570 U.S. 1 (2013).....	7, 10, 45
<i>Becker v. United States</i> 451 U.S. 1306 (1981).....	25
<i>Bellitto v. Snipes</i> 935 F.3d 1192 (11th Cir. 2019)	12
<i>Brooks v. Nacrelli</i> 331 F. Supp. 1350 (E.D. Pa. 1971).....	41
<i>Buckley v. Am. Const. L. Found., Inc.</i> 525 U.S. 182 (1999).....	49
<i>California v. Trump</i> 786 F. Supp. 3d 359 (D. Mass. 2025).....	7, 31
<i>Confederated Tribes and Bands of Yakama Nation v. Yakima County</i> 963 F.3d 982 (9th Cir. 2020)	32
<i>Cook v. Schriro</i> 538 F.3d 1000 (9th Cir. 2008)	21
<i>Crooks v. Harrelson</i> 282 U.S. 55 (1930).....	32
<i>Dep’t of Transp. v. Pub. Citizen</i> 541 U.S. 752 (2004).....	42

TABLE OF AUTHORITIES
(continued)

	Page
<i>Donaldson v. United States</i> 400 U.S. 517 (1971).....	25
<i>Dubin v. United States</i> 599 U.S. 110 (2023).....	42
<i>EEOC v. Karuk Tribe Housing Authority</i> 260 F.3d 1071 (9th Cir. 2001)	26, 28, 35
<i>Elec. Priv. Info. Ctr. v. Presidential Advisory Comm’n on Election Integrity</i> 878 F.3d 371 (D.C. Cir. 2017).....	55
<i>FDA v. Brown & Williamson Tobacco Corp.</i> 529 U.S. 120 (2000).....	37, 38
<i>Fish v. Kobach</i> 189 F. Supp. 3d 1107 (D. Kan. 2016).....	11
<i>Florence v. Order Express, Inc.</i> 674 F. Supp. 3d 472 (N.D. Ill. 2023).....	8
<i>FTC v. Owens-Corning Fiberglas Corp.</i> 626 F.2d 966 (D.C. Cir. 1980).....	27
<i>Garris v. Fed. Bureau of Investigation</i> 937 F.3d 1284 (9th Cir. 2019)	50, 51, 52
<i>Gonzalez v. Arizona</i> 677 F.3d 383 (9th Cir. 2012) (en banc)	9, 46
<i>Greidinger v. Davis</i> 998 F.2d 1344 (4th Cir. 1993)	36
<i>Howard v. Criminal Information Services, Inc.</i> 654 F.3d 887 (9th Cir. 2011)	58

TABLE OF AUTHORITIES
(continued)

	Page
<i>Husted v. A. Philip Randolph Institute</i> 584 U.S. 756 (2018).....	16
<i>In re Bankruptcy Estate of MarkAir, Inc.</i> 308 F.3d 1038 (9th Cir. 2002)	6
<i>Japan Gas Lighter Ass’n v. Ronson Corp.</i> 257 F. Supp. 219 (D.N.J. 1966).....	5
<i>Kennedy v. Lynd</i> 306 F.2d 222 (5th Cir. 1962)	10, 24, 26
<i>Khoja v. Orexigen Therapeutics, Inc.</i> 899 F.3d 988 (9th Cir. 2018)	24
<i>Kwan v. SanMedica Int’l</i> 854 F.3d 1088 (9th Cir. 2017)	23, 26
<i>Larsen v. PTT, LLC</i> 2025 WL 1786239 (W.D. Wash. June 27, 2025)	31
<i>Lewis v. United States</i> 523 U.S. 155 (1998).....	42
<i>Loper Bright Enters. v. Raimondo</i> 603 U.S. 369 (2024).....	33
<i>MacPherson v. I.R.S.</i> 803 F.2d 479 (9th Cir. 1986)	49, 50
<i>Martin v. Chandis Sec. Co.</i> 128 F.2d 731 (9th Cir. 1942)	26
<i>Mi Familia Vota v. Fontes</i> 129 F.4th 691 (9th Cir. 2025)	31
<i>Niz-Chavez v. Garland</i> 593 U.S. 155 (2021).....	34

TABLE OF AUTHORITIES
(continued)

	Page
<i>Orion Tire Corp. v. Goodyear Tire & Rubber Co., Inc.</i> 268 F.3d 1133 (9th Cir. 2001)	31
<i>Orr v. Plumb</i> 884 F.3d 923 (9th Cir. 2018)	51
<i>Peters v. United States</i> 853 F.2d 692 (9th Cir. 1988)	27
<i>Petroleum Exploration Int’l, S.A. v. Canrig Drilling Techs., Ltd.</i> 2010 WL 11583449 (S.D. Tex. Jan. 22, 2010).....	46
<i>Project Vote/Voting for Am., Inc. v. Long</i> 682 F.3d 331 (4th Cir. 2012)	9
<i>Project Vote/Voting for Am., Inc. v. Long</i> 752 F. Supp. 2d 697 (E.D. Va. 2010)	8
<i>Pub. Int. Legal Found., Inc. v. Bellows</i> 92 F.4th 36 (1st Cir. 2024).....	12, 38, 46
<i>Pub. Int. Legal Found., Inc. v. N.C. State Bd. of Elections</i> 996 F.3d 257 (4th Cir. 2021)	13
<i>Pub. Int. Legal Found. v. Benson</i> 136 F.4th 613 (6th Cir. 2025)	11, 34, 35
<i>Reno v. Condon</i> 528 U.S. 141 (2000).....	58
<i>Roudebush v. Hartke</i> 405 U.S. 15 (1972).....	6
<i>Rouse v. U.S. Dep’t of State</i> 567 F.3d 408 (9th Cir. 2009)	48, 52
<i>Rutan v. Republican Party of Illinois</i> 497 U.S. 62 (1990).....	49, 50

TABLE OF AUTHORITIES
(continued)

	Page
<i>Scott v. Schedler</i> 771 F.3d 831 (5th Cir. 2014)	10
<i>SEC v. Wheeling-Pittsburgh Steel Corp.</i> 648 F.2d 118 (3d Cir. 1981)	27
<i>Senne v. Village of Palatine, Ill.</i> 695 F.3d 597 (7th Cir. 2012) (en banc)	58, 59
<i>Uncork and Create LLC v. Cincinnati Ins. Co.</i> 498 F. Supp. 3d 878 (S.D. W.V. 2020)	32
<i>United States v. Amore</i> 2026 WL 2026 WL 1040637 (D.R.I. Apr. 17, 2026)	21
<i>United States v. Benson</i> 2026 WL 362789 (W.D. Mich. Feb. 10, 2026)	21
<i>United States v. California</i> 921 F.3d 865 (9th Cir. 2019)	40
<i>United States v. Galvin,</i> 2026 WL 972129 (D. Mass. Apr. 9, 2026)	21, 28, 32, 33
<i>United States v. Oregon</i> 2026 WL 318402 (D. Or. Feb. 5, 2026)	21
<i>United States v. Porter</i> 745 F.3d 1035 (10th Cir. 2014)	38
<i>United States v. Powell</i> 379 U.S. 48 (1964)	26, 27
<i>United States v. Ritchie</i> 342 F.3d 903 (9th Cir. 2003)	24
<i>United States v. Witkovich</i> 353 U.S. 194 (1957)	40

TABLE OF AUTHORITIES
(continued)

	Page
<i>Vinton v. Turstbank Sav., F.S.B.</i> 798 F. Supp. 1055 (D. Del. 1992).....	5
 CONSTITUTIONAL PROVISIONS	
United States Constitution	
Article I, § 4, cl. 1	6, 45
Amendment XV, § 1	9
 FEDERAL STATUTES	
United States Code, Title 5	
§ 552a note	48
§ 552a(a)(3).....	51
§ 552a(a)(5).....	49
§ 552a(e)(4).....	48, 52, 53, 54
§ 552a(e)(7).....	48, 49, 50, 51
 United States Code, Title 18	
§ 2721.....	13, 58
§ 2725.....	13, 58
 United States Code, Title 28	
§ 1291.....	5
 United States Code, Title 42	
§ 1971 (1964).....	41
 United States Code, Title 44	
§ 3502.....	56
 United States Code, Title 50	
§ 3371.....	44
 United States Code, Title 52	
§ 20504.....	58
§ 20505.....	7, 11

TABLE OF AUTHORITIES
(continued)

	Page
§ 20507(a)(4)	10, 35
§ 20507(i).....	<i>passim</i>
§ 20508(b)(2)	11
§ 20510.....	12, 39
§ 20701.....	9, 43
§ 20703.....	<i>passim</i>
§ 20704.....	47
§ 20705.....	5, 6, 27
§ 20901.....	44
§ 21083.....	7, 12
 Pub. L. No. 86-449, 74 Stat. 86 (1960).....	 41, 42
 Pub. L. No. 93-579, 88 Stat. 1896 (1974).....	 48
 Pub. L. No. 107-347, 116 Stat. 2899 (2002).....	 13, 55, 56, 57
 STATE STATUTES	
 California Elections Code	
§ 2150.....	7, 49
§ 2166.5.....	8
§ 2166.7.....	8
§ 2194.....	8, 44
§ 2201.....	12
§ 2265.....	58
 California Government Code	
§ 7924.000.....	8
 REGULATIONS	
 Code of Federal Regulations, Title 11	
§ 9428.4.....	7

TABLE OF AUTHORITIES
(continued)

	Page
California Code of Regulations, Title 2	
§ 19001.....	14
§ 19074.....	58
 COURT RULES	
Federal Rules of Civil Procedure	
Rule 12.....	25
Rule 26.....	39
Rule 81.....	25
Federal Rules of Evidence	
Rule 201, advisory committee’s notes.....	24
 OTHER AUTHORITIES	
106 Cong. Rec. 6392 (Mar. 23, 1960).....	33, 42
68 Fed. Reg. 47,610 (Aug. 11, 2003).....	53, 54
70 Fed. Reg. 43,904 (July 29, 2005).....	53, 54
82 Fed. Reg. 24,147 (May 25, 2017).....	53, 54
Brennan Center for Justice, Justice, <i>Tracker of Justice</i> <i>Department Requests for Voter Information</i>	17
<i>Ensuring Citizenship Verification and Integrity in Federal Elections</i> , Exec. Order No. 14399, 91 Fed. Reg. 17125 (Mar. 31, 2026).....	2, 30
Hearings Before the Subcomm. on Constitutional Rights of the S. Comm. on the Judiciary, 86th Cong. 191 (1959).....	43
H.R. Rep. No. 86-956 (1959).....	6
H.R. Rep. No. 107-329 (2001).....	7

TABLE OF AUTHORITIES
(continued)

	Page
National Conference of State Legislatures, <i>Access to and Use of Voter Registration Lists</i>	8
Off. of Mgmt. & Budget, Circular No. A-108 (2016)	54
OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22 (Sept. 26, 2003)	57
3 Records of the Federal Convention of 1787 (M. Farrand ed. 1911)	7
Secretary, <i>Report of Registration for June 2, 2026 Primary Election, 154-Day Report I</i> (Dec. 30, 2025)	17
S. Comm. on Gov't Operations and H.R. Comm. on Gov't Operations, 94th Cong., 2d Sess., <i>Source Book on Privacy</i> (1976)	52
S. Rep. No. 103-6 (1993)	11
<i>Available</i> , Merriam-Webster	45
<i>Basis</i> , Merriam-Webster	28
<i>Purpose</i> , Merriam-Webster	28
<i>Requisite</i> , Merriam-Webster	43

INTRODUCTION

The U.S. Department of Justice has sued most States in the Nation, including California, in an unprecedented effort to collect the sensitive information of tens of millions of registered voters. The federal government asserts that it seeks to evaluate California's compliance with the National Voter Registration Act of 1993 (NVRA), which requires States to conduct a reasonable program for removing registered voters who are ineligible to vote due to death or a change in residence. But U.S. DOJ has never explained why it needs 23 million California voters' sensitive information, including social security and driver's license numbers, to assess the reasonableness of the State's program. The California Secretary of State offered U.S. DOJ the opportunity to inspect the state voter roll—redacted to exclude sensitive information—in accordance with the NVRA and state privacy laws. The Secretary has also provided the federal government with comprehensive information demonstrating California's full compliance with the NVRA.

As the district court correctly recognized, U.S. DOJ's continued insistence that it needs voters' sensitive information makes sense only if its purpose is something *other* than enforcing the NVRA. Representations made by the federal government after the district court's decision leave no room for doubt on that score: U.S. DOJ's asserted purpose of evaluating NVRA compliance is pretextual. The federal government stated in its motion to expedite this appeal that it needs to

investigate whether noncitizens are on California's voter rolls. But the NVRA requirement invoked by U.S. DOJ does not cover noncitizens: it requires only that a State have a reasonable program that addresses deceased voters and voters who have moved. In its opening brief, U.S. DOJ's story has changed yet again. It now omits any mention of what it previously characterized as a pressing need to investigate noncitizen voters, and instead asserts a need to investigate NVRA compliance without providing any specifics. But eight days after it filed that brief, a U.S. DOJ lawyer told a district court in a different case that the federal government intends to run voter information through a U.S. Department of Homeland Security (DHS) citizenship database. And last month, President Trump issued an executive order calling for the creation of a national voter list for purposes of citizenship verification. *Ensuring Citizenship Verification and Integrity in Federal Elections*, Exec. Order No. 14399, 91 Fed. Reg. 17125 (Mar. 31, 2026). That too suggests that NVRA compliance is not the federal government's goal here.

These pretextual and shifting explanations provide just one of myriad legal deficiencies that led the district court to dismiss the federal government's complaint. On appeal, U.S. DOJ does not challenge the court's dismissal of its claims that it is entitled to California voters' sensitive information under the NVRA or the Help America Vote Act of 2002 (HAVA). Abandoning these claims,

it now argues only that it is entitled to that information under Title III of the Civil Rights Act of 1960. Four courts, including the district court below, have now properly held that U.S. DOJ is not entitled to voters' sensitive information under Title III.

In its opening brief, U.S. DOJ hinges its case on the theory that courts are effectively powerless to review demands for records under Title III. But courts must, at a minimum, evaluate whether the demand stated “the basis and the purpose therefor.” 52 U.S.C. § 20703. The federal government’s demand offered no “basis” whatsoever for its unprecedented attempt to obtain sensitive data about millions of voters. And as discussed, U.S. DOJ’s purported “purpose”—evaluating whether California has a reasonable program for removing two categories of voters from its voter rolls under NVRA—is completely pretextual. Making matters worse, U.S. DOJ’s most recent apparent purpose—removing noncitizens from voter rolls or creating a national voter list—strays far beyond the Executive Branch’s constitutional role. When it comes to elections, the Executive Branch’s role is to enforce the statutes Congress has enacted, and U.S. DOJ identifies no part of the NVRA authorizing it to undertake either of those actions.

Even if U.S. DOJ’s asserted purpose of NVRA compliance were somehow credited, that purpose falls outside the scope of Title III as a matter of law. The NVRA’s separate records-inspection provision—which the federal government has

abandoned any claim under—is the exclusive authority for records inspection when evaluating NVRA compliance. Further, the only permissible purpose for the Attorney General to demand records under Title III is investigating voter discrimination based on race and other protected characteristics, and U.S. DOJ has never invoked that purpose here. Even assuming Title III allowed the Attorney General to make demands for the purpose of evaluating NVRA compliance, nothing in Title III preempts California privacy laws, which require the State to redact sensitive voter information like social security and driver’s license numbers before making voter information available for inspection. Proper respect for state sovereignty—and the ordinary balance of power among the States and federal government when it comes to elections and voting—requires that Title III and California privacy laws be construed to operate harmoniously.

While the Court need not go further, federal privacy protections provide yet another independent basis for affirmance. The federal government does not meaningfully respond to the district court’s careful analysis of the federal Privacy Act of 1974. And its principal contention on appeal—that the Act governs only *disclosure* by the federal government, not *collection* of records—is plainly irreconcilable with the statute’s text. U.S. DOJ also fails to offer any persuasive response to the district court’s application of the E-Government Act of 2002 and the Driver’s Privacy Protection Act of 1994 (DPPA). The Court should affirm.

STATEMENT OF JURISDICTION

The district court entered a final order dismissing the case on January 15, 2026. 1-ER-2. U.S. DOJ timely filed a notice of appeal. 2-ER-329. This Court has jurisdiction under 28 U.S.C. § 1291. Whether the district court had jurisdiction turns on a provision of Title III providing that the “district court for the district in which a demand [for a record or paper] is made,” or “in which a record or paper so demanded is located, shall have jurisdiction by appropriate process to compel the production of such record or paper.” 52 U.S.C. § 20705. As the district court recognized, 1-ER-13, U.S. DOJ’s complaint did not allege that the federal government demanded the records in the Central District or that the records demanded are located in that district, 2-ER-309–310. On appeal, U.S. DOJ asserts that Section 20705 addresses venue, not subject-matter jurisdiction. Opening Br. 49. Other statutes with similar “shall have jurisdiction” language have sometimes been interpreted as jurisdictional provisions and sometimes as venue provisions. *See, e.g., Japan Gas Lighter Ass’n v. Ronson Corp.*, 257 F. Supp. 219, 227 (D.N.J. 1966); *Vinton v. Turstbank Sav., F.S.B.*, 798 F. Supp. 1055, 1065 (D. Del. 1992). If the Court concludes that such language relates to venue, then the district court had jurisdiction to reach the merits.¹

¹ Below, California took the position that Section 20705 is a jurisdictional provision, *see* 2-ER-283, and although the question is debatable, the State

(continued...)

STATEMENT OF THE ISSUES

I. Whether the district court’s dismissal of the Title III claim should be affirmed because the federal government is not entitled to enforcement of its demand for California voters’ sensitive information.

II. Whether the district court’s dismissal should be affirmed because the federal government’s records demand violates federal privacy laws.

ADDENDUM OF STATUTORY AND REGULATORY PROVISIONS

Relevant statutory and regulatory provisions are in an addendum to this brief.

STATEMENT OF THE CASE

A. Statutory Background

The Elections Clause of the U.S. Constitution provides that the “Times, Places and Manner of holding” federal elections “shall be prescribed in each State by the Legislature thereof,” unless Congress “make[s] or alter[s] such Regulations.” U.S. Const., art. I, § 4, cl. 1. States therefore have “authority to provide a complete code for congressional elections”—including as to voter “registration, supervision of voting, protection of voters, [and] prevention of fraud and corrupt practices,” *Roudebush v. Hartke*, 405 U.S. 15, 24 (1972)—so long as

continues to believe the provision is best viewed as jurisdictional. When a statute’s language is ambiguous, it is appropriate to consider its purpose. *See, e.g., In re Bankruptcy Estate of MarkAir, Inc.*, 308 F.3d 1038, 1043 (9th Cir. 2002). Here, Congress intended for Section 20705 to “confer[]” “*jurisdiction*” on district courts. H.R. Rep. No. 86-956, at 7 (1959) (emphasis added).

Congress does not “pre-empt” state choices, *Arizona v. Inter Tribal Council of Ariz., Inc. (ITCA)*, 570 U.S. 1, 9 (2013). The Constitution “does not grant the President any specific powers over elections”; instead, the President’s role is limited to enforcing the laws Congress passes. *California v. Trump*, 786 F. Supp. 3d 359, 373 (D. Mass. 2025), *appeal docketed*, No. 25-1726 (1st Cir. 2025).

The Constitution strikes this balance, in which States have primary responsibility over election administration, for good reason. As Madison stated, “[i]t was found necessary to leave the regulation of [federal elections], in the first place, to the state governments, as being best acquainted with the situation of the people.” 3 Records of the Federal Convention of 1787, p. 312 (M. Farrand ed. 1911). More recently, members of Congress observed that placing “the power and responsibility for running elections” in “the hands of the citizens” makes “it impossible for a single centrally controlled authority to dictate how elections will be run” and thus “to control the outcome.” H.R. Rep. No. 107-329, at 32 (2001).

Under both state and federal law, California requires individuals to provide certain personal information when they register to vote to confirm their voter eligibility. Cal. Elec. Code § 2150(a)(7); 52 U.S.C. § 20505(a)(1); 11 C.F.R. § 9428.4. That personal information includes highly sensitive information, such as social security and driver’s license numbers. Cal. Elec. Code § 2150; 52 U.S.C. § 21083(a)(5)(A)(i)-(ii).

California law provides that voter registration information is generally “confidential.” Cal. Elec. Code § 2194(a)(1). An exception to that rule permits certain voter registration information—including names, addresses, and dates of birth—to be disclosed “for governmental purposes.” *Id.* § 2194(a)(3). But California law categorically provides that certain information—including social security and driver’s license numbers—is “confidential and shall not be disclosed to any person.” *Id.* § 2194(b)(1); *see* Cal. Gov. Code § 7924.000(b) (same). California law also permits certain voters to have their address, phone number, and email address treated as confidential—for example, if the voter is a survivor of sexual assault or a public safety officer. Cal. Elec. Code §§ 2166.5, 2166.7.

Like California, most States place restrictions on the disclosure of voter registration information.² Social security numbers “are uniquely sensitive and vulnerable to abuse,” *Project Vote/Voting for Am., Inc. v. Long*, 752 F. Supp. 2d 697, 711-712 (E.D. Va. 2010), especially when they are exposed alongside other personal information such as name, date of birth, and address. The same is true of driver’s license numbers. *Florence v. Order Express, Inc.*, 674 F. Supp. 3d 472, 481 (N.D. Ill. 2023). States protect such information so that voting is not conditioned “on public release of a voter’s Social Security number” or other

² National Conference of State Legislatures, *Access to and Use of Voter Registration Lists* (updated July 17, 2025), <https://tinyurl.com/44wmazby>.

sensitive information, which would “create[] an intolerable burden” on the right to vote. *Project Vote/Voting for Am., Inc. v. Long*, 682 F.3d 331, 339 (4th Cir. 2012).

While “state governments are given the initial responsibility for regulating the mechanics of federal elections,” Congress has occasionally stepped in to “‘make or alter’ the states’ regulations.” *Gonzalez v. Arizona*, 677 F.3d 383, 390 (9th Cir. 2012) (en banc). In the 1950s and 1960s, Congress enacted legislation to enforce the Fifteenth Amendment, which provides that the “right of citizens of the United States to vote shall not be denied or abridged” “on account of race, color, or previous condition of servitude.” U.S. Const., amend. XV, § 1. One such statute was Title III of the Civil Rights Act of 1960

Under Title III, an “officer of election” must “retain and preserve” for 22 months after a federal election “all records and papers which come into his possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election.” 52 U.S.C. § 20701. “Any record or paper” that must be “retained and preserved shall, upon demand in writing by the Attorney General . . . be made available for inspection, reproduction, and copying at the principal office of [the] custodian.” *Id.* § 20703. The “demand shall contain a statement of the basis and the purpose therefor.” *Id.* Shortly after Title III’s enactment, the Attorney General interpreted this requirement to mean that the demand must state a purpose (*e.g.*, investigating a violation of federal law) and a

basis (e.g., that there is a specific factual basis for believing the law has been violated). See *Kennedy v. Lynd*, 306 F.2d 222, 229 n.6 (5th Cir. 1962).

Title III's "legislative history leaves no doubt but that it is designed to secure a more effective protection of the right to vote." *Alabama ex rel. Gallion v. Rogers*, 187 F. Supp. 848, 853 (M.D. Ala. 1960). Specifically, Title III was intended to provide "an effective means whereby preliminary investigations" could be made by the Attorney General "in order to determine whether" there had been a denial of such "constitutional principles." *Id.*

Decades after Title III's enactment, Congress imposed certain "federal regulation atop state voter-registration systems." *ITCA*, 570 U.S. at 5. The NVRA requires "each State" to "conduct a general program that makes a reasonable effort to remove the names of ineligible voters from the official lists of eligible voters by reason of" (1) "the death of the registrant" or (2) "a change in the residence of the registrant." 52 U.S.C. § 20507(a)(4)(A)-(B). Such programs are called "list maintenance" programs. The NVRA places "compliance responsibility" for its requirements in "the state" and "the [state's] chief elections officer." *Scott v. Schedler*, 771 F.3d 831, 839 (5th Cir. 2014).

To comply with the NVRA, a State must establish a general list maintenance program "that makes a rational and sensible attempt to remove" the two designated categories of ineligible voters, but a State need not "go to 'extravagant or

excessive' lengths." *Pub. Int. Legal Found. v. Benson*, 136 F.4th 613, 625 (6th Cir. 2025). California has a "comprehensive list maintenance program" that fully complies with the NVRA. SER-98. California's list maintenance program—which is laid out in state law and guidance issued by the Secretary—is administered by counties. SER-98. For example, counties must follow procedures to confirm voters' residence prior to elections through confirmation postcards or alternative procedures, such as using U.S. Postal Service change-of-address data. SER-98. The Secretary also alerts a county when a voter may have died based on weekly data from the California Department of Public Health, after which the county must review the matter and determine whether to cancel the voter's registration record. SER-101.

Congress chose not to require in the NVRA that States have a list maintenance program for removing voters who are ineligible to vote because they are noncitizens. *See Fish v. Kobach*, 189 F. Supp. 3d 1107, 1114 n.11 (D. Kan. 2016). The NVRA provides that voter registration forms accepted by the States require applicants to attest that they are citizens under penalty of perjury. 52 U.S.C. §§ 20505(a)(1)-(2), 20508(b)(2). Members of Congress determined that this requirement, combined with criminal penalties for falsely attesting to citizenship, would constitute "sufficient safeguards to prevent noncitizens from registering to vote." S. Rep. No. 103-6, at 11 (1993). If a noncitizen does register

to vote, States may remove them from voter rolls in accordance with state law. *See* Cal. Elec. Code § 2201(a)(8) (requiring cancellation of registration “[u]pon proof that the person is otherwise ineligible to vote”); SER-103.

The NVRA contains a provision governing records inspection. In relevant part, that provision requires States to “maintain for at least 2 years” and “make available for public inspection and, where available, photocopying at a reasonable cost, all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters.” 52 U.S.C. § 20507(i)(1). The provision allows parties to obtain information to “evaluate and enforce compliance with the NVRA.” *Pub. Int. Legal Found., Inc. v. Bellows*, 92 F.4th 36, 54 (1st Cir. 2024). The NVRA provides that “[t]he Attorney General may bring a civil action” to enforce its requirements, and also provides a private right of action. 52 U.S.C. § 20510(a)-(b).

HAVA requires “each State” to have a “computerized statewide voter registration list defined, maintained, and administered at the State level.” 52 U.S.C. § 21083(a)(1)(A). HAVA also reiterates, but does not “broaden[],” the “scope of the NVRA’s list-maintenance obligations.” *Bellitto v. Snipes*, 935 F.3d 1192, 1202 (11th Cir. 2019); *see* 52 U.S.C. § 21083(a)(4)(A) (reaffirming that the “State election system” must include a “system of file maintenance that makes a reasonable effort to remove registrants who are ineligible to vote”).

Federal law regarding voter information does not exist in a vacuum but alongside “statutes enacted by Congress to protect the privacy of individuals and confidential information held by certain governmental agencies.” *Pub. Int. Legal Found., Inc. v. N.C. State Bd. of Elections*, 996 F.3d 257, 264 (4th Cir. 2021). The Privacy Act and the E-Government Act contain requirements for the federal government’s collection and maintenance of certain personal information. *See* 5 U.S.C. § 552a(e) (Privacy Act); Pub. L. No. 107-347, § 208(a)-(b), 116 Stat. 2899, 2921-2922 (E-Government Act). Additionally, DPPA generally prohibits States from disclosing certain information obtained by a state department of motor vehicles (DMV), which can include information collected by a DMV that is used for voter registration purposes. 18 U.S.C. §§ 2721(a), 2725(a)(3).

B. Factual Background

On July 10, 2025, U.S. DOJ sent a letter to the Secretary requesting information “regarding the state’s procedures for complying with the statewide voter registration list maintenance provisions of [the NVRA].” 2-ER-267. Citing the NVRA’s records-inspection provision, 52 U.S.C. § 20507(i), U.S. DOJ demanded that the Secretary produce the current copy of the full, unredacted computerized statewide voter registration list. 2-ER-267. U.S. DOJ also asked the Secretary to provide “a list of the election officials who are responsible for implementing California’s general program of voter registration list maintenance,”

and “the steps you have taken . . . to ensure that the state’s list maintenance program has been properly carried out in full compliance with the NVRA.” 2-ER-267. Additionally, U.S. DOJ posed questions about California’s submissions to the U.S. Election Assistance Commission’s 2024 Election Administration and Voting Survey (EAVS), and asked the Secretary to provide data related to the EAVS submissions. 2-ER-268. U.S. DOJ requested that the Secretary respond within 14 days. 2-ER-268. The federal government’s letter did not state that it believed California’s list maintenance program violated the NVRA.

The Secretary responded on July 22, explaining that she needed more than the 14 days requested by U.S. DOJ to provide detailed responses. SER-66. A week later, the federal government sent a second letter demanding immediate responses to some questions, a copy of the statewide voter registration list by August 8, and the remainder of the information by August 29. SER-68–69.

On August 8, the Secretary offered to make available for the U.S. DOJ’s inspection a copy of California’s voter registration database at her Sacramento office. SER-72. The Secretary offered to allow inspection of all information disclosable under California law, which includes “name, residential address, mailing address, phone number, email address,” “date of birth, gender, party preference, registration status, registration date, precinct, registration method, place of birth,” “voting participation history,” and other information. Cal. Code Regs.

tit. 2, § 19001(h). The Secretary explained that, in accordance with the NVRA and California voter privacy laws, information like driver's license and social security numbers would be redacted from the records. SER-72. The Secretary also responded to some of the federal government's questions and explained that others required compiling records and would take more time to answer. SER-73.

On August 13, U.S. DOJ rejected the Secretary's invitation to inspect the voter registration list. Instead, U.S. DOJ again asserted that it was entitled to an unredacted copy of the statewide voter registration list and invoked new legal grounds for its demand—Title III and HAVA, as well as the NVRA. 2-ER-263–264. Under Title III, a records demand “shall contain a statement of the basis and the purpose therefor.” 52 U.S.C. § 20703. The federal government explained that it had provided “a statement of the basis and the purpose therefore” in its original letter: “to assist in [U.S. DOJ's] determination of whether California's list maintenance program complies with the NVRA.” 2-ER-264. U.S. DOJ did not state that “the basis and the purpose” of its demand had anything to do with HAVA compliance.

On August 21, the Secretary responded to U.S. DOJ, again inviting it to inspect the California voter registration list at her office, with appropriate redactions pursuant to state and federal law. 2-ER-258. The Secretary also asked U.S. DOJ whether its efforts to build a system of records of California voters

complied with the Privacy Act. 2-ER-260. And the Secretary pointed out that DOJ's efforts to obtain similar data from all 50 states undercut its claim that such data was necessary for investigating *California's* NVRA compliance. 2-ER-259.

On August 29 and September 12, the Secretary provided comprehensive responses to every question posed in U.S. DOJ's July 10 letter. SER-76–77, 97–104. For example, the Secretary explained that California lacks data regarding duplicate voter registrants because—like nearly three-quarters of States—California “merge[s]” information from a duplicate record into the voter's record. SER-100–101. The Secretary also explained that a decrease in inactive voters “may have various causes,” including “amendments to state law made to conform to” the Supreme Court's decision in *Husted v. A. Philip Randolph Institute*, 584 U.S. 756 (2018). SER-102–103. The Secretary explained that, because prior to that decision state law provided that canceling certain inactive voters' registrations was permissive, the data “may reflect an increase in removal of inactive voters” after *Husted*. SER-102–103.

U.S. DOJ never responded to the Secretary's August 21, August 29, and September 12 letters, and never conducted an inspection of California's voter registration list.

C. Proceedings Below

On September 25, 2025, U.S. DOJ sued California and five other states. As of today, the federal government has sued most States in the country—30 States and the District of Columbia—“in an effort to receive the full voter registration files of millions of voters across the entire country.” 1-ER-8; *see* Brennan Center for Justice, *Tracker of Justice Department Requests for Voter Information* (updated Mar. 4, 2026), <https://tinyurl.com/26a3hpu6>. At least 48 States and the District of Columbia have received “demands for complete copies of statewide voter registration files.” 1-ER-8; *see* Brennan Center for Justice, *supra*. In its suit against California, U.S. DOJ alleged it was entitled to “the current electronic copy” of the entire, unredacted computerized statewide voter registration list under Title III, the NVRA, and HAVA. 2-ER-319-322. California’s voter registration list presently contains the information of more than 23 million voters.³

California and Defendants-Intervenors filed motions to dismiss the complaint. On December 1, 2025—more than two months after filing its complaint, and less than 72 hours before the motion-to-dismiss hearing, *see* SER-36—U.S. DOJ filed a “Motion to Compel Production” of the unredacted statewide voter registration list under Title III. SER-43–60. The federal government argued that Title III requires

³ *See* Secretary, *Report of Registration for June 2, 2026 Primary Election, 154-Day Report I* (Dec. 30, 2025), <https://tinyurl.com/a32axs2>.

“summary” proceedings and that it was entitled to relief in such proceedings.

SER-49, SER-57. The district court denied the motion. 2-ER-40. U.S. DOJ then re-filed another “Motion to Compel Production.” SER-18–36. The district court deferred briefing on the motion. SER-5, SER-6–17.

In January 2026, the district court granted the motions to dismiss. The court determined that Title III does not “require[] a special statutory proceeding,” and that the Federal Rules of Civil Procedure applied. 1-ER-14. The court then explained that under Title III, U.S. DOJ’s demand needed to contain a “statement of *both* the purpose and basis.” 1-ER-15. The object of Title III the court observed, is “to detect voting-related racial discrimination,” and the statute was “not passed as a tool for NVRA compliance.” 1-ER-14–16. Accordingly, the court held that U.S. DOJ’s “stated purpose” of assessing compliance with the NVRA’s list maintenance requirements was “outside” Title III’s scope. 1-ER-16.

The district court also stated that it was “not required to accept” a “pretextual” explanation of U.S. DOJ’s purpose. 1-ER-18. The court explained that the federal government’s litigation against numerous States “point[s] at a larger pattern than the DOJ’s stated purpose” of NVRA compliance—“one that involves collecting sensitive, personally identifying information . . . then utilizing that information in a completely different context than what the information was provided for.” 1-ER-8-9. The court stated that in “similar cases involving two other states, the DOJ

asked election officials to run their entire voter list through the SAVE database—a database housed in DHS and used as the central federal database for citizenship records.” 1-ER-19; *see also* 1-ER-18–19 (noting anonymous U.S. DOJ lawyer’s stated concern that voter information would be used “for broader immigration enforcement”). To the court, it “appear[ed] that the DOJ is on a nationwide quest to gather the sensitive, private information of millions of Americans for use in a centralized federal database.” 1-ER-17. The court did “not take lightly DOJ’s obfuscation of its true motives in the present matter” or its “circumvent[ion]” of the “authority granted” by Congress. 1-ER-20.

Even if there was a “valid purpose” for U.S. DOJ’s demand, the district court held, the federal government had failed to “establish[] the basis for its request.” 1-ER-17. U.S. DOJ had not explained “why it believed the NVRA was violated in its letter to the Secretary,” or “why unredacted voter files for millions of Californians” was “necessary” for its investigation. 1-ER-17.

The district court also dismissed the NVRA and HAVA claims. As to the NVRA, the court emphasized that the NVRA addresses “states’ *policies* regarding reasonable voter roll maintenance,” but U.S. DOJ “makes no persuasive argument for why [a] large amount of unredacted voter information is necessary to evaluate state *policies*.” 1-ER-22 (emphases added). As to HAVA, the court explained that U.S. DOJ “fail[ed] to allege any violations of HAVA.” 1-ER-26. The court stated

that California's EAVS submissions showed that its list maintenance program was "properly serving as a net," and that U.S. DOJ had "been unable to identify any actual issues with California's list maintenance standards." 1-ER-27–28.

Finally, the district court concluded that U.S. DOJ's request for the unredacted statewide voter registration list "violates a plethora of federal privacy laws." 1-ER-28. The Privacy Act generally forbids federal agencies from "collect[ing] or maintain[ing] records regarding Americans' First Amendment activities." 1-ER-29. Because the federal government's records demand "include[d] information regarding previous election participation and party affiliation," the court determined that the Privacy Act "bars DOJ's request." 1-ER-29. Further, the Privacy Act requires that notice be published in the Federal Register before a federal agency establishes or revises a "system of records," and none of the prior notices identified by U.S. DOJ were "sufficient." 1-ER-30. The court also held that the federal government's records demand violates the E-Government Act and DPPA. 1-ER-31–32.

Nearly six weeks after the district court's order in this case, U.S. DOJ filed a notice of appeal, followed by motions to expedite and to consolidate this appeal with a parallel case seeking Oregon's unredacted voter registration list. 2-ER-329; Dkts. 12.1, 18.1. In its motion to expedite, the U.S. DOJ asserted that it needs sensitive voter information to "confirm that California's voter rolls are composed

solely of individuals who are eligible to vote in federal elections”—and, for the first time in this litigation, referred to the “specter of noncitizen[s]” remaining on the voter rolls. Dkt. 12-1 at 14-15. This Court granted the motion to expedite in part and denied the motion to consolidate. Dkt. 37.1. On appeal, U.S. DOJ “does not challenge” the district court’s dismissal of its NVRA and HAVA claims, Opening Br. 10 n.2, and has therefore abandoned them. *See Cook v. Schriro*, 538 F.3d 1000, 1014 n.5 (9th Cir. 2008).

The four other district courts that have addressed actions brought by U.S. DOJ to obtain a State’s unredacted voter registration list have likewise dismissed those actions. *United States v. Oregon*, 2026 WL 318402 (D. Or. Feb. 5, 2026); *United States v. Benson*, 2026 WL 362789 (W.D. Mich. 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).

SUMMARY OF ARGUMENT

I. The district court’s dismissal of the Title III claim should be affirmed. The Federal Rules of Civil Procedure’s pleading standard generally applies when the federal government seeks court enforcement of a demand for records. The federal government must plausibly allege that it satisfies the standard for court enforcement of a records demand, including that it followed the procedures required by statute, and that the records sought are relevant and material to its

investigation. Here, U.S. DOJ failed to plausibly allege that its “demand” for records “contain[ed] a statement of the basis and the purpose therefor,” 52 U.S.C. § 20703—especially because its asserted purpose of assessing California’s compliance with the NVRA is pretextual. Nor did the federal government plausibly allege that more than 23 million California voters’ sensitive information is material to its purported investigation into NVRA compliance. The NVRA imposes only a modest requirement to have a program for updating voter rolls when registered voters die or move. And the Secretary comprehensively demonstrated California’s compliance with that requirement.

In any event, U.S. DOJ’s records demand for the asserted purpose of enforcing the NVRA’s list maintenance requirements falls outside the scope of Title III as a matter of law. It is the NVRA’s records-inspection provision—not Title III—that governs demands for records made with the purpose of enforcing the NVRA. Further, the most reasonable interpretation of Title III is that it permits demands for the sole purpose of investigating racial and similar types of discrimination that prevent eligible voters from exercising their voting rights. If Title III were read literally, it would allow the Attorney General to demand certain voting records for *any* purpose—even ones unrelated to elections. The Court should reject that implausible reading. Finally, Title III does not preempt California’s privacy laws prohibiting the disclosure of sensitive voter information,

because nothing in Title III’s text conflicts with such laws. California can fully comply with Title III’s records-inspection provision by disclosing redacted voter information—just as the State has repeatedly offered to do in this case.

II. Dismissal of U.S. DOJ’s complaint should be affirmed for an independent reason. Its demand for an unredacted copy of the statewide voter registration list violates three federal privacy laws. First, the Privacy Act prohibits the federal government’s collection and maintenance of records regarding how individuals exercise their First Amendment rights. That restriction applies here and bars U.S. DOJ’s demand. The federal government also failed to follow the procedures in the Privacy Act for collecting and maintaining the sensitive voter information it seeks. Second, U.S. DOJ has failed to comply with the E-Government Act’s requirement that it prepare a privacy impact assessment before collecting the sensitive information of millions of voters. Third, DPPA forbids the Secretary from disclosing to the federal government certain voter information obtained from the DMV.

STANDARD OF REVIEW

On a motion to dismiss for failure to state a claim, the complaint “must allege enough facts to state a claim to relief that is plausible on its face.” *Kwan v. SanMedica Int’l*, 854 F.3d 1088, 1096 (9th Cir. 2017). Documents may be “incorporated by reference into a complaint if the plaintiff refers extensively to the

document or the document forms the basis of the plaintiff’s claim.” *United States v. Ritchie*, 342 F.3d 903, 908 (9th Cir. 2003). Courts at the motion-to-dismiss stage may also “take judicial notice” of legislative history and other “matters of public record.” *Khoja v. Orexigen Therapeutics, Inc.*, 899 F.3d 988, 999 (9th Cir. 2018). And without taking judicial notice, courts may consider legislative facts—facts relevant to “legal reasoning and the lawmaking process.” Fed. R. Evid. 201(a) advisory committee’s notes to 1972 proposed rules.

ARGUMENT

I. THE FEDERAL GOVERNMENT IS NOT ENTITLED TO THE UNREDACTED VOTER REGISTRATION LIST UNDER TITLE III

The district court’s dismissal of the Title III claim should be affirmed. U.S. DOJ’s complaint does not plausibly allege that it is entitled to enforcement of its demand for the sensitive information of more than 23 million California voters.

A. The Federal Government Has Not Plausibly Alleged That It Is Entitled to Voters’ Sensitive Information

1. The Rule 12(b)(6) pleading standard applies, and usual standards for judicial review of records requests govern

The district court correctly ruled that the familiar pleading standard of the Federal Rules of Civil Procedure governs. 1-ER-14. U.S. DOJ relies on a Fifth Circuit case to argue that Title III provides for summary proceedings, and that the usual pleading standard does not apply. Opening Br. 14-15 (discussing *Kennedy v. Lynd*, 306 F.2d 222 (5th Cir. 1962)). But when U.S. DOJ initiated this action, it

brought claims not only under Title III but also under the NVRA and HAVA—and the federal government makes no argument that the NVRA and HAVA provide for summary proceedings. Indeed, the federal government did not ask the district court to use any sort of summary process and instead allowed regular motion-to-dismiss proceedings to move forward. 2-ER-195–224. Although U.S. DOJ later filed motions to compel production arguing that it was entitled to immediate relief under summary process, SER-18–35, 43–60, what the federal government has appealed here is the ruling on the motions to dismiss. 2-ER-239 (notice of appeal). Whether the district court properly granted those motions to dismiss is governed by the Federal Rules of Civil Procedure’s pleading requirements.

In any event, ample authority refutes U.S. DOJ’s assertion that the ordinary civil pleading standard does not govern in summary proceedings regarding governmental demands for records. The Federal Rules of Civil Procedure state that they generally apply in such proceedings, and the Supreme Court has explained the same. *See* Fed. R. Civ. P. 81(a)(5); *Becker v. United States*, 451 U.S. 1306, 1307-1308 (1981). U.S. DOJ relies on *Donaldson v. United States*, 400 U.S. 517 (1971), but all that case provides is that a district court can *choose* to “limit the application of the rules in a summons proceeding” when appropriate. *Id.* at 529-530; *see* Opening Br 17. Here, the district court did not do so—and for good reason. It would not have been appropriate to suspend application of the usual

pleading standard, because this Court has ruled that it governs in summary proceedings. *See Martin v. Chandis Sec. Co.*, 128 F.2d 731, 734 (9th Cir. 1942); *see also United States v. Powell*, 379 U.S. 48, 58 n.18 (1964) (invoking *Martin*). Thus, under binding precedent, U.S. DOJ cannot avoid the familiar pleading rule, which requires it to “allege enough facts to state a claim to relief that is plausible on its face.” *Kwan*, 854 F.3d at 1096.

The district court also correctly ruled that it was empowered to review whether U.S. DOJ met the “statutory requirements” of Title III. 1-ER-14. U.S. DOJ contends, based on the same Fifth Circuit case discussed above, that when the Attorney General seeks enforcement of a records demand under Title III, the district court’s review is highly circumscribed and only pro forma. In U.S. DOJ’s view, the court can assess only whether there was a “written demand,” and whether the records’ custodians were given “reasonable notice of the pendency of the proceeding.” Opening Br. 19 (quoting *Lynd*, 306 F.2d at 226). But shortly after the Fifth Circuit case was decided, the Supreme Court in *United States v. Powell* set forth more searching requirements for judicial enforcement of a demand for records by the federal government. 379 U.S. at 57-58. Under *Powell*, the “critical questions” are whether (1) “Congress has granted the authority to investigate”; (2) “procedural requirements have been followed”; and (3) the records sought are “relevant and material to the investigation.” *EEOC v. Karuk Tribe Hous. Auth.*,

260 F.3d 1071, 1076 (9th Cir. 2001) (citing, inter alia, *Powell*, 379 U.S. at 57-58).

U.S. DOJ was therefore required to plausibly “alleg[e] compliance with the *Powell* standards,” including that it complied with Title III’s procedural requirements.

SEC v. Wheeling-Pittsburgh Steel Corp., 648 F.2d 118, 128 (3d Cir. 1981).⁴

As this Court has explained, “case law necessarily imposes” those limits on an agency’s “otherwise broad . . . power” to demand records. *Peters v. United States*, 853 F.2d 692, 699 (9th Cir. 1988). Congress chose to give “courts” the “power” to enforce Title III demands, which “indicates that judges should not simply rubber-stamp” the Attorney General’s demands. *FTC v. Owens-Corning Fiberglas Corp.*, 626 F.2d 966, 974 (D.C. Cir. 1980) (emphasis added); see 52 U.S.C. § 20705. And because it “is the *court’s* process which is invoked to enforce” the demand, the court “may not permit its process to be abused”—which it would be if the “underlying reasons” for the demand were “improper” or if the government was acting in bad faith. *Powell*, 379 U.S. at 58 (emphasis added). U.S. DOJ’s assertion that the district court had virtually no power to review whether the Attorney General’s demand complies with Title III is untenable.

⁴ Even if U.S. DOJ plausibly alleged satisfaction of *Powell’s* requirements at the pleading stage—which it did not, see *infra* pp. 28-36—that would not automatically entitle it to the records it seeks. *Contra* Opening Br. 52. Instead, U.S. DOJ would have to *prove* “its compliance with the *Powell* standards,” and California would have an opportunity to “prove that enforcement” of the records demand “would be improper.” *SEC*, 648 F.2d at 128.

2. The federal government did not comply with Title III’s requirement to state “the basis and the purpose” of the demand

U.S. DOJ’s complaint does not plausibly allege that Title III’s “procedural requirements have been followed.” *EEOC*, 260 F.3d at 1076. Specifically, U.S. DOJ has failed to satisfy Title III’s express requirement that the Attorney General’s “demand shall contain a statement of *the basis and the purpose therefor*.” 52 U.S.C. § 20703 (emphasis added). The “purpose” is the “reason” behind the demand. *Purpose*, Merriam-Webster, <https://tinyurl.com/2v4w5s26>. The basis is the thing “on which” the demand is “established or based.” *Basis*, Merriam-Webster, <https://tinyurl.com/3ynj8myh>. In other words, the basis is the “factual basis giving rise to the demand for records.” *Galvin*, 2026 WL 972129, at *5. Further, Title III’s use of the definite article “the” makes clear that the statement must include the *actual* purpose and basis, “not just a conceivable or possible” purpose and basis. *Id.* at *3.

a. The purported purpose invoked by U.S. DOJ is pretextual

The federal government’s demand purported to state a purpose: “to assist in [U.S. DOJ’s] determination of whether California’s list maintenance program complies with the NVRA.” 2-ER-264. But as the district court properly determined, it was not obligated to accept that entirely “pretextual” purpose. 1-ER-18. Earlier in this litigation, the federal government claimed that it needed to

“identify duplicate registration records, registrants who have moved, and registrants who have died.” 2-ER-208–209. In its motion to expedite this appeal, U.S. DOJ stated for the first time an entirely new purpose: to investigate “the specter of noncitizen . . . voters” on California’s voter rolls. Dkt. 12.1 at 15. But the federal government has omitted any mention of that new purpose from its opening brief—which provides *no* specific explanation of why the government needs sensitive voter information. *See, e.g.*, Opening Br. 29 (vaguely asserting a need for “identifiers” to determine “problems” with “voter roll registrations”).

Despite U.S. DOJ’s silence in its opening brief, it has made public representations elsewhere about what it intends to do with voter information. During a recent hearing, a U.S. DOJ lawyer told a district court that “our intention” is to run voters’ information “against DHS’s SAVE database,” which is a database with citizenship records. Transcript on Motion to Compel and Motions to Dismiss at 50, *United States v. Amore*, No. 25-CV-639 (D. R.I. Mar. 26, 2026), Dkt. 47 (*Amore* Transcript); Reply to Response in Opposition to Emergency Motion to Expedite at 6, *United States v. Benson*, No. 26-1225 (6th Cir. Mar. 10, 2026), Dkt. 19 (similar U.S. DOJ representation about SAVE database); 1-ER-19 (SAVE database is “central federal database for citizenship records”). The lawyer stated that the SAVE database would be used to “cross-check” whether voter rolls contained noncitizens. *Amore* Transcript at 51.

In addition to U.S. DOJ's representations in litigation, a recent executive order calls for the creation of a national list of citizens who are eligible to vote. That "State Citizenship List" would contain "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." Exec. Order No. 14399, § 2(a), 91 Fed. Reg. at 17125. Although U.S. DOJ previously disavowed that it would use voter information it obtains from States to create "a national voting database," *Amore* Transcript at 78, the recent executive order casts significant doubt on that claim. If the federal government were to obtain unredacted voter registration lists from States, that would plainly assist it in creating the "State Citizenship List."

U.S. DOJ's own representations and actions lay bare that the actual purpose of its demand to California is *not* "to assist in [U.S. DOJ's] determination of whether California's list maintenance program complies with the NVRA." 2-ER-264. The NVRA does not require States to have list maintenance programs to remove noncitizens from their voter rolls. *Supra* pp. 10-11. Instead, the NVRA mandates only that States use voter registration forms that require applicants to attest to their citizenship status—which California does. *Supra* p. 11. Similarly, no part of the NVRA permits the federal government to create a national voter database. Thus, U.S. DOJ's apparent actual purpose for pursuing California

voters' sensitive information has nothing whatsoever to do with enforcing or implementing any requirement of the NVRA.

Not only is U.S. DOJ's "obfuscation" of its actual purpose troubling in and of itself, 1-ER-20, the federal government's actions here raise serious separation-of-powers concerns. When it comes to elections, the Executive Branch's role is limited to enforcing the statutes Congress has enacted. *See California*, 786 F. Supp. 3d at 373. But the one statute cited by the federal government here—the NVRA—does not authorize U.S. DOJ to remove noncitizens from voter rolls or create a national voter list. Making matters worse, use of the SAVE database to check voters' citizenship *violates* the NVRA. *Mi Familia Vota v. Fontes*, 129 F.4th 691, 714-715 (9th Cir. 2025). Thus, in addition to acting extra-constitutionally, it appears the federal government plans to also act in open defiance of the NVRA.

The federal government contends that it would be improper at the pleading stage to evaluate whether the purpose of its records demand was pretextual. Opening Br. 29-30. But each of the points discussed above turns on information and sources that courts can appropriately consider when evaluating dismissal of a complaint. *See Orion Tire Corp. v. Goodyear Tire & Rubber Co., Inc.*, 268 F.3d 1133, 1138 (9th Cir. 2001) (courts may consider parties' briefing); *Larsen v. PTT, LLC*, 2025 WL 1786239, at *3 (W.D. Wash. June 27, 2025) (courts can consider

“litigation conduct”); *see generally* *Uncork and Create LLC v. Cincinnati Ins. Co.*, 498 F. Supp. 3d 878, 883 (S.D.W. Va. 2020) (“[W]hile factual allegations drive the analysis of a motion to dismiss, courts” need not “set aside common sense.”).

b. U.S. DOJ has never provided the basis for its investigation

The district court also properly ruled that the federal government’s demand did not contain a statement of “the basis” for the request. 1-ER-17. U.S. DOJ contends that its stated purpose of determining compliance with the NVRA does double duty as its basis. Opening Br. 21.⁵ But Title III requires a statement of “the basis *and* the purpose.” 52 U.S.C. § 20703 (emphasis added). “[W]hen ‘and’ is used to join two concepts, it is usually interpreted to require ‘not one or the other, but *both*.’” *Confederated Tribes and Bands of Yakama Nation v. Yakima County*, 963 F.3d 982, 990 (9th Cir. 2020) (emphasis added) (quoting *Crooks v. Harrelson*, 282 U.S. 55, 58 (1930)). Allowing U.S. DOJ to obtain records without separately stating both the basis and the purpose “would render part of the statutory text superfluous.” *Galvin*, 2026 WL 972129, at *4. It would also contradict “the construction given Title III by the Justice Department and federal courts in the

⁵ In its August 13 letter, U.S. DOJ asserted: “As required by Section 303 of the [Civil Rights Act], our letter dated July 10, 2025, provided you with ‘a statement of the basis and the purpose therefore,’ . . . namely, to assist in our determination of whether California’s list maintenance program complies with the NVRA.” 2-ER-264.

early months and years following the statute’s enactment.” *Id.* (citing cases); *Loper Bright Enters. v. Raimondo*, 603 U.S. 369, 386 (2024) (contemporaneous Executive Branch interpretation entitled to “respect”).

In the alternative, U.S. DOJ contends that it did state a separate “basis”: alleged “discrepancies” in California’s EAVS submissions, which suggest a “possible violation” of NVRA. Opening Br. 21-22. But U.S. DOJ’s letters did not identify any “discrepancies” or otherwise indicate that California was not in compliance with the NVRA. Instead, U.S. DOJ simply requested information about California’s EAVS submissions. 2-ER-267–268. U.S. DOJ’s questions—which are demands for information in and of themselves—could not have served as the “basis” for its demand for California’s voter rolls. The Secretary responded to each of the federal government’s questions with comprehensive answers that demonstrated California’s full compliance with NVRA. SER-97–104. Further, because it is far from self-evident that the purported “discrepancies” in the EAVS submissions could indicate non-compliance with NVRA, the Secretary could not possibly have been on notice of the “basis” U.S. DOJ belatedly asserts. *See* 106 Cong. Rec. 6392 (Mar. 23, 1960) (Title III’s “the basis and the purpose” language intended to give “notice as to why such an inspection was being made”).⁶

⁶ None of the discrepancies alleged by U.S. DOJ provides an indication of NVRA noncompliance. The fact that a handful of *counties*’ data was missing, 2-
(continued...)

It was not until the federal government’s motion-to-dismiss opposition that it contended—without mentioning the Secretary’s thorough responses, much less explaining why they did not show compliance with NVRA—that the EAVS submissions were “inconsistent with reasonable list maintenance efforts.” 2-ER-205. But Title III is clear: it is the “demand,” not briefing by counsel, that must contain a “statement of the basis.” 52 U.S.C. § 20703; *see Niz-Chavez v. Garland*, 593 U.S. 155, 172 (2021) (“If men must turn square corners when they deal with the government, it cannot be too much to expect the government to turn square corners when it deals with them.”).

3. The complaint does not allege that sensitive voter information is material to its asserted purpose

U.S. DOJ’s complaint also fails to plausibly allege that the sensitive information of more than 23 million voters is “relevant and material” to its supposed investigation into NVRA compliance. *EEOC*, 260 F.3d at 1076. The

ER-268, does not suggest any problem with the *State*’s laws and guidance establishing its list maintenance program. Nor does the missing data on removed duplicate registrants, 2-ER-268, suggest noncompliance, given that California’s practice of merging duplicate records is used by nearly three-quarters of States, SER-100. And statistics regarding deceased and inactive voters who might remain on the voter registration list, 2-ER-268, do not suggest that the Secretary failed to engage in reasonable efforts to remove such voters—especially in light of the explanation the Secretary provided in response to U.S. DOJ’s information request. SER-101–103; *cf. Pub. Int. Legal Found. v. Benson*, 136 F.4th at 628 (even if there were “27,000 deceased voters on the state’s voter rolls,” that would represent a small percentage of voters and indicate “rational, sensible steps to maintain accurate voter rolls”).

NVRA requires California to have a general program that makes a reasonable effort to remove two categories of ineligible voters from the voter registration list. *See* 52 U.S.C. § 20507(a)(4)(A)-(B); *Pub. Int. Legal Found. v. Benson*, 136 F.4th at 625 (State’s program must be “rational and sensible” but “need not be perfect, or even optimal”). The federal government’s complaint does not come close to plausibly alleging that the sensitive information of every single registered California voter is material to ascertaining whether California has such a reasonable program. 1-ER-22. All the complaint has to say on the matter is that the “information is necessary for the Attorney General to determine” California’s compliance with NVRA. 2-ER-320; *see Abagninin v. AMVAC Chemical Corp.*, 545 F.3d 733, 740 (9th Cir. 2008) (“conclusory” allegations are “insufficient to overcome a motion to dismiss”).

U.S. DOJ contends that it needs social security and driver’s license numbers in order “to make a verified finding as to the various voter roll registrations that may have problems.” Opening Br. 29. But in accordance with California privacy laws, the Secretary offered U.S. DOJ a robust set of information about voters, including names, addresses, email addresses, language preferences, dates of birth, and places of birth. *See supra* pp. 14-15. The federal government has never explained why this information is insufficient to “know if it’s an actual person that lives in that location and is who the voter registration [roll] says it is.” 2-ER-111;

see Greidinger v. Davis, 988 F.2d 1344, 1354-1355 (4th Cir. 1993) (interest in “preventing voter fraud” could be met “without the disclosure of the SSN,” as “an address or date of birth would sufficiently distinguish among voters that shared a common name”). In the past, U.S. DOJ has had no trouble investigating potential noncompliance under NVRA without access to a State’s unredacted voter registration list. *See, e.g., United States v. Kentucky*, No. 3:17-cv-00094 (E.D. Ky. June 21, 2018), Dkt. 35. Indeed, NVRA’s own records-inspection provision—which allows parties to obtain information to investigate potential NVRA violations—does not require States to produce sensitive information like social security numbers. *See infra*, p. 38. As the district court determined, there is “no explanation for why unredacted voter files for millions of Californians” is “necessary for the [U.S.] DOJ’s investigation.” 1-ER-17.⁷

⁷ U.S. DOJ also contends that it needs social security and driver’s license numbers to assess compliance with the NVRA’s recordkeeping requirement, but never explains why this is so. Opening Br. 29. Regardless, this argument is irrelevant because the federal government’s only asserted purpose for demanding records under Title III concerned the NVRA’s *list maintenance* requirements. 2-ER-264.

B. The Federal Government’s Demand Falls Outside Title III’s Scope

U.S. DOJ’s Title III claim also fails as a matter of law because Title III does not permit the Attorney General to make a records demand for the purpose of assessing compliance with the NVRA’s list maintenance requirements.

1. The NVRA exclusively governs the inspection of records for the purpose of enforcing the NVRA

On appeal, U.S. DOJ has abandoned its NVRA claim, Opening Br. 10 n.2, and instead seeks to use Title III to obtain an unredacted copy of the statewide voter registration list—but still for the asserted purpose of investigating NVRA compliance, 2-ER-264. The NVRA’s own records-inspection provision provides the exclusive authority for seeking records for that purpose.

“At the time a statute is enacted, it may have a range of plausible meanings,” but over time, “subsequent acts can shape or focus those meanings.” *FDA v. Brown & Williamson Tobacco Corp.*, 529 U.S. 120, 143 (2000). The “implications of a statute may be altered by the implications of a later statute,” particularly where “the scope of the earlier statute is broad but the subsequent statutes more specifically address the topic at hand.” *Id.* Thus, “a specific policy embodied in a later federal statute should control [the] construction of the [earlier] statute.” *Id.*

Whatever the scope of Title III as originally enacted, it has been narrowed by the NVRA. It is the NVRA that “specifically address[es] the topic at hand,” *FDA*,

529 U.S. at 143: the inspection of records for the purpose of enforcing the NVRA’s list maintenance requirements. Under the NVRA, the federal government and other interested parties can obtain certain records regarding list maintenance programs, *see* 52 U.S.C. § 20507(i)(1), and States may redact sensitive information from the records before making them available for inspection, 1-ER-21. Those records can then be used to “evaluate and enforce” compliance with the NVRA’s list maintenance requirements. *Bellows*, 92 F.4th at 54. It is the NVRA’s “specific policy” that controls the inspection of records for the purpose of enforcing the NVRA—not Title III. *FDA*, 529 U.S. at 143; *see United States v. Porter*, 745 F.3d 1035, 1049 (10th Cir. 2014) (narrower statute reflects Congress’s “deliberat[ion]” and “intent” with respect to particular issue).

U.S. DOJ asserts that Title III nevertheless controls here because it is “implausible that Congress intended for the Attorney General to lack the ability to inspect complete records so pertinent to her enforcement authority under the NVRA.” Opening Br. 27. But there is nothing “implausible” about the choices Congress made. The NVRA permits access to plenty of information: “all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters,” *id.* § 20507(i)(1), with the exception of sensitive information like social security and driver’s license numbers, 1-ER-21. For example, the Secretary in this case

explained that, consistent with the NVRA, her office would permit U.S. DOJ to inspect a massive amount of information—including names, addresses, dates of birth, places of birth, and voting participation history. SER-72. The NVRA further provides that it can be enforced in court by the Attorney General and private parties alike. 52 U.S.C. § 20510(a)-(b). And after a plaintiff files a lawsuit plausibly alleging an NVRA violation, the plaintiff may seek discovery of additional information. *See* Fed. R. Civ. P. 26(b). U.S. DOJ should not be permitted to end-run the sensible enforcement scheme Congress enacted in the NVRA by simply turning to Title III.⁸

2. Title III permits demands only for the purpose of investigating voting discrimination

U.S. DOJ's records demand falls outside Title III's scope for another independent reason: Title III permits the Attorney General to make demands only for the purpose of investigating discrimination based on race and other protected characteristics that prevents eligible voters from exercising their voting rights.

⁸ U.S. DOJ suggests that Title III must permit it to demand records to investigate HAVA compliance because "HAVA has no explicit inspection provision." Opening Br. 27. But the federal government admits the purpose of its record demand under Title III was only NVRA compliance, not HAVA compliance. Opening Br. 21; *see* 2-ER-264. In any event, HAVA's list maintenance requirement simply reaffirms NVRA's requirement, *supra* p. 12, so records to investigate list maintenance under HAVA would presumably be available under NVRA's records-inspection provision—meaning Title III's records-inspection provision is not needed as a backstop.

U.S. DOJ's asserted purpose here—evaluating NVRA list maintenance compliance—is wholly unrelated to alleged voting-related discrimination.

Under Title III, the Attorney General may make a demand for certain “record[s]” and “paper[s]” related to voting, and the demand “shall contain a statement of the basis and the purpose therefor.” 52 U.S.C. § 20703. If Section 20703 were read literally, as U.S. DOJ suggests it should be, that provision would allow the Attorney General to obtain certain voting records for *any purpose whatsoever*—even one completely unrelated to elections. Opening Br. 24 (asserting U.S. DOJ may obtain records whenever it is “investigating possible violations of a Federal statute”). The Attorney General could, for instance, demand that a State provide voting records “for broader immigration enforcement” purposes. 1-ER-18–19. Such a demand would have nothing to do with election administration and could even pose serious constitutional concerns. *See United States v. California*, 921 F.3d 865, 891 (9th Cir. 2019) (States have authority, “pursuant to the anticommandeering rule, to refrain from assisting with federal [immigration] efforts”). Section 20703 should not be read “literally” so as “to confer upon the Attorney General” such “unbounded,” and potentially unconstitutional, authority. *United States v. Witkovich*, 353 U.S. 194, 199 (1957).

Thus, the critical question here is not *whether* to give a limiting construction to Section 20703 but *what* limiting construction to give. As U.S. DOJ

acknowledges, the original purpose of Title III was to better enable the Attorney General to investigate discrimination based on race, color, or prior enslavement that prevented eligible voters from exercising their Fifteenth Amendment voting rights. Opening Br. 4; *see supra*, p. 10. Prior to Title III, Congress had enacted the Civil Rights Act of 1957, which permitted the Attorney General to bring a “civil action or other proper proceeding” to enforce eligible citizens’ right to vote “without distinction of race, color, or previous condition of servitude,” 42 U.S.C. § 1971(a)(1), (c) (1964), and without “voter intimidation [that] is racially motivated,” *Brooks v. Nacrelli*, 331 F. Supp. 1350, 1352 (E.D. Pa. 1971); *see* 42 U.S.C. § 1971(b) (1964). But as President Eisenhower explained, the Attorney General faced a “serious obstacle” to exercising that authority. SER-164. During “preliminary investigations of complaints,” U.S. DOJ had “no authority to require the production of election records in a civil proceeding,” and “[s]tate or local authorities [had] refused to permit the inspection of their election records.” SER-164. Congress responded by enacting Title III as part of the Civil Rights Act of 1960. Pub. L. No. 86-449, 74 Stat. 86 (May 6, 1960).

In light of Title III’s clear objective, and the need to give the statute a sensible and workable construction, Section 20703 should be interpreted to allow the Attorney General to demand records only for the purpose of investigating discrimination based on race and other protected characteristics that prevents

eligible voters from exercising their voting rights. *See Lewis v. United States*, 523 U.S. 155, 160 (1998) (rejecting literal construction of statute and adopting limiting construction based on statute’s overriding purpose); *see also Dep’t of Transp. v. Pub. Citizen*, 541 U.S. 752, 768 (2004) (rejecting literal construction of statute and instead applying statute in light of “underlying policies behind [statute] and Congress’ intent”).⁹

Two other “features” of Title III also “indicate a congressional intent to confine the scope of the” statute “more narrowly” than “a literal reading might suggest.” *Lewis*, 523 U.S. at 161. The Civil Rights Act of 1960—which contains Title III—was titled “An Act [t]o *enforce constitutional rights*, and for other purposes.” Pub. L. No. 86-449, 74 Stat. 86 (emphasis added). That title reflects Title III’s objective: to enforce the constitutional rights enshrined in the Fifteenth Amendment. *See Dubin v. United States*, 599 U.S. 110, 120-121 (2023) (“title of a statute” may assist with interpretation).

It is also noteworthy that Title III requires election officers to preserve, and allows the Attorney General to demand, a limited subset of records: “records and

⁹ Title III’s history demonstrates that the requirement that the demand “contain a statement of the basis and purpose therefor” was intended to have such a limiting effect. As explained by an author of that language, the Attorney General’s power to “demand” records “should have some relationship to” Title III’s purpose of “enforc[ing] constitutional rights.” 106 Cong. Rec. 6392 (Mar. 23, 1960).

papers” relating “to any application, registration, payment of poll tax, or other act *requisite to voting in such [federal] election.*” 52 U.S.C. § 20701 (emphasis added); *see id.* § 20703. In other words, Title III covers only records “needed for [the] particular purpose” of voting.¹⁰ It makes perfect sense that Congress narrowed the records available to the Attorney General in this manner if Title III is understood to permit demands only for the purpose of investigating the denial of voting rights based on racial or similar types of discrimination. As the Attorney General explained in a hearing regarding Title III, investigating the denial of voting rights often requires “evidence that individuals of a particular race” had “either satisfactorily demonstrated their qualifications [or] had offered to do so, and were nevertheless not allowed to register or vote, while individuals of another race no better qualified had been permitted to register or vote.” *Proposals to Secure, Protect, and Strengthen Civil Rights of Persons under the Constitution and Laws of the United States*, Hearings Before the Subcomm. on Constitutional Rights of the S. Comm. on the Judiciary, 86th Cong. 191 (1959). Such evidence would be reflected in “applications, registrations, or other acts, tests, and procedures *requisite to voting.*” *Id.* (emphasis added).

¹⁰ *Requisite*, Merriam-Webster, <https://tinyurl.com/3hufvrnh>.

By contrast, if Congress intended to permit the Attorney General to demand voting records for “investigating possible violations of [any] Federal statute,” Opening Br. 24—or even for any purpose related to elections—then it is unlikely Congress would have so limited the types of records which Attorney General could demand. For example, federal law requires reporting and assessment regarding foreign interference with elections, 50 U.S.C. § 3371, yet Title III does not require States to retain and make available all records relating to any foreign attempts to interfere with federal elections. And federal law requires States to purchase certain voting technology with federal funds, 52 U.S.C. § 20901, but Title III does not require retention and disclosure of all records relevant to that law. Title III plainly does not enable the Attorney General to “investigat[e] possible violations of [any] Federal statute.” Opening Br. 24. Its records-demand provision should not be interpreted to have a meaning incongruent with its overall operation.

C. Title III Does Not Preempt California Privacy Laws

U.S. DOJ’s Title III claim should be dismissed for another reason still: Title III does not preempt California privacy laws that forbid the disclosure of sensitive voter information like driver’s license numbers and social security numbers. *See, e.g.,* Cal. Elec. Code § 2194(b)(1); *supra*, p. 8. California’s privacy laws thus remain applicable and prohibit the Secretary from providing DOJ with an unredacted copy of the statewide voter registration list.

In the elections context, the preemption analysis is generally governed by the Elections Clause, not the Supremacy Clause. *ITCA*, 570 U.S. at 13-15. The Elections Clause provides that the “Times, Places and Manner of holding” federal elections “shall be prescribed in each State by the Legislature thereof,” but that Congress can “make or alter such Regulations.” U.S. Const., art. I, § 4, cl. 1. If a state law “conflicts with” a federal law governing the time, place, or manner of federal elections, then “the state law, so far as the conflict extends, ceases to be operative.” *ITCA*, 570 U.S. at 9 (quotation marks omitted). But Congress’s authority over federal elections preempts state law only “so far as it is exercised, and no farther.” *Id.* If state and federal obligations “can be read to operate harmoniously,” state law is not preempted. *Id.*

There is no conflict between federal and state law here. Title III requires only that certain voting records “be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative.” 52 U.S.C. § 20703. Nothing in Title III’s text overrides state privacy laws requiring redaction of highly sensitive voter information from records before disclosure to the Attorney General. The text of Title III requires records to be “made available.” *Id.* The ordinary meaning of “available” is “present or ready for immediate use.” *Available*, Merriam-Webster, <https://tinyurl.com/2ffdjn9u>. Records with a small subset of sensitive information redacted in accordance with

state privacy laws are still “present or ready for immediate use.” *See, e.g., Petroleum Exploration Int’l, S.A. v. Canrig Drilling Techs., Ltd.*, 2010 WL 11583449, at *5 (S.D. Tex. Jan. 22, 2010) (ordering that “counsel shall make available” certain documents “redacted as appropriate”). Title III and California’s voter privacy protections therefore “operate harmoniously in a single procedural scheme.” *Gonzalez*, 677 F.3d at 394.

Ruling that Title III does not preempt state privacy laws would be consistent with how courts have interpreted the NVRA’s records-inspection provision. The NVRA requires States to “make available for public inspection and, where available, photocopying at a reasonable cost,” certain records. 52 U.S.C. § 20507(i)(1). As the First Circuit recently explained, “nothing in the text of the NVRA prohibits the appropriate redaction of uniquely or highly sensitive personal information in the Voter File” or “the redaction of personal information that can be particularly sensitive in certain circumstances.” *Bellows*, 92 F.4th at 56. The relevant text of Title III is not materially distinguishable.

U.S. DOJ does not dispute that the NVRA allows States to redact sensitive information. Opening Br. 27. It instead argues that the NVRA is distinguishable from Title III because the NVRA has a “*public*-inspection requirement,” which renders redactions of sensitive information appropriate, whereas Title III requires disclosure only to the Attorney General. Opening Br. 26. But this distinction is

not relevant to the preemption analysis. The pertinent text of the NVRA and Title III is the same. If the NVRA’s directive to “make available” records does not require States to produce sensitive information, neither does Title III’s mandate that records “be made available.” 52 U.S.C. § 20507(i)(1); *id.* § 20703.

U.S. DOJ is correct that Title III prohibits the Attorney General from disclosing records produced under the statute except to “Congress,” other “governmental agencies,” and by court order. 52 U.S.C. § 20704; *see* Opening Br. 46-47. But U.S. DOJ fails to articulate how Title III’s disclosure limitation cannot operate harmoniously with California’s narrow voter data protections. Congress’ decision to impose limits on *transfer* of *collected* materials does not suggest Congress intended to oust States from restricting the *initial disclosure* of sensitive information. Moreover, States’ legitimate interest in protecting sensitive voter information does not dissipate just because information must stay within the government. *See infra*, pp. 55-59; *see also Amore* Transcript at 65-66 (acknowledging that once DHS has voter information, U.S. DOJ “cannot promise what any other agency will or will not do”).

If Congress wishes to depart from the sensible federal-state balance struck by Title III and state privacy laws, it can do so. Until that time, however, the statutory text and principles of federalism allow California to take reasonable measures to protect voters’ privacy.

II. THE FEDERAL GOVERNMENT’S RECORDS DEMAND ALSO VIOLATES FEDERAL PRIVACY LAWS

If the Court agrees that U.S. DOJ’s Title III claim fails for any of the above reasons, that is a sufficient basis to affirm the district court’s dismissal. But even if the Court does not agree with those arguments, it should still affirm because U.S. DOJ’s demand for California’s unredacted statewide voter registration list violates federal privacy laws.

A. The Federal Government’s Demand Violates the Privacy Act

The Privacy Act “protect[s] the privacy of individuals’ through regulation of the ‘collection [and] maintenance’” of information by federal agencies. *Rouse v. U.S. Dep’t of State*, 567 F.3d 408, 413 (9th Cir. 2009) (quoting 5 U.S.C. § 552a note); *see* Pub. L. No. 93-579, 88 Stat. 1896 (1974). Two of the Privacy Act’s requirements are at issue here. First, the Act prohibits federal agencies from collecting or maintaining any records describing an individual’s First Amendment activities, unless narrow exceptions apply. 5 U.S.C. § 552a(e)(7). Second, it requires that agencies provide public notice in the Federal Register about the character of the records they are collecting and how they plan to use those records. *Id.* § 552a(e)(4). The district court correctly held that U.S. DOJ’s attempted collection of California’s unredacted voter registration list violates both requirements. 1-ER-29–31.

1. The Privacy Act restricts the federal government from collecting records regarding individuals' First Amendment activities

The Privacy Act imposes requirements on federal agencies that maintain a “system of records,” 5 U.S.C. § 552a(e), which is defined as “a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number,” *id.* § 552a(a)(5). It is “undisputed” that U.S. DOJ is “an agency that maintains ‘a system of records,’” *MacPherson v. I.R.S.*, 803 F.2d 479, 481 (9th Cir. 1986), and that California’s unredacted voter registration list includes a “litany of personal and sensitive information that is governed by the Privacy Act,” 1-ER-29.

The Privacy Act prohibition at issue here provides, in relevant part, that U.S. DOJ shall collect or maintain “no record describing how any individual exercises rights guaranteed by the First Amendment.” 5 U.S.C. § 552a(e)(7). This provision applies to its demand for California’s unredacted voter registration list because the requested records include information regarding an individual’s party affiliation, previous voter registration, and voting participation history. *See, e.g.*, Cal. Elec. Code § 2150(a)(8), (10). That information undisputedly involves “political expression protected by the First Amendment.” 1-ER-29; *see, e.g.*, *Buckley v. Am. Const. L. Found., Inc.*, 525 U.S. 182, 195 (1999) (choice of whether to register to vote “implicates political thought and expression”); *Rutan v. Republican Party of*

Illinois, 497 U.S. 62, 69, 75-76 (1990) (expression of political beliefs and association through party affiliation protected by First Amendment).

To be sure, the Privacy Act’s “general proscription” on collecting records describing individuals’ First Amendment activities includes “narrow” exceptions allowing the collection of such records in certain circumstances. *MacPherson*, 803 F.2d at 481-482 (emphasis omitted). But as the district court concluded, “none of the exceptions . . . apply in the present case.” 1-ER-29. The one exception U.S. DOJ invoked below was for records “pertinent to and within the scope of an authorized law enforcement activity.” 2-ER-218 (citing 5 U.S.C. § 552a(e)(7)). This Court applies a “*narrow* reading” to that exception to better serve the statute’s privacy goals and “avoid[] infringing on the overall First Amendment concerns.” *MacPherson*, 803 F.2d at 482. Because the statute is “meant to *limit* what government agencies may collect,” an agency must demonstrate “good reason to believe” that the First Amendment-related records are “relevant” to the claimed law enforcement basis. *Garris v. Fed. Bureau of Investigation*, 937 F.3d 1284, 1299, 1301 (9th Cir. 2019). Here, even assuming the federal government’s stated desire to investigate compliance with the NVRA constitutes an authorized law enforcement activity under the exception, it has provided “at best only speculative” reason to believe that California’s full unredacted list—including individuals’ party affiliation—is “pertinent to” and “within the scope” of that purpose. *Id.* at 1299,

1301; *see supra* pp. 34-36 (detailing why U.S. DOJ has offered no plausible explanation for why the requested records would be needed for this purpose). Accordingly, U.S. DOJ “has not carried its burden to establish that the [records are] exempt from Privacy Act requirements.” *Garris*, 937 F.3d at 1299.

On appeal, U.S. DOJ ignores the central Privacy Act provision at issue here, *see* 5 U.S.C. § 552a(e)(7), and makes no argument about whether the requested records describe “how any individual exercises rights guaranteed by the First Amendment,” or whether that provision’s narrow exception applies, *id.*; *see* Opening Br. 37-40. It has therefore forfeited any arguments about that provision. *See Orr v. Plumb*, 884 F.3d 923, 932 (9th Cir. 2018).

Instead, U.S. DOJ hinges its Privacy Act arguments on the assertion that the statute “only applies to a federal agency’s *disclosure* of private information,” and therefore “has no bearing on the Attorney General’s demand to California.” Opening Br. 39. That argument is plainly meritless. The Privacy Act provides that an agency shall “maintain no record describing how any individual exercises rights guaranteed by the First Amendment,” 5 U.S.C. § 552a(e)(7), and defines “maintain” to include “collect,” *id.* § 552a(a)(3). Under the plain terms of the statute, then, “an agency may not ‘collect’ a record describing any individual’s protected First Amendment activity.” *Garris*, 937 F.3d at 1295. The Act therefore “bars [U.S.] DOJ’s request for California’s unredacted voter roll.” 1-ER-29.

U.S. DOJ’s contrary argument defies not only the Privacy Act’s text but also its purpose. Indeed, its opening brief acknowledges that the statute was designed to regulate, among other things, the “‘collection . . . of information’ by federal agencies.” Opening Br. 37-38 (quoting *Rouse*, 567 F.3d at 413). Congress enacted the Privacy Act in response to concerns about the federal government *collecting* and *centralizing* data banks of individuals’ sensitive personal information, in the wake of the Watergate and Counterintelligence Program (COINTELPRO) scandals. *See Garris*, 937 F.3d at 1295-1296. As district court observed, the federal government’s demands for unredacted voter registration lists from California and other States implicate the “very issues that animated Congress to pass the Privacy Act”—namely, to “prevent the creation of ‘formal or de facto national data banks.’” 1-ER-31 (quoting S. Comm. on Gov’t Operations and H.R. Comm. on Gov’t Operations, 94th Cong., 2d Sess., *Source Book on Privacy* at 168 (1976), https://www.justice.gov/d9/privacy_source_book.pdf).

2. The Privacy Act requires the federal government to provide public notice about the nature and scope of the records it requested

U.S. DOJ’s demand also violates the Privacy Act’s separate procedural requirement that U.S. DOJ “publish in the Federal Register . . . a notice of the existence and character of the system of records” it seeks to collect. 5 U.S.C. § 552a(e)(4). This mandatory notice—referred to as a System of Records Notice

(SORN)—is an important component of the Privacy Act. The notice “shall include” several categories of information, including the “categories of individuals on whom records are maintained in the system”; the “categories of records maintained in the system”; “each routine use of the records contained in the system”; and “the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records.” *Id.* § 552a(e)(4)(B)-(E). These details promote government transparency and accountability by informing the public about what records the agency is compiling, how it intends to use them, and how it will protect any sensitive personal information that appears in those records.

U.S. DOJ does not dispute that this notice requirement applies to its demand for California’s unredacted voter registration list. Instead, it suggests that it has complied with the requirement through earlier Federal Register notices regarding its “Central Civil Rights Division Index File.” Opening Br. 39-40 (citing 68 Fed. Reg. 47,610 (Aug. 11, 2003); 70 Fed. Reg. 43,904 (July 29, 2005); 82 Fed. Reg. 24,147 (May 25, 2017)). Not so. The system of records described in the first notice cited by U.S. DOJ consists 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,” and identifies individuals covered by those records as “[s]ubjects of investigations, victims, [and] potential

witnesses.” 68 Fed. Reg. at 47,611. The second and third notices identified additional uses of those records: namely, that U.S. DOJ may disclose information after an investigation is closed, 70 Fed. Reg. at 43,904, or in response to a data breach, 82 Fed. Reg. at 24,147.

These earlier notices do not provide the public with “notice of the existence and character of the system of records” that the agency would be amassing here. 5 U.S.C. § 552a(e)(4). In this case, the federal government seeks sensitive voter information of more than 23 million Californians. The earlier notices invoked by the federal government did not give California voters notice that their “voter registration data is going to be collected on an unprecedented level,” nor do they “alleviate concerns regarding what private and sensitive information will be shared and when.” 1-ER-30. And even if the requested voter registration data could be shoehorned into the “system of records” described in those earlier notices, U.S. DOJ has not satisfied the Act’s obligation to publish another Federal Register notice before “revis[ing]” that system to include this massive new source of records that raises distinct privacy concerns. 5 U.S.C. § 552a(e)(4).¹¹ To deem the

¹¹ See also Off. of Mgmt. & Budget, Circular No. A-108, *Federal Agency Responsibilities for Review, Reporting, and Publication Under the Privacy Act* at 5 (2016), <https://perma.cc/QZZ3-EB67> (explaining that an agency must provide notice in the Federal Register when “making significant changes to an existing system of records,” including a “substantial increase in the number, type, or

(continued...)

earlier notices sufficient to cover U.S. DOJ's present request would render the Privacy Act's public notice requirement essentially meaningless.

B. The Federal Government's Demand Violates the E-Government Act

U.S. DOJ's demand also violates the E-Government Act's requirement to prepare a privacy impact assessment before collecting sensitive information about millions of California voters. The E-Government Act generally requires federal agencies to conduct a "privacy impact assessment" before "initiating a new collection of information" that "includes any information in an identifiable form permitting the physical or online contacting of a specific individual." Pub. L. No. 107-347, § 208(b)(1)(A)(ii), (B)(i), 116 Stat. 2899, 2921-2922; *see Elec. Priv. Info. Ctr. v. Presidential Advisory Comm'n on Election Integrity*, 878 F.3d 371, 375 (D.C. Cir. 2017). The privacy impact assessment must address, at minimum: "what information is to be collected"; "why the information is being collected"; "the intended use of the . . . information"; "with whom the information will be shared"; "what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared"; "how the information will be secured"; and whether the information will be maintained in a system of records under the Privacy Act. Pub. L. No. 107-347,

category of individuals about whom records are maintained," or a "change that expands the types of categories of records maintained").

§ 208(b)(2)(B)(ii). If practicable, the agency shall “make the privacy impact assessment publicly available.” *Id.* § 208(b)(1)(B)(iii).

U.S. DOJ admits that it did not conduct a privacy impact assessment before demanding California’s unredacted voter registration list. Opening Br. 40-43. Nor does U.S. DOJ dispute that its demand is a “collection of information” under the E-Government Act. Pub. L. No. 107-347, § 208(b)(1)(A)(ii); *see id.* § 201; 44 U.S.C. § 3502(3). The names, addresses, and other sensitive information contained in the list are precisely the types of personal information the statute seeks to protect. *See* Pub. L. No. 107-347 § 208(b)(1)(A)(ii). U.S. DOJ argues only that collecting information “already maintained by the State” does not “initiate” a “new” collection. Opening Br. 42-43. That argument fails. As the district court explained, “the request made by the DOJ to California is a new one, thus initiating a new collection.” 1-ER-31.

The E-Government Act’s reference to “initiating a new collection of information,” Pub. L. No. 107-347, § 208(b)(1)(A)(ii), focuses on whether the collection is “new” to the federal agency—i.e., whether a federal agency is acquiring sensitive personal information for the first time—rather than on the source from which the agency is acquiring that information. Congress enacted the E-Government Act to “make the *Federal Government* more transparent and accountable, *id.* § 2(b)(9) (emphasis added), and to “ensure sufficient protections

for the privacy of personal information,” *id.* § 208(a). The topics to be addressed in an assessment—such as why the information is being collected, with whom the information will be shared, and how the information will be secured, *id.*

§ 208(b)(2)(B)(ii)—are relevant whenever a federal agency acquires sensitive personal information for the first time, irrespective of whether that information was previously compiled by another source. As the Office of Management and Budget has explained, assessments are required when a federal agency’s collection of information “*creates new privacy risks,*” including when an agency incorporates into existing information systems “databases of information . . . obtained from . . . public sources.” OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002, M-03-22, Art. A, § II(B)(b), (6) (Sept. 26, 2003), <https://perma.cc/E6PW-YQTP>. If a privacy impact assessment is required when compiling data from public sources, U.S. DOJ certainly must do so when demanding California’s unredacted voter registration list and amassing sensitive confidential data about more than 23 million individuals—particularly when it is simultaneously attempting to compile similar lists from dozens of other States.

C. The Federal Government’s Demand Violates DPPA

Finally, U.S. DOJ’s demand for California’s unredacted computerized statewide voter registration list violates DPPA. That law generally prohibits States from disclosing “personal information” about any individual—such as a social

security number, driver’s license number, name, address, or telephone number—that is obtained by a state DMV in connection with motor vehicle records. 18 U.S.C. §§ 2721(a), 2725(a)(3); *see Reno v. Condon*, 528 U.S. 141, 143-144 (2000). This prohibition extends to authorized recipients of personal information, like the Secretary, who receives such information from the DMV in carrying out her functions related to voter registration. 18 U.S.C. § 2721(b)(1), (c). In California, the DMV provides to the Secretary personal information about individuals who apply for a driver’s license, Cal. Elec. Code § 2265(b), and the State’s voter registration system also pulls driver’s license numbers from the DMV on an ongoing basis, *see* Cal. Code Regs. tit. 2, § 19074(a); *see also* 52 U.S.C. § 20504.

DPPA therefore restricts the Secretary’s ability to disclose to U.S. DOJ the personal information about individuals that she obtained from the DMV. U.S. DOJ does not dispute this. Instead, it invokes the statutory exception that allows disclosure “[f]or use by any government agency . . . in carrying out its functions,” 18 U.S.C. § 2721(b)(1), and asserts that the function here is to assess California’s compliance with the NVRA. Opening Br. 44.

The exception “[f]or use by any government agency” is just that—an *exception* to the statute’s “broad prohibition against disclosure.” *Senne v. Village of Palatine, Ill.*, 695 F.3d 597, 606 (7th Cir. 2012) (en banc). The exception focuses on “the *use* to which the information will be put,” *Howard v. Criminal*

Info. Servs., Inc., 654 F.3d 887, 891 (9th Cir. 2011); any disclosed personal information “must be information that is *used* for the identified purpose,” *Senne*, 695 F.3d at 606. “When a particular piece of disclosed information is not *used* to effectuate that purpose in any way, the exception provides no protection for the disclosing party.” *Id.*

Here, U.S. DOJ never explained “how the use of millions of Californian’s driver’s license numbers” would help it assess the State’s compliance with federal election statutes. 1-ER-32. Instead, U.S. DOJ merely points to a single page of the motion-to-dismiss hearing transcript (2-ER-111) to argue that the “absence of identifiers” would “substantially hamper its ability to make verified findings as to the various voter roll registrations that may have problems.” Opening Br. 45. But U.S. DOJ never explained *how* driver’s license numbers would be *used* in that process. The federal government’s failure on this score not only dooms its DPPA argument but more broadly exemplifies a fundamental problem with its demand for records: U.S. DOJ seeks highly sensitive information about more than 23 million voters without plausibly explaining why that information is necessary for its purported purpose of evaluating NVRA compliance. Its sweeping demands for such sensitive information from California and nearly every other State have no precedent in history and no support in law.

CONCLUSION

The judgment of the district court should be affirmed. The Court should also reject U.S. DOJ's request that the mandate issue immediately or that the time for filing a petition for rehearing or rehearing en banc be shortened. Opening Br. 52. A mandate is issued immediately "[o]nly in exceptional circumstances," including "where a petition for rehearing, or petition for writ of certiorari would be legally frivolous; or where an emergency situation requires that the action of the Court become final and mandate issue at once." Circuit Advisory Committee Note to Rule 41-1. Neither circumstance is present here. For the same reason, there is not good cause to shorten the 14-day period for filing a petition for rehearing or rehearing en banc.

RETRIEVED FROM DEMOCRACYDOCKET.COM

Dated: April 17, 2026

Respectfully submitted,

s/ Andra Lim

ROB BONTA
Attorney General of California

SAMUEL T. HARBOUR
Solicitor General

ANDRA LIM

IAN FEIN
Deputy Solicitors General

R. MATTHEW WISE

SETH E. GOLDSTEIN
*Supervising Deputy
Attorneys General*

ROBERT WILLIAM SETRAKIAN

ANNE P. BELLOWS

LISA C. EHRLICH

MICHAEL S. COHEN

KEVIN L. QUADE

WILLIAM BELLAMY

MALCOLM A. BRUDIGAM
Deputy Attorneys General

Attorneys for Defendants and Appellees

RETRIEVED FROM DEMOCRACYDOCKET.COM

STATEMENT OF RELATED CASES

The following related case is pending: *United States v. Oregon*, No. 26-1231.

RETRIEVED FROM DEMOCRACYDOCKET.COM

CERTIFICATE OF COMPLIANCE

Form 8. Certificate of Compliance for Briefs

9th Cir. Case Number(s): 26-1232

I am the attorney or self-represented party.

This brief contains 13,990 **words**, including 0 words manually counted in any visual images, and excluding the items exempted by FRAP 32(f). The brief's type size and typeface comply with FRAP 32(a)(5) and (6).

I certify that this brief (*select only one*):

complies with the word limit of Cir. R. 32-1.

is a **cross-appeal** brief and complies with the word limit of Cir. R. 28.1-1.

is an **amicus** brief and complies with the word limit of FRAP 29(a)(5), Cir. R. 29-2(c)(2), or Cir. R. 29-2(c)(3).

is for a **death penalty** case and complies with the word limit of Cir. R. 32-4.

complies with the longer length limit permitted by Cir. R. 32-2(b) because (*select only one*):

it is a joint brief submitted by separately represented parties.

a party or parties are filing a single brief in response to multiple briefs.

a party or parties are filing a single brief in response to a longer joint brief.

complies with the length limit designated by court order dated _____.

is accompanied by a motion to file a longer brief pursuant to Cir. R. 32-2(a).

Signature s/ Andra Lim **Date** 4/17/2026

STATUTORY AND REGULATORY ADDENDUM

RETRIEVED FROM DEMOCRACYDOCKET.COM

STATUTORY AND REGULATORY ADDENDUM**TABLE OF CONTENTS**

	Page
Pub. L. No. 107-347, § 208.....	ADD-2
5 U.S.C. § 552a.....	ADD-5
18 U.S.C. § 2721.....	ADD-7
18 U.S.C. § 2725.....	ADD-9
52 U.S.C. § 20507.....	ADD-10
52 U.S.C. § 20510.....	ADD-11
52 U.S.C. § 20701.....	ADD-12
52 U.S.C. § 20703.....	ADD-13
52 U.S.C. § 20705.....	ADD-14
52 U.S.C. § 21083.....	ADD-15
11 C.F.R. § 9428.4.....	ADD-19
California Elections Code § 2150.....	ADD-23
California Elections Code § 2194.....	ADD-26
California Government Code § 7924.000.....	ADD-28
California Code of Regulations, title 2, § 19001.....	ADD-29

Pub. L. No. 107-347, § 208

(A) Purpose.—The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

(B) Privacy Impact Assessments.—

(1) Responsibilities of Agencies.—

(A) In general.—An agency shall take actions described under subparagraph (B) before—

(i) developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or

(ii) initiating a new collection of information that—

(I) will be collected, maintained, or disseminated using information technology; and

(II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government.

(B) Agency activities.—To the extent required under subparagraph (A), each agency shall—

- (i) conduct a privacy impact assessment;
- (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and
- (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

(2) Contents of a privacy impact assessment.—

(A) In general.—The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.

(B) Guidance.—The guidance shall—

- (i) ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
- (ii) require that a privacy impact assessment address—
 - (I) what information is to be collected;

- (II) why the information is being collected;
- (III) the intended use of the agency of the information;
- (IV) with whom the information will be shared;
- (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
- (VI) how the information will be secured; and
- (VII) whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the “Privacy Act”).

(3) Responsibilities of the Director.—The Director shall—

- (A) develop policies and guidelines for agencies on the conduct of privacy impact assessments;
- (B) oversee the implementation of the privacy impact assessment process throughout the Government; and
- (C) require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

5 U.S.C. § 552a

(a) Definitions.—For purposes of this section—

(3) the term “maintain” includes maintain, collect, use, or disseminate;

(4) the term “record” means any item, collection, or grouping of information about an individual that is maintained by an agency, including, but not limited to, his education, financial transactions, medical history, and criminal or employment history and that contains his name, or the identifying number, symbol, or other identifying particular assigned to the individual, such as a finger or voice print or a photograph;

(5) the term “system of records” means a group of any records under the control of any agency from which information is retrieved by the name of the individual or by some identifying number, symbol, or other identifying particular assigned to the individual;

(e) Agency Requirements.—Each agency that maintains a system of records shall—

(4) subject to the provisions of paragraph (11) of this subsection, publish in the Federal Register upon establishment or revision a notice of the existence and character of the system of records, which notice shall include—

(A) the name and location of the system;

- (B) the categories of individuals on whom records are maintained in the system;
 - (C) the categories of records maintained in the system;
 - (D) each routine use of the records contained in the system, including the categories of users and the purpose of such use;
 - (E) the policies and practices of the agency regarding storage, retrievability, access controls, retention, and disposal of the records;
 - (F) the title and business address of the agency official who is responsible for the system of records;
 - (G) the agency procedures whereby an individual can be notified at his request if the system of records contains a record pertaining to him;
 - (H) the agency procedures whereby an individual can be notified at his request how he can gain access to any record pertaining to him contained in the system of records, and how he can contest its content; and
 - (I) the categories of sources of records in the system;
- (7) maintain no record 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;

18 U.S.C. § 2721

(a) In General.—A State department of motor vehicles, and any officer, employee, or contractor thereof, shall not knowingly disclose or otherwise make available to any person or entity:

- (1) personal information, as defined in 18 U.S.C. 2725(3), about any individual obtained by the department in connection with a motor vehicle record, except as provided in subsection (b) of this section; or
- (2) highly restricted personal information, as defined in 18 U.S.C. 2725(4), about any individual obtained by the department in connection with a motor vehicle record, without the express consent of the person to whom such information applies, except uses permitted in subsections (b)(1), (b)(4), (b)(6), and (b)(9): Provided, That subsection (a)(2) shall not in any way affect the use of organ donation information on an individual's driver's license or affect the administration of organ donation initiatives in the States.

(b) Permissible Uses.— Personal information referred to in subsection (a) shall be disclosed for use in connection with matters of motor vehicle or driver safety and theft, motor vehicle emissions, motor vehicle product alterations, recalls, or advisories, performance monitoring of motor vehicles and dealers by motor vehicle manufacturers, and removal of non-owner records from the original owner records of motor vehicle manufacturers to carry out the purposes of titles I and IV of the

Anti Car Theft Act of 1992, the Automobile Information Disclosure Act (15 U.S.C. 1231 et seq.), the Clean Air Act (42 U.S.C. 7401 et seq.), and chapters 301, 305, and 321–331 of title 49, and, subject to subsection (a)(2), may be disclosed as follows:

(1) For use by any government agency, including any court or law enforcement agency, in carrying out its functions, or any private person or entity acting on behalf of a Federal, State, or local agency in carrying out its functions.

(c) Resale or Redislosure—

An authorized recipient of personal information (except a recipient under subsection (b)(11) or (12)) may resell or redisclose the information only for a use permitted under subsection (b) (but not for uses under subsection (b)(11) or (12)).

An authorized recipient under subsection (b)(11) may resell or redisclose personal information for any purpose. An authorized recipient under subsection (b)(12) may resell or redisclose personal information pursuant to subsection (b)(12). Any authorized recipient (except a recipient under subsection (b)(11)) that resells or rediscloses personal information covered by this chapter must keep for a period of 5 years records identifying each person or entity that receives information and the permitted purpose for which the information will be used and must make such records available to the motor vehicle department upon request.

18 U.S.C. § 2725

In this chapter—

- (1) “motor vehicle record” means any record that pertains to a motor vehicle operator’s permit, motor vehicle title, motor vehicle registration, or identification card issued by a department of motor vehicles;
- (2) “person” means an individual, organization or entity, but does not include a State or agency thereof;
- (3) “personal information” means information that identifies an individual, including an individual’s photograph, social security number, driver identification number, name, address (but not the 5-digit zip code), telephone number, and medical or disability information, but does not include information on vehicular accidents, driving violations, and driver’s status.
- (4) “highly restricted personal information” means an individual’s photograph or image, social security number, medical or disability information;

52 U.S.C. § 20507

(a) In general

In the administration of voter registration for elections for Federal office, each State shall--

(4) conduct a general program that makes a reasonable effort to remove the names of ineligible voters from the official lists of eligible voters by reason of--

(A) the death of the registrant; or

(B) a change in the residence of the registrant, in accordance with subsections (b), (c), and (d); . . .

(i) Public disclosure of voter registration activities

(1) Each State shall maintain for at least 2 years and shall make available for public inspection and, where available, photocopying at a reasonable cost, all records concerning the implementation of programs and activities conducted for the purpose of ensuring the accuracy and currency of official lists of eligible voters, except to the extent that such records relate to a declination to register to vote or to the identity of a voter registration agency through which any particular voter is registered.

52 U.S.C. § 20510

(a) Attorney General

The Attorney General may bring a civil action in an appropriate district court for such declaratory or injunctive relief as is necessary to carry out this chapter.

(b) Private right of action

(1) A person who is aggrieved by a violation of this chapter may provide written notice of the violation to the chief election official of the State involved.

(2) If the violation is not corrected within 90 days after receipt of a notice under paragraph (1), or within 20 days after receipt of the notice if the violation occurred within 120 days before the date of an election for Federal office, the aggrieved person may bring a civil action in an appropriate district court for declaratory or injunctive relief with respect to the violation.

(3) If the violation occurred within 30 days before the date of an election for Federal office, the aggrieved person need not provide notice to the chief election official of the State under paragraph (1) before bringing a civil action under paragraph (2).

52 U.S.C. § 20701

Every officer of election shall retain and preserve, for a period of twenty-two months from the date of any general, special, or primary election of which candidates for the office of President, Vice President, presidential elector, Member of the Senate, Member of the House of Representatives, or Resident Commissioner from the Commonwealth of Puerto Rico are voted for, all records and papers which come into his possession relating to any application, registration, payment of poll tax, or other act requisite to voting in such election, except that, when required by law, such records and papers may be delivered to another officer of election and except that, if a State or the Commonwealth of Puerto Rico designates a custodian to retain and preserve these records and papers at a specified place, then such records and papers may be deposited with such custodian, and the duty to retain and preserve any record or paper so deposited shall devolve upon such custodian. Any officer of election or custodian who willfully fails to comply with this section shall be fined not more than \$1,000 or imprisoned not more than one year, or both.

52 U.S.C. § 20703

Any record or paper required by section 20701 of this title to be retained and preserved shall, upon demand in writing by the Attorney General or his representative directed to the person having custody, possession, or control of such record or paper, be made available for inspection, reproduction, and copying at the principal office of such custodian by the Attorney General or his representative. This demand shall contain a statement of the basis and the purpose therefor.

RETRIEVED FROM DEMOCRACYDOCKET.COM

52 U.S.C. § 20705

The United States district court for the district in which a demand is made pursuant to section 20703 of this title, or in which a record or paper so demanded is located, shall have jurisdiction by appropriate process to compel the production of such record or paper.

RETRIEVED FROM DEMOCRACYDOCKET.COM

52 U.S.C. § 21083

(a) Computerized statewide voter registration list requirements

(1) Implementation

(A) In general

Except as provided in subparagraph (B), each State, acting through the chief State election official, shall implement, in a uniform and nondiscriminatory manner, a single, uniform, official, centralized, interactive computerized statewide voter registration list defined, maintained, and administered at the State level that contains the name and registration information of every legally registered voter in the State and assigns a unique identifier to each legally registered voter in the State (in this subsection referred to as the “computerized list”), and includes the following:

- (i) The computerized list shall serve as the single system for storing and managing the official list of registered voters throughout the State.
- (ii) The computerized list contains the name and registration information of every legally registered voter in the State.
- (iii) Under the computerized list, a unique identifier is assigned to each legally registered voter in the State.

(iv) The computerized list shall be coordinated with other agency databases within the State.

(v) Any election official in the State, including any local election official, may obtain immediate electronic access to the information contained in the computerized list.

(vi) All voter registration information obtained by any local election official in the State shall be electronically entered into the computerized list on an expedited basis at the time the information is provided to the local official.

(vii) The chief State election official shall provide such support as may be required so that local election officials are able to enter information as described in clause (vi).

(viii) The computerized list shall serve as the official voter registration list for the conduct of all elections for Federal office in the State. . . .

(4) Minimum standard for accuracy of State voter registration records

The State election system shall include provisions to ensure that voter registration records in the State are accurate and are updated regularly, including the following:

(A) 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. Under such system, consistent with the National Voter Registration Act of 1993 (42 U.S.C. 1973gg et seq.)¹, registrants who have not responded to a notice and who have not voted in 2 consecutive general elections for Federal office shall be removed from the official list of eligible voters, except that no registrant may be removed solely by reason of a failure to vote.

(B) Safeguards to ensure that eligible voters are not removed in error from the official list of eligible voters.

(5) Verification of voter registration information

(A) Requiring provision of certain information by applicants

(i) In general

Except as provided in clause (ii), notwithstanding any other provision of law, an application for voter registration for an election for Federal office may not be accepted or processed by a State unless the application includes--

(I) in the case of an applicant who has been issued a current and valid driver's license, the applicant's driver's license number; or

(II) in the case of any other applicant (other than an applicant to whom clause (ii) applies), the last 4 digits of the applicant's social security number.

(ii) Special rule for applicants without driver's license or social security number

If an applicant for voter registration for an election for Federal office has not been issued a current and valid driver's license or a social security number, the State shall assign the applicant a number which will serve to identify the applicant for voter registration purposes. To the extent that the State has a computerized list in effect under this subsection and the list assigns unique identifying numbers to registrants, the number assigned under this clause shall be the unique identifying number assigned under the list.

(iii) Determination of validity of numbers provided

The State shall determine whether the information provided by an individual is sufficient to meet the requirements of this subparagraph, in accordance with State law.

11 C.F.R. § 9428.4

(a) Information about the applicant.

The application shall provide appropriate fields for the applicant's:

- (1) Last, first, and middle name, any suffix, and (optional) any prefix;
- (2) Address where the applicant lives including: street number and street name, or rural route with a box number; apartment or unit number; city, town, or village name; state; and zip code; with instructions to draw a locational map if the applicant lives in a rural district or has a non-traditional residence, and directions not to use a post office box or rural route without a box number;
- (3) Mailing address if different from the address where the applicant lives, such as a post office box, rural route without a box number, or other street address; city, town, or village name; state; and zip code;
- (4) Month, day, and year of birth;
- (5) Telephone number (optional); and
- (6) Voter identification number as required or requested by the applicant's state of residence for election administration purposes.

(i) The application shall direct the applicant to consult the accompanying state-specific instructions to determine what type of voter identification number, if any, is required or requested by the applicant's state.

(ii) For each state that requires the applicant's full social security number as its voter identification number, the state's Privacy Act notice required at 11 CFR 9428.6(c) shall be reprinted with the instructions for that state.

(7) Political party preference, for an applicant in a closed primary state.

(i) The application shall direct the applicant to consult the accompanying state-specific instructions to determine if the applicant's state is a closed primary state.

(ii) The accompanying instructions shall state that if the applicant is registering in a state that requires the declaration of party affiliation, then failure to indicate a political party preference, indicating "none", or selecting a party that is not recognized under state law may prevent the applicant from voting in partisan races in primary elections and participating in political party caucuses or conventions, but will not bar an applicant from voting in other elections.

(8) Race/ethnicity, if applicable for the applicant's state of residence. The application shall direct the applicant to consult the state-specific instructions to determine whether race/ethnicity is required or requested by the applicant's state.

(b) Additional information required by the Act. (42 U.S.C. 1973gg-7(b)(2) and (4))¹.

The form shall also:

- (1) Specify each eligibility requirement (including citizenship). The application shall list U.S. Citizenship as a universal eligibility requirement and include a statement that incorporates by reference each state's specific additional eligibility requirements (including any special pledges) as set forth in the accompanying state instructions;
- (2) Contain an attestation on the application that the applicant, to the best of his or her knowledge and belief, meets each of his or her state's specific eligibility requirements;
- (3) Provide a field on the application for the signature of the applicant, under penalty of perjury, and the date of the applicant's signature;
- (4) Inform an applicant on the application of the penalties provided by law for submitting a false voter registration application;
- (5) Provide a field on the application for the name, address, and (optional) telephone number of the person who assisted the applicant in completing the form if the applicant is unable to sign the application without assistance;

(6) State that if an applicant declines to register to vote, the fact that the applicant has declined to register will remain confidential and will be used only for voter registration purposes; and

(7) State that if an applicant does register to vote, the office at which the applicant submits a voter registration application will remain confidential and will be used only for voter registration purposes.

(c) Other information. The form will, if appropriate, require an applicant's former address or former name or request a drawing of the area where the applicant lives in relation to local landmarks.

RETRIEVED FROM DEMOCRACYDOCKET.COM

California Elections Code § 2150

(a) The affidavit of registration shall show:

(1) The facts necessary to establish the affiant as an elector.

(2) The affiant's name at length, including the person's given name, and a middle name or initial, or if the initial of the given name is customarily used, then the initial and middle name. The affiant's given name may be preceded, at the affiant's option, by the designation of "Miss," "Ms.," "Mrs.," or "Mr."

A person shall not be denied the right to register because of that person's failure to mark a prefix to the given name and shall be so advised on the voter registration card. This subdivision shall not be construed as requiring the printing of prefixes on an affidavit of registration.

(3) The affiant's place of residence, residence telephone number, if furnished, and email address, if furnished. A person shall not be denied the right to register because of the person's failure to furnish a telephone number or email address, and shall be so advised on the voter registration card.

(4) The affiant's mailing address, if different from the place of residence.

(5) The affiant's date of birth to establish that the affiant will be at least 18 years of age on or before the date of the next election. In the case of an affidavit of registration submitted pursuant to subdivision (d) of Section 2102, the affiant's date of birth to establish that the affiant is at least 16 years of age.

(6) The state or country of the affiant's birth.

(7)

(A) In the case of an affiant who has been issued a current and valid driver's license, the affiant's driver's license number.

(B) In the case of any other affiant, other than an affiant to whom subparagraph (C) applies, the last four digits of the affiant's social security number.

(C) If a voter registration affiant has not been issued a current and valid driver's license or a social security number, the state shall assign the affiant a number that will serve to identify the affiant for voter registration purposes. If the state has a computerized list in effect under this paragraph and the list assigns unique identifying numbers to registrants, the number assigned under this subparagraph shall be the unique identifying number assigned under the list.

(8) The affiant's political party preference.

(9) That the affiant is currently not imprisoned for the conviction of a felony.

(10) A prior registration portion indicating whether the affiant has been registered at another address, under another name, or as preferring another party. If the affiant has been so registered, the affiant shall give an additional statement giving that address, name, or party.

(b) The affiant shall certify the content of the affidavit of registration as to its truthfulness and correctness, under penalty of perjury, with the signature of the affiant's name and the date of signing. If the affiant is unable to write, the affiant shall sign with a mark or cross. An affiant who is an individual with a disability may complete the affidavit with reasonable accommodations as needed.

(c) The affidavit of registration shall also contain a space that would enable the affiant to state the affiant's ethnicity or race, or both. An affiant shall not be denied the ability to register because the affiant declines to state the affiant's ethnicity or race.

(d) If a person assists the affiant in completing the affidavit of registration, that person shall sign and date the affidavit below the signature of the affiant.

(e) The Secretary of State may continue to supply existing affidavits of registration to county elections officials before printing new or revised forms that reflect the changes made to this section by Chapter 508 of the Statutes of 2007.

California Elections Code § 2194

(a) Except as provided in Section 2194.1, the affidavit of voter registration information identified in Section 7924.000 of the Government Code:

(1) Shall be confidential and shall not appear on any computer terminal, list, affidavit, duplicate affidavit, or other medium routinely available to the public at the county elections official's office.

(2) Shall not be used for any personal, private, or commercial purpose, including, but not limited to:

(A) The harassment of any voter or voter's household.

(B) The advertising, solicitation, sale, or marketing of products or services to any voter or voter's household.

(C) Reproduction in print, broadcast visual or audio, or display on the internet or any computer terminal unless pursuant to paragraph (3).

(3) Shall be provided with respect to any voter, subject to the provisions of Sections 2166, 2166.5, 2166.7, 2166.8, 2166.9, and 2188, to any candidate for federal, state, or local office, to any committee for or against any initiative or referendum measure for which legal publication is made, and to any person for election, scholarly, journalistic, or political purposes, or for governmental purposes, as determined by the Secretary of State.

(b)

(1) Notwithstanding any other law, the California driver's license number, the California identification card number, the social security number, and any other unique identifier used by the State of California for purposes of voter identification shown on the affidavit of voter registration of a registered voter, or added to voter registration records to comply with the requirements of the federal Help America Vote Act of 2002 (52 U.S.C. Sec. 20901 et seq.), are confidential and shall not be disclosed to any person.

(2) Notwithstanding any other law, the signature of the voter shown on the affidavit of voter registration or an image thereof is confidential and shall not be disclosed to any person, except as provided in subdivision (c).

California Government Code § 7924.000

(a) Except as provided in Section 2194 of the Elections Code, both of the following are confidential and shall not be disclosed to any person:

(1) The home address, telephone number, email address, precinct number, or other number specified by the Secretary of State for voter registration purposes.

(2) Prior registration information shown on an affidavit of registration.

(b) The California driver's license number, the California identification card number, the social security number, and any other unique identifier used by the State of California for purposes of voter identification shown on an affidavit of registration, or added to the voter registration records to comply with the requirements of the federal Help America Vote Act of 2002 (52 U.S.C. Sec. 20901 et seq.), are confidential and shall not be disclosed to any person.

(c) The signature of the voter that is shown on an affidavit of registration is confidential and shall not be disclosed to any person.

(d) For purposes of this section, "home address" means street address only, and does not include an individual's city or post office address.

California Code of Regulations, title 2, § 19001

As used in this Article, the following terms have the following meanings:

(h) “Voter registration information” means information on registered voters that may be provided to an authorized applicant by a source agency under the provisions of this Article, Elections Code section 2194, and Government Code section 6254.4. This information includes the following for each voter, to the extent that it is included in any individual voter’s record: registration county, unique registration identification number, name, residential address, mailing address, phone number, email address, language preference, date of birth, gender, party preference, registration status, registration date, precinct, registration method, place of birth, registration status reason (reason for the most recent update to the registration), voting assistance request status, permanent vote-by-mail status, county voter identification number, and voting participation history (election date and voting method).