

No. 26-2217

**UNITED STATES COURT OF APPEALS
FOR THE SEVENTH CIRCUIT**

UNITED STATES OF AMERICA,

Plaintiff-Appellant,

v.

WISCONSIN ELECTIONS COMMISSION, ET AL.,

Defendants-Appellees,

COMMON CAUSE, ET AL.,

Intervenors-Appellees.

On Appeal from the United States District Court for the Western
District of Wisconsin, No. 3:25-cv-1036-JDP, Before the Honorable
Judge James D. Peterson

**BRIEF FOR THE ELECTRONIC PRIVACY INFORMATION
CENTER AS AMICUS CURIAE IN SUPPORT OF APPELLEES
AND AFFIRMANCE**

CHRISTOPHER T. CASAMASSIMA

MAIREAD C. AHLBACH

SARA R. ORTON

WILMER CUTLER PICKERING

HALE AND DORR LLP

350 South Grand Avenue,

Suite 2400

Los Angeles, CA 90071

(213) 443-5300

chris.casamassima@wilmerhale.com

mairead.ahlbach@wilmerhale.com

sara.orton@wilmerhale.com

Counsel for Amicus Curiae Electronic Privacy Information Center

August 24, 2026

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 26-2217Short Caption: United States v. Wisconsin Elections Commission

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐

PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

- (1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):
Electronic Information Privacy Center
- (2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:
Wilmer Cutler Pickering Hale and Dorr LLP
- (3) If the party, amicus or intervenor is a corporation:
- i) Identify all its parent corporations, if any; and
None
- ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:
None
- (4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:
N/A
- (5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:
N/A

Attorney's Signature: /s/ Christopher T. Casamassima Date: 8/24/2026Attorney's Printed Name: Christopher T. CasamassimaPlease indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d).

Yes

☒

No

☐Address: 350 South Grand Avenue, Suite 2400Los Angeles, California 90071Phone Number: (213) 443-5300Fax Number: (213) 443-5400E-Mail Address: chris.casamassima@wilmerhale.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 26-2217Short Caption: United States v. Wisconsin Elections Commission

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐

PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

- (1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):
Electronic Information Privacy Center
- (2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:
Wilmer Cutler Pickering Hale and Dorr LLP
- (3) If the party, amicus or intervenor is a corporation:
- i) Identify all its parent corporations, if any; and
None
- ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:
None
- (4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:
N/A
- (5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:
N/A

Attorney's Signature: /s/ Sara R. Orton Date: 8/24/2026Attorney's Printed Name: Sara R. OrtonPlease indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d).

Yes

☐

No

☒Address: 350 South Grand Avenue, Suite 2400Los Angeles, California 90071Phone Number: (213) 443-5300Fax Number: (213) 443-5400E-Mail Address: sara.orton@wilmerhale.com

APPEARANCE & CIRCUIT RULE 26.1 DISCLOSURE STATEMENT

Appellate Court No: 26-2217Short Caption: United States v. Wisconsin Elections Commission

To enable the judges to determine whether recusal is necessary or appropriate, an attorney for a non-governmental party, amicus curiae, intervenor or a private attorney representing a government party, must furnish a disclosure statement providing the following information in compliance with Circuit Rule 26.1 and Fed. R. App. P. 26.1.

The Court prefers that the disclosure statements be filed immediately following docketing; but, the disclosure statement must be filed within 21 days of docketing or upon the filing of a motion, response, petition, or answer in this court, whichever occurs first. Attorneys are required to file an amended statement to reflect any material changes in the required information. The text of the statement must also be included in the front of the table of contents of the party's main brief. **Counsel is required to complete the entire statement and to use N/A for any information that is not applicable if this form is used.**

☐

PLEASE CHECK HERE IF ANY INFORMATION ON THIS FORM IS NEW OR REVISED AND INDICATE WHICH INFORMATION IS NEW OR REVISED.

- (1) The full name of every party that the attorney represents in the case (if the party is a corporation, you must provide the corporate disclosure information required by Fed. R. App. P. 26.1 by completing item #3):
Electronic Information Privacy Center
- (2) The names of all law firms whose partners or associates have appeared for the party in the case (including proceedings in the district court or before an administrative agency) or are expected to appear for the party in this court:
Wilmer Cutler Pickering Hale and Dorr LLP
- (3) If the party, amicus or intervenor is a corporation:
- i) Identify all its parent corporations, if any; and
None
- ii) list any publicly held company that owns 10% or more of the party's, amicus' or intervenor's stock:
None
- (4) Provide information required by FRAP 26.1(b) – Organizational Victims in Criminal Cases:
N/A
- (5) Provide Debtor information required by FRAP 26.1 (c) 1 & 2:
N/A

Attorney's Signature: /s/ Mairead C. Ahlbach Date: 8/24/2026Attorney's Printed Name: Mairead C. AhlbachPlease indicate if you are *Counsel of Record* for the above listed parties pursuant to Circuit Rule 3(d).

Yes

☐

No

☒Address: 350 South Grand Avenue, Suite 2400Los Angeles, California 90071Phone Number: (213) 443-5300Fax Number: (213) 443-5400E-Mail Address: mairead.ahlbach@wilmerhale.com

TABLE OF CONTENTS

	Page
TABLE OF AUTHORITIES	iii
INTEREST OF AMICUS CURIAE.....	1
BACKGROUND	2
SUMMARY OF ARGUMENT.....	5
ARGUMENT.....	6
I. THE DOJ’S DEMAND VIOLATES THE PRIVACY ACT.....	6
A. The Privacy Act Protects Individuals Against The Misuse, Wrongful Disclosure, And Breach Of Personal Data Held By Federal Agencies	7
B. The DOJ Failed To Adequately Provide Required Safeguards For Sensitive Personal Data.....	10
1. Noncompliance with FISMA is strong evidence of a Privacy Act violation.	11
2. The VRL data sought by the DOJ warrants the highest security classification under FISMA.	12
3. The security measures in the DOJ’s MOU are wholly inadequate.	14
a. Data access control.....	15
b. Third-party contractors.....	16
c. Audit protocols	16
d. Encryption.....	17

e.	Data breaches.....	18
f.	Data archiving.....	18
g.	Expedited collection	19
4.	States should rightly be concerned by DOJ's ongoing failure to comply with federal data security standards.....	20
C.	The Privacy Act Prohibits The DOJ From Collecting And Maintaining Records Of Protected First Amendment Activity, Including Unredacted VRLs.....	22
1.	The DOJ's demand for unredacted VRLs violates Section 552a(e)(7) of the Privacy Act.	22
2.	No exception to Section 552a(e)(7) applies.	24
D.	The DOJ Failed To Publish The Required System Of Records Notice.....	28
II.	THE DOJ'S DEMAND VIOLATES THE E-GOVERNMENT ACT	31
	CONCLUSION	34
	CERTIFICATE OF COMPLIANCE	
	CERTIFICATE OF SERVICE	

TABLE OF AUTHORITIES

CASES

	Page(s)
<i>Albright v. United States</i> , 631 F.2d 915 (D.C. Cir. 1980)	22, 23
<i>Buckley v. American Constitutional Law Foundation, Inc.</i> , 525 U.S. 182 (1999)	23
<i>Clarkson v. IRS</i> , 678 F.2d 1368 (11th Cir. 1982)	23, 26
<i>Doe v. Chao</i> , 540 U.S. 614 (2004)	2
<i>Doe v. Office of Personnel Management</i> , 2025 WL 513268 (D.D.C. Feb. 17, 2025)	33
<i>Electronic Privacy Information Center v. Presidential Advisory Commission on Election Integrity</i> , 878 F.3d 371 (D.C. Cir. 2017)	31
<i>FAA v. Cooper</i> , 566 U.S. 284 (2012)	1
<i>FCC v. AT&T</i> , 562 U.S. 397 (2011)	1
<i>In re United States Office of Personnel Management Data Security Breach Litigation</i> , 928 F.3d 42 (D.C. Cir. 2019)	11
<i>Public Interest Legal Foundation, Inc. v. Bellows</i> , 92 F.4th 36 (1st Cir. 2024)	1
<i>Reno v. Condon</i> , 528 U.S. 141 (2000)	2
<i>United States v. Councilman</i> , 385 F.3d 793 (1st Cir. 2004)	1

DOCKETED CASES

<i>American Federation of State, County and Municipal Employees, AFL-CIO v. SSA</i> , No. 1:25-cv-00596 (D. Md. Jan. 16, 2026)	21
<i>California v. HHS</i> , No. 25-5536 (N.D. Cal. 2025)	1

<i>Centro de Trabajadores Unidos v. Bessent</i> , No. 1:25-cv-00677 (D.D.C. Feb. 11, 2026)	21
<i>United States v. Weber</i> , No. 25-9149 (C.D. Cal.).....	29
<i>United States v. Wisconsin Elections Commission</i> , No. 25-1036 (W.D. Wis.)	3, 23, 26, 32

STATUTES AND RULES

5 U.S.C. §552a	7, 9, 10, 22-26, 28, 31
40 U.S.C. §11331	12
44 U.S.C.	
§3554.....	11, 12
§3555.....	20
§3601.....	31
E-Government Act, Pub. L. No. 107-347, §208, 116 Stat. 2899 (2002)	31, 32, 33
Privacy Act of 1974, Pub. L. No. 93-579, §2(a), 88 Stat. 1896 (codified at 5 U.S.C. §552a)	7
Fed. R. App. P. 29.....	1

ADMINISTRATIVE AND LEGISLATIVE MATERIALS

Exec. Order No. 14399, <i>Ensuring Citizenship Verification and Integrity in Federal Elections</i> , 91 Fed. Reg. 17125 (Mar. 31, 2026)	4
Privacy Act Guidelines, 40 Fed. Reg. 28949 (July 1, 1975) ...	22-23, 25-26, 28
Privacy Act of 1974; Systems of Records, 68 Fed. Reg. 47610 (Aug. 11, 2003).....	29, 30
Privacy Act of 1974; Systems of Records, 70 Fed. Reg. 43904 (July 29, 2005)	29, 30

Privacy Act of 1974; Systems of Records, 82 Fed. Reg. 24147 (May 25, 2017)	29, 31
120 Cong. Rec. H10892 (daily ed. Nov. 20, 1974)	26
120 Cong. Rec. H10952 (daily ed. Nov. 21, 1974)	26
Senate Committee on Government Operations, 94th Cong., Legislative History of the Privacy Act of 1974 (Comm. Print 1976)	7, 8, 9
S. Rep. No. 1183, <i>as reprinted in</i> 1974 U.S.C.C.A.N. 6916, 6971	26

OTHER AUTHORITIES

Barrett, Devlin & Nick Corasaniti, <i>Trump Administration Quietly Seeks to Build National Voter Roll</i> , N.Y. Times (Sept. 9, 2025), https://www.nytimes.com/2025/09/09/us/politics/trump- voter-registration-data.html	27
Bolten, Joshua B., Dir., OMB, Executive Office of the President, M03-22, Memorandum for Heads of Executive Departments and Agencies (Sept. 26, 2003)	32
Brennan Center, <i>Tracker of Justice Department Requests for Voter Information</i> (last updated Aug. 18, 2026), https://www.brennancenter.org/our-work/research- reports/tracker-justice-department-requests-voter- information	2, 3, 14
Colorado Memorandum of Understanding (Dec. 1, 2025), https://www.brennancenter.org/media/14806/download/ 2025-12-01-doj-mou-to-colorado.pdf?inline=1	14-19, 21
Electronic Privacy Information Center, <i>FISMA Gap Analysis of the U.S. Department of Justice’s Collection of State Voter Registration List Data</i> (Feb. 13, 2026), https://epic.org/wp-content/uploads/2026/02/FISMA- Gap-Analysis-Explanation-and-Appendix.pdf	14

Electronic Privacy Information Center, <i>The Privacy Act of 1974</i> , https://epic.org/the-privacy-act-of-1974	9
<i>Help America Vote Verification (HAVV) Transactions by State</i> , SSA.gov, https://www.ssa.gov/data/havv	13
<i>Information Systems and Organizations</i> , NIST SP 800-53B (Oct. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf	13
Joffe-Block, Jude, <i>The Justice Department Plans to Share Sensitive Voter Data with Homeland Security</i> , NPR (Mar. 27, 2026), https://www.npr.org/2026/03/27/nx-s1-5764266/voter-data-trump-doj-dhs	15
NIST, <i>Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations</i> , SP 800-161 Rev. 1 (May 2022), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf	16
NIST, <i>Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)</i> , NIST SP 800-122 (Apr. 2010)	13
NIST, <i>Security and Privacy Controls for Information Systems and Organizations</i> , NIST SP 800-53 Rev. 5 (Sept. 2020), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf	13, 14, 15, 17, 18
NIST, <i>Standards for Security Categorization of Federal Information and Information Systems</i> , FIPS PUB 199 (Feb. 2004), https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf	12

NIST, <i>Transitioning the Use of Cryptographic Algorithms and Key Lengths</i> , NIST SP 800-131Ar3 ipd, (Oct. 2024), https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar3.ipd.pdf	17
Office of Management & Budget, Executive Office of the President, OMB Circular A-130 Revised, <i>To the Heads of Executive Departments and Agencies</i> (July 28, 2016), https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource	33
Office of Management & Budget, Executive Office of the President, OMB Memorandum M-17-12, <i>Preparing for and Responding to a Breach of Personally Identifiable Information</i> (Jan. 3, 2017), https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12.pdf	18
<i>The SSN Numbering Scheme</i> , SSA.gov, https://www.ssa.gov/history/ssn/geocard.html	13
United States Department of Health, Education & Welfare, Report of the Secretary’s Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (1973).....	9
United States Department of Justice, Office of the Inspector General, <i>Audit of the Civil Rights Division’s Information Security Management Program Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2025</i> , Report Number 26-044, (Mar. 2026), https://oig.justice.gov/sites/default/files/reports/26-044.pdf	20
United States Participation in Interpol Computerized Search File Project, 5 U.S. Op. Off. Legal Counsel 373 (1981)	24

INTEREST OF AMICUS CURIAE

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and other constitutional values. EPIC's Advisory Board includes distinguished experts in law, technology, and public policy concerned about the protection of privacy in the modern era.¹

EPIC has routinely participated as amicus curiae before numerous courts in leading cases involving the application of federal privacy and voting rights law. *E.g.*, *California v. HHS*, No. 25-5536 (N.D. Cal. 2025) (Privacy Act); *Public Int. Legal Found., Inc. v. Bellows*, 92 F.4th 36 (1st Cir. 2024) (interaction of National Voter Registration Act and state voter privacy protections); *FAA v. Cooper*, 566 U.S. 284 (2012) (Privacy Act); *FCC v. AT&T*, 562 U.S. 397 (2011) (personal privacy exemptions in the Freedom of Information Act); *United States v. Councilman*, 385

¹ In accordance with Federal Rule of Appellate Procedure 29: all parties consented to the filing of this brief; no monetary contributions were made for the preparation or submission of this brief; and this brief was not authored, in whole or in part, by counsel for a party.

F.3d 793 (1st Cir. 2004) (Electronic Communications Privacy Act); *Doe v. Chao*, 540 U.S. 614 (2004) (Privacy Act); *Reno v. Condon*, 528 U.S. 141 (2000) (Drivers Privacy Protection Act).

In addition to participating as amicus curiae in leading privacy cases, EPIC has engaged in numerous other forms of advocacy, including through authoring extensive publications and analysis on emerging issues of privacy law and policy.

BACKGROUND

Since 2025, the government has undertaken dramatic and unprecedented efforts to centralize control over election administration in the Federal Executive—at the expense of the autonomy of states, the security of sensitive voter data, and the privacy rights of individual citizens. At the center of these efforts is the Department of Justice’s demand for unredacted voter registration lists (VRLs) from at least 48 states and Washington, DC. *See* Brennan Ctr., *Tracker of Justice Department Requests for Voter Information* (last updated Aug. 18, 2026).² These VRLs contain highly sensitive, personally identifiable

² Available at <https://www.brennancenter.org/our-work/research-reports/tracker-justice-department-requests-voter-information>.

data on millions of voters, including driver's license numbers and partial or full Social Security Numbers (SSNs). *Id.*

This appeal arises from the DOJ's June and December 2025 demands for Wisconsin's unredacted VRL. *See* Order Granting Mots. to Dismiss 3, *United States v. Wisconsin Elections Comm'n*, No. 25-1036 (W.D. Wis. May 21, 2026). The DOJ claimed to need this list to ensure Wisconsin's compliance with the Help America Vote Act (HAVA). *Id.* In response to the first request, the Wisconsin Elections Commission ("Commission") referred the DOJ to a redacted copy of the VRL and "answered the [DOJ's] questions about its list maintenance procedures." *Id.* at 3. When the DOJ demanded an unredacted version, the Commission refused, citing state privacy laws. *Id.* The DOJ then sued the Commission and each of its members to compel disclosure, invoking its alleged authority to obtain the VRL under Title III of the Civil Rights Act of 1960 (CRA). *Id.* The district court dismissed the case, finding that the VRL was "not a record subject to production under Title III." *Id.* at 5. The DOJ appealed to this Court. *See* Notice of Appeal (June 5, 2026), Dkt. 1.

EPIC submits this amicus brief as an authority on the protection of civil liberties, privacy, the First Amendment, and other constitutional values to underscore that the DOJ's collection of this data would violate various federal privacy and data security statutes—namely the Privacy Act of 1974, the Federal Information Security Modernization Act, and the E-Government Act.

The privacy and security risks posed by the federal government's attempt to obtain the information it seeks through its demands of Wisconsin's unredacted VRL—alone more than sufficient to warrant filing this brief—are only heightened by other recent federal government activity. The executive branch's effort to federalize elections has continued since this appeal was filed. In March 2026, President Trump issued an executive order instructing the United States Postal Service, working in conjunction with the Social Security Administration and the Department of Homeland Security, to refuse to send mail-in ballots to voters in states across the country unless the federal government first verifies their citizenship against its own “citizenship list.” Exec. Order No. 14399, *Ensuring Citizenship Verification and Integrity in Federal Elections*, 91 Fed. Reg. 17125 (Mar.

31, 2026).³ While that executive action is not the subject of this appeal, it is illustrative of the federal government's unprecedented and ongoing attempt to federalize elections at the expense of bedrock privacy, security, and constitutional safeguards. The DOJ's demand at issue here is a critical part of this overall effort by the executive branch and should be viewed in that context.

SUMMARY OF ARGUMENT

First, this Court should decline to enforce the DOJ's demand because it violates the Privacy Act. The Privacy Act requires agencies to comply with various restrictions on the collection, maintenance, and use of personal data. The DOJ's demand violates the Privacy Act because: (1) the DOJ has failed to comply with federal data privacy and security standards, as detailed within the Federal Information Security Modernization Act (FISMA); (2) the DOJ's demand violates the Privacy Act's prohibition on the collection of records detailing the exercise of First Amendment freedoms, and no exception applies; and (3) the DOJ

³ *Available at* <https://www.whitehouse.gov/presidential-actions/2026/03/ensuring-citizenship-verification-and-integrity-in-federal-elections>.

has failed to publish a required system of records notice informing the public of the character and uses of the data it intends to collect.

Second, the DOJ's demand violates the E-Government Act. The E-Government Act requires that the DOJ conduct a Privacy Impact Assessment (PIA) before initiating a new collection of personally identifiable information. The DOJ failed to do so. And given that it has already begun collecting data from states, it can no longer remedy the violation.

ARGUMENT

I. THE DOJ'S DEMAND VIOLATES THE PRIVACY ACT

The Privacy Act provides crucial guardrails which govern how federal agencies collect and manage large swaths of sensitive personal information. This Court should refuse to enforce the DOJ's demand for unredacted state VRLs because the DOJ's demand violates the Privacy Act in at least three distinct ways. First, the DOJ has failed to implement the safeguards for maintaining sensitive personal data that are required by the Act. Second, the Act prohibits the DOJ from collecting records of the individual exercise of First Amendment freedoms, including VRLs, and none of the three recognized statutory

exceptions applies here. Finally, the Act requires the DOJ to publish a system of records notice in connection with establishing or revising a system of records, which the DOJ has failed to do.

A. The Privacy Act Protects Individuals Against The Misuse, Wrongful Disclosure, And Breach Of Personal Data Held By Federal Agencies

In 1974, Congress enacted the Privacy Act in response to growing concerns that the federal government's increasing use of computerized record-keeping systems posed serious threats to privacy and civil liberties. Pub. L. No. 93-579, §2(a), 88 Stat. 1896, codified at 5 U.S.C. §552a ("Congress finds that ... the increasing use of computers ... has greatly magnified the harm to individual privacy that can occur from any collection, maintenance, use, or dissemination of personal information[.]"); *see also* S. Comm. on Gov't Operations, 94th Cong., Legislative History of the Privacy Act of 1974, at 1195 (Comm. Print 1976) (hereinafter "S. Rep. on Privacy Act") (noting that "concern that government and business accumulate too much data on private citizens" made "the protection of individual privacy an issue high on the priority list of scores of government policy makers").⁴ As technological

⁴ Available at https://www.justice.gov/d9/privacy_source_book.pdf.

advancements in the 1960s and early 1970s made it easier for the government to aggregate, cross-reference, and disseminate personal information, lawmakers and the public became increasingly alarmed by the risk that detailed dossiers could be compiled on individuals without adequate safeguards or transparency. *Cf.* S. Rep. on Privacy Act, at 1195-1196 (noting that “fear about the creation of a ‘national data bank’ [first] arose in the mid-1960s” and resurfaced following “[t]he abuses of individual liberties documented by Watergate”).

The Privacy Act was influenced by a 1973 report by the Department of Health, Education, and Welfare (HEW) which recommended adoption of a Code of Fair Information Practices to govern the collection, maintenance, and use of personal data by federal agencies. S. Rep. on Privacy Act, at 300, 828. The HEW Report articulated several core principles: (1) no system of personal records should exist in secret; (2) individuals should have the ability to learn what information the government maintains about them and how it is used; (3) personal data collected for one purpose should not be used for another without consent; (4) individuals should be able to correct inaccurate records; and (5) agencies must ensure data accuracy and guard against misuse. *See*

Elec. Priv. Info. Ctr., *The Privacy Act of 1974* (summarizing the HEW Report) (citing U.S. Dep't of Health, Educ. & Welfare, Report of the Secretary's Advisory Committee on Automated Personal Data Systems, Records, Computers, and the Rights of Citizens (1973)).⁵ Congress incorporated these principles into the Privacy Act, making the statute the central federal framework governing the collection and handling of personal information by executive-branch agencies. S. Rep. on Privacy Act, at 300 (noting that the Privacy Act “embodies the major principles of [the HEW Report’s] recommendations as they apply to an individual’s access to records in the Federal Government”).

The Act grants individuals the right to review records about themselves that are maintained by federal agencies. 5 U.S.C. §552a(f). The Act additionally imposes several duties and obligations on federal agencies in connection to the maintenance of data concerning U.S. citizens. Notably, the Act requires agencies to publish a system of records notice (SORN) in the Federal Register before establishing a new system of records, to notify the public of the intended uses of the system and to permit individuals to submit feedback to the agency. *Id.*

⁵ Available at <https://epic.org/the-privacy-act-of-1974>.

§552a(e)(4). The Act also imposes strict limitations on an agency's ability to disclose information placed in a system of records and requires the agency to keep accurate accounts of when and to whom personal records are disclosed. *Id.* §552a(b)-(c). The Act additionally requires that agencies maintain in their records only the minimum amount of information "relevant and necessary" to accomplish their purposes, and that agencies "establish appropriate ... safeguards" to protect the security and integrity of personal data. *Id.* §552a(e)(1), (10). And the Act prohibits agencies from maintaining any records "describing how an individual exercises rights guaranteed by the First Amendment" unless the record meets one of three very narrow exceptions. *Id.* §552a(e)(7).

B. The DOJ Failed To Adequately Provide Required Safeguards For Sensitive Personal Data

The DOJ's failure to develop adequate safeguards to protect sensitive data in VRLs violates the Privacy Act. The Privacy Act broadly requires federal agencies to "establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records" and to "protect against any anticipated threats or hazards to their security or integrity." 5 U.S.C. §552a(e)(10). This requires the DOJ—*both during collection and*

beyond—to proactively maintain specific data security standards to prevent the inadvertent disclosure or destruction of data. As discussed below, the DOJ’s procedures for “protecting” VRLs fall well short of complying with the security safeguards contemplated by the Privacy Act.

1. Noncompliance with FISMA is strong evidence of a Privacy Act violation.

Courts look to an agency’s compliance with the Federal Information Security Modernization Act of 2014 (FISMA) in evaluating whether it has fulfilled its obligations to establish adequate safeguards for data under the Privacy Act. *E.g., In re U.S. Office of Pers. Mgmt. Data Security Breach Litig.*, 928 F.3d 42, 54-60 (D.C. Cir. 2019) (holding that noncompliance with FISMA data security standards and ignored warnings in FISMA audits by the Inspector General was evidence of a willful violation of the Privacy Act). FISMA is the principal federal statute governing data security. It requires federal agencies to provide information security protections for both the information they collect and the databases this information is housed in. 44 U.S.C. §§3554(a)(1)(A)(i)-(ii). The protections that are required vary based on the security categorization of the collected information and must be

based on federal standards set by the National Institute for Standards and Technology (NIST). 44 U.S.C. §§3554(a)(1)(A), (B)(i); 40 U.S.C. §11331(b)(2)(A)(i).

2. The VRL data sought by the DOJ warrants the highest security classification under FISMA.

Following the process set up by NIST, an agency designates a security category (low, medium, or high) based on the information's risk level and the magnitude of harm in the event of a breach.⁶ These categories reflect the potential impact on the confidentiality, integrity, and availability of data should an information system be jeopardized. For example, a dataset might be classified as "high" in terms of confidentiality because it contains a large volume of SSNs and a breach could therefore result in widespread identity theft.

The DOJ's planned collection of state VRLs triggers FISMA's most stringent data security safeguards. The VRLs at issue contain highly sensitive information on millions of voters. At a minimum, the DOJ seeks each voter's full name, date of birth, residential address, and

⁶ NIST, *Standards for Security Categorization of Federal Information and Information Systems*, FIPS PUB 199, at 1-3 (Feb. 2004), <https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf>.

state driver's license number or the last four digits of their Social Security Number.⁷ NIST standards make clear that such “personally identifiable information” should be categorized especially carefully, and requires considering, among other things, how easily the data can be used to identify people, the quantity of records, the sensitivity of the data put together, the context of collection, and existing confidentiality obligations on the data.⁸ The data in the VRLs are numerous, can easily identify people when combined, and are being collected amid a larger-scale campaign by the executive branch to create a national repository of voter data. Thus, the VRL data should be classified as “high” risk, and the DOJ must take extra precautions to protect it.⁹

⁷ The last four digits of a SSN are the most sensitive and uniquely identifying portion because of the way SSNs were generated prior to 2011. The remaining five numbers are more easily inferred because of their basis in birthplace and approximate birth year. See *The SSN Numbering Scheme*, SSA.gov (last accessed Apr. 16, 2026), <https://www.ssa.gov/history/ssn/geocard.html>. Five states—New Mexico, Kentucky, South Carolina, Tennessee, and Virginia—still use full SSNs on voter registration and thus would be providing the DOJ with all nine digits. See *Help America Vote Verification (HAVV) Transactions by State*, SSA.gov, <https://www.ssa.gov/data/havv>.

⁸ NIST, *Guide to Protecting the Confidentiality of Personally Identifiable Information* (PII), NIST SP 800-122, at 3-3, 3-5 (Apr. 2010), <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-122.pdf>.

⁹ NIST, *Control Baselines for Information Systems and Organizations*, NIST SP 800-53B, at 6 (Oct. 2020), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53B.pdf> (hereinafter “NIST SP 800-53B”). Explanations of these security controls are available at NIST, *Security and Privacy Controls for Information Systems and Organizations*, NIST SP 800-53 Rev. 5 (Sept. 2020),

3. The security measures in the DOJ's MOU are wholly inadequate.

Despite the high risk level of the data sought, the DOJ has done nothing to suggest that it will implement adequate security measures as required by FISMA. Beginning in December 2025, the DOJ sent states a draft Memorandum of Understanding (MOU).¹⁰ This MOU comprises the procedures that the DOJ proposes to enact to govern the collection, dissemination, and storage of the data it seeks from states. Despite containing boilerplate recitations of compliance with DOJ's data protection obligations, it falls far short of the particularized security controls that the DOJ is required to establish under FISMA and corresponding NIST standards.¹¹

<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf> (hereinafter "NIST, SP 800-53r5").

¹⁰ Based on publicly available information—including MOUs signed by Alaska and Texas, which have agreed to give the DOJ their voter data—the MOUs sent to states are identical. See Brennan Ctr., *Tracker of Justice Department Requests for Voter Information* (last updated Aug. 18, 2026), <https://www.brennancenter.org/our-work/research-reports/tracker-justice-department-requests-voter-information>. The analysis in this brief is based on the contents of Colorado's MOU (which it has not signed) but the application to Wisconsin's data would be identical. See Colorado MOU, (Dec. 1, 2025), <https://www.brennancenter.org/media/14806/download/2025-12-01-doj-mou-to-colorado.pdf?inline=1> (hereinafter "the MOU").

¹¹ EPIC's full analysis of the MOU's deficiencies under FISMA, which includes many more issues than can be discussed in this brief, is available at the EPIC website. See Elec. Privacy Info. Ctr., *FISMA Gap Analysis of the U.S. Department of Justice's Collection of State Voter Registration List Data* (Feb. 13, 2026),

a. Data access control

The MOU is silent on some of the most basic data access-control safeguards. NIST standards require agencies handling sensitive personal data to clearly define who can access that data, limit access to only those with a legitimate need, and periodically review and revoke permissions.¹² The MOU does none of this. It contains no plan for authenticating users, restricting VRL data to those with an actual need for it, or reviewing user privileges. Without these protections, unauthorized users, including other federal agencies, may access this data and use it to further their own goals. Indeed, the Trump administration has made clear that it specifically intends to share VRLs collected by states with the Department of Homeland Security (DHS) to run the data through a citizenship lookup tool. Joffe-Block, *The Justice Department Plans to Share Sensitive Voter Data with Homeland Security*, NPR (Mar. 27, 2026).¹³

<https://epic.org/wp-content/uploads/2026/02/FISMA-Gap-Analysis-Explanation-and-Appendix.pdf>.

¹² NIST, SP 800-53r5 at 18-28.

¹³ Available at <https://www.npr.org/2026/03/27/nx-s1-5764266/voter-data-trump-doj-dhs>.

b. Third-party contractors

The MOU specifically contemplates giving voter data to third-party contractors without any vetting framework. NIST's supply-chain guidance requires agencies to vet contractors and bind them to certain security controls before giving them access to sensitive data.¹⁴ Section IX of the MOU permits contractors assisting with "list maintenance" to access VRL data but contains no explicit language to bind contractors to the same controls as the government. This lack of oversight risks leaving sensitive VRL data in the hands of contractors with substandard data security protocols.

c. Audit protocols

The MOU lacks meaningful review and accountability provisions. Under NIST standards, agencies must actively audit their data security practices and preserve audit records.¹⁵ Although Section IX of the MOU states that the DOJ will "activate audit logging," it includes none of the required specificity for when or whether audit records will be protected.

¹⁴ NIST, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*, SP 800-161 Rev. 1 at 38, 42-43, 64 (May 2022), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-161r1.pdf>.

¹⁵ NIST, SP 800-53r at 70-725.

The MOU also includes no discussion of how breaches found in audits will be reported to states, leaving states no way of knowing about potential misuses of their voter data. The lack of these protections renders the MOU's vague "audit logging" language meaningless and raises serious questions of accountability.

d. Encryption

The MOU does not require encryption of voter data stored on DOJ systems. Unencrypted data, if exposed to unauthorized parties, is easily readable. NIST standards therefore instruct agencies to use cryptographic keys, so that only users with these keys can "unlock" and view sensitive data.¹⁶ Yet the only reference of encryption in the MOU is a note that VRL data will not be copied to unencrypted external storage. The MOU does not require encryption of the DOJ's internal voter database itself, which would allow VRL data to be easily readable if the DOJ system were ever compromised.

¹⁶ NIST, SP 800-53r5 at 307-309; NIST, *Transitioning the Use of Cryptographic Algorithms and Key Lengths*, NIST SP 800-131Ar3 ipd (Oct. 2024), <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-131Ar3.ipd.pdf>.

e. Data breaches

The MOU does not have a clear plan for responding to data breaches. NIST standards require agencies to establish a specific “incident-response” plan, which would include timelines, reporting obligations, and investigative steps.¹⁷ OMB guidance even requires some breaches to be reported within an hour.¹⁸ In contrast, Section X of the MOU merely says the DOJ will make “reasonable and timely efforts” to notify states if a breach occurs, leaving this largely up to DOJ’s discretion. The MOU’s discretionary language does not reflect the specific reporting standards set by FISMA and NIST and leaves uncertain how, or if, states will learn of data breaches concerning their voters.

f. Data archiving

The MOU states that while hard copies of data will be destroyed, “electronic data containing confidential information” will be archived

¹⁷ NIST, SP 800-53r5 at 152-161.

¹⁸ Office of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-17-12, *Preparing for and Responding to a Breach of Personally Identifiable Information*, at 45 (Jan. 3, 2017), <https://obamawhitehouse.archives.gov/sites/default/files/omb/memoranda/2017/m-17-12.pdf> (“FY 2014 FISMA Reporting and Privacy Management Guidance for the requirement that agencies report to US-CERT cyber-related (electronic) incidents with confirmed loss of confidentiality, integrity, or availability within one hour”).

even after the DOJ is done using it. The MOU does not offer any explanation for why this concededly “confidential information” will be permanently archived. And even if there were a basis for retaining the data, under NIST standards, agencies should create data architectures that minimize the risks associated with retaining unnecessary data.¹⁹ The MOU does nothing of the sort. As a general matter, permanently storing rather than deleting information presents some additional risk of its dissemination, accidental or otherwise. But more specifically here, when the DOJ archives VRL data, such data may be subject to the National Archives and Records Administration retention schedules, which would create a *permanent* record of voter data that cannot be deleted.

g. Expedited collection

Finally, the MOU includes expedited timelines for the transfer of VRL data, raising added concern that the security controls in place at the time of transfer will be insufficient or nonexistent. Section IV of the MOU, for example, asks that the Agreement be signed within seven (7) days of the DOJ having presented it. The same Section further presses

¹⁹ NIST, SP 800-53r5 at 198-200.

for states to act as quickly as possible, stating that “no part of this Agreement or execution is intended to, or will, cause delay of the transmission of your state’s VRL” to the DOJ for analysis. This pressure on states to move quickly and lack of any negotiation process casts serious doubt on the DOJ’s commitment to data security.

4. States should rightly be concerned by DOJ’s ongoing failure to comply with federal data security standards.

Concerns that the DOJ would not adhere to FISMA standards post-collection are well-founded. FISMA requires agency Inspectors General to complete annual audits of their agencies’ information security practices to ensure effectiveness and compliance with FISMA.²⁰ An audit of DOJ’s Civil Rights Division conducted just last year found “weaknesses in 3 of the 10 FISMA domain areas.”²¹ The audit determined that these areas “need to be strengthened” to ensure that the data held by the Civil Rights Division were adequately protected. Concerns about FISMA compliance are especially valid when considered

²⁰ 44 U.S.C. §3555(b).

²¹ U.S. Dep’t of Justice, Office of the Inspector General, *Audit of the Civil Rights Division’s Information Security Management Program Pursuant to the Federal Information Security Modernization Act of 2014, Fiscal Year 2025*, Report Number 26-044 (Mar. 2026) <https://oig.justice.gov/sites/default/files/reports/26-044.pdf>.

against the backdrop of recent data security violations by federal agencies involving the wrongful disclosure of personal data from thousands of individuals. *See* Notice of Corrections to the Record, *American Federation of State, County And Municipal Employees, AFL-CIO v. SSA*, No. 1:25-cv-00596 (D. Md. Jan. 16, 2026), Dkt. 197 (admission by government that DOGE employees circumvented agency procedures by using unauthorized third-party servers for data sharing and agreeing to share Social Security data with an advocacy group looking for evidence of voter fraud to overturn election results); Defendant's Corrected Notice on Status of Requests for Return Information, *Centro de Trabajadores Unidos, v. Bessent*, No. 1:25-cv-00677 (D.D.C. Feb. 11, 2026), Dkt. 73 (admission by government that IRS used a faulty automated verification system to improperly share the sensitive information of thousands of taxpayers).

In sum, to the extent that the DOJ may lawfully collect bulk VRL data at all, FISMA requires that this data be protected by strict security controls. The MOU makes clear that the DOJ has no plan to implement these controls, which is strong evidence of a Privacy Act violation.

C. The Privacy Act Prohibits The DOJ From Collecting And Maintaining Records Of Protected First Amendment Activity, Including Unredacted VRLs

The Privacy Act additionally prohibits federal agencies from maintaining any records describing how individuals exercise First Amendment rights—unless maintenance of such records is “expressly authorized” by another statute, by the individuals whose information the record contains, or for the purposes of “an authorized law enforcement activity.” 5 U.S.C. §552a(e)(7). And though the Privacy Act states that agencies shall not “maintain” records pertaining to the individual exercise of First Amendment rights, the term “maintain” also encompasses the “collect[ion], use, or disseminat[ion]” of such records, *see id.* §552a(a)(3) (defining terms), as well as “any combination of ... record-keeping functions” regulated under the Privacy Act, OMB Privacy Act Guidelines, 40 Fed. Reg. 28949, 28951 (July 1, 1975); *accord Albright v. United States*, 631 F.2d 915, 918 (D.C. Cir. 1980) (citing 5 U.S.C. §552a(a)(3)).

1. The DOJ’s demand for unredacted VRLs violates Section 552a(e)(7) of the Privacy Act.

VRLs are squarely within the scope of the Privacy Act’s prohibition on the collection, maintenance, use, or dissemination of records of

protected First Amendment expression. *See Buckley v. American Const. L. Found., Inc.*, 525 U.S. 182, 195 (1999) (holding that choosing whether to register to vote necessarily implicates “political thought and expression”); *see also* OMB Privacy Act Guidelines, 40 Fed. Reg. at 28965 (“In determining whether or not a particular activity constitutes the exercise of a right guaranteed by the First Amendment, agencies will apply the broadest reasonable interpretation.”) (internal quotations omitted). As such, the DOJ’s demand for unredacted state VRLs violates Section 552a(e)(7) of the Privacy Act.

The DOJ seems to suggest that the Privacy Act only regulates management of information stored within a federal agency’s system of records and does not prevent states from sharing information with federal agencies. *See* U.S. Mem. in Opp. to Mots. to Dismiss 29, *United States v. Wisconsin Elections Comm’n*, No. 25-1036 (W.D. Wis. Mar. 2, 2026). But the Act’s prohibition on collecting records of First Amendment expression applies regardless of how an agency stores such records. *See Clarkson v. IRS*, 678 F.2d 1368, 1374-1377 (11th Cir. 1982) (citing *Albright*, 631 F.2d at 918 (holding that the Privacy Act prohibited the federal government even from videotaping a meeting

between federal employees and their supervisor regarding the analysts' recent demotions, despite the fact that the agency never intended to make the tape part of a system of records)). And the fact that a record originates from a state government does not exempt the record from the provisions of the Privacy Act. *See* U.S. Participation in Interpol Computerized Search File Project, 5 U.S. Op. Off. Legal Counsel 373, 378 (1981) ("There is no suggestion ... in either the Privacy Act or FOIA that records collected by a federal agency are exempt from the requirements of those statutes if they are contributed by a state agency."). Since the DOJ seeks records of protected First Amendment Activity, the DOJ's demand violates the Privacy Act, regardless of the source of the records or how the DOJ intends to store them.

2. No exception to Section 552a(e)(7) applies.

The DOJ has not invoked any of the three statutory exceptions to the Privacy Act's prohibition on the collection of First Amendment records, which are that the collection is: (1) authorized by the individual; (2) expressly authorized by statute; or (3) "pertinent to and within the scope of an authorized law-enforcement activity." 5 U.S.C.

§552a(e)(7). While the DOJ's silence is alone dispositive of the issue, none of the exceptions apply here in any event.

First, there is no evidence to suggest that individual voters have in any way authorized the DOJ to collect their personal data from state VRLs.

Second, the DOJ has not identified any statute which authorizes the collection of unredacted state VRLs. *See* OMB Privacy Act Guidelines, 40 Fed. Reg. at 28965 (“Specific authorization means that a statute *explicitly* provides that an agency may maintain records on activities whose exercise is covered by the First Amendment; not merely that the agency is authorized to establish a system of records.”) (emphasis added).

And finally, the DOJ has not identified any “authorized law enforcement activity” which would require the collection of unredacted VRLs from states. As Congress made clear, the purpose of this exception was “to make certain that political and religious activities are not *used as a cover for illegal or subversive activities*.” OMB Privacy Act Guidelines, 40 Fed. Reg. at 28965 (quoting 120 Cong. Rec. H10892 (daily ed. Nov. 20, 1974)) (emphasis added). “[T]here was no intention

to interfere with First Amendment rights.” *Id.* (quoting 120 Cong. Rec. H10952 (daily ed. Nov. 21, 1974)). Accordingly, this exception must be applied narrowly, in cases where the information sought is “immediately needed” by law enforcement. *Clarkson*, 678 F.2d at 1375 (quoting S. Rep. No. 1183, 93d Cong., *as reprinted in* 1974 U.S.C.C.A.N. 6916, 6971). This interpretation of Section 552a(e)(7) justly prevents the government from “collect[ing] protected information ... about law-abiding Americans, on the off-chance that” it “might possibly have to deal with them in the future.” *Id.* (quoting S. Rep. No. 1183, 1974 U.S.C.C.A.N. at 6971).

Here, the DOJ comes nowhere close to demonstrating the immediate law enforcement need for unredacted VRLs. In its demand letter to the Commission on June 17, 2025, the DOJ cited a desire to “assess Wisconsin’s compliance with the Help America Vote Act (“HAVA”).” *See* U.S. Mot. for Ord. to Produce Records, Ex. 1 at 5, *United States v. Wisconsin Elections Comm’n*, No. 25-1036 (W.D. Wis. Dec. 18, 2025). But the DOJ failed to articulate any factual basis for a plausible suspicion that Wisconsin is in violation of HAVA. This scant and generalized purported concern—which is not an immediate law

enforcement justification required by the Privacy Act—is an obvious pretext. Since May of 2025, the DOJ has sent nearly identical demands for unredacted VRLs to over 48 states and the District of Columbia. *See* Brennan Ctr., *Tracker of Justice Department Requests for Voter Information* (last updated Aug. 18, 2026). It strains credulity for the DOJ to ask this Court to believe that such a series of unprecedented, blanket demands for sensitive voter data could be related to any immediate law enforcement need. The DOJ has failed to articulate any plausible basis to even suspect that *virtually every state in the country* has failed to comply with HAVA (or the NVRA), nor does it make any particularized showing with respect to Wisconsin to justify its extraordinary demand. The true purpose of the DOJ’s demand is not to enforce compliance with federal election law, but to create a national database of voter information that the Trump administration will utilize to accomplish its political ends. *See* Barrett & Corasaniti, *Trump Administration Quietly Seeks to Build National Voter Roll*, N.Y. Times (Sept. 9, 2025).²²

²² Available at <https://www.nytimes.com/2025/09/09/us/politics/trump-voter-registration-data.html>.

D. The DOJ Failed To Publish The Required System Of Records Notice

Even if the DOJ could lawfully collect the records it seeks, the Privacy Act nonetheless requires that “upon establishment or revision” of a system of records, a federal agency must publish “a notice of the existence and character of the system of records” in the Federal Register (known as a system of records notice, or “SORN”). 5 U.S.C. §552a(e)(4). This public notice provision is “central to the achievement of one of the basic objectives of the Act: fostering agency accountability through a system of public scrutiny.” OMB Privacy Act Guidelines, 40 Fed. Reg. at 28962. It is “premised on the concept that there should be no system of records whose very existence is secret.” *Id.* The SORN itself must include extensive details about the system of records to be established, and these details are catalogued expressly in Section 552a(e)(4). But at its core, the purpose of the SORN is “to *inform the public* of the existence of systems of records,” “[t]he kinds of information maintained,” “[t]he kinds of individuals on whom information is maintained,” “[t]he purposes for which [records] are used,” and “[h]ow individuals can exercise their rights under the Act.” OMB Privacy Act Guidelines, 40 Fed. Reg. at 28962 (emphasis added).

The DOJ has not complied with the Privacy Act's statutory mandate to publish a SORN which would adequately inform the public of the existence, character, and intended uses of the records it seeks to collect. In its relentless campaign to obtain unredacted VRLs from nearly every state, the DOJ has tried citing several existing SORNs as evidence of compliance with its public notice obligations under the Privacy Act: 68 Fed. Reg. 47610, 47611-47613 (Aug. 11, 2003) (2003 SORN); 70 Fed. Reg. 43904, 43904 (July 29, 2005) (2005 SORN); and 82 Fed. Reg. 24147, 24147-24151 (May 25, 2017) (2017 SORN). Yet none of these SORNs does anything "to put a member of the American public on notice that specifically, their voter registration data is going to be collected on an unprecedented level and used for a plethora of government activity." Order Granting Mots. to Dismiss 29, *United States v. Weber*, No. 25-9149 (C.D. Cal. Jan. 15, 2026).

The 2003 SORN, entitled "Central Civil Rights Division Index File and Associated Records, CRT-001," describes the categories of records contained in the system as "case files, matters, memoranda, correspondence, studies, and reports relating to enforcement of civil rights laws and other various duties of the Civil Rights Division."

68 Fed. Reg. at 47611. It describes the purpose of the system as “assist[ing] all the sections within the [Civil Rights] Division in maintaining names of Division employees and their case investigation assignments, names of defendants or investigation targets, victims, witnesses or potential witnesses, or other persons or organizations as they relate to potential or actual cases.” *Id.* Routine uses described by the 2003 SORN largely encompass disclosure in the context of civil and criminal enforcement proceedings undertaken by the DOJ against individual investigation targets. *Id.* at 47611-47612. These descriptions suggest a compilation of files related to specific enforcement matters; and nothing in these descriptions, or in the catalogue of routine uses of the SORN, suggests that the system would contain a nationwide database of unredacted state VRLs wholly unconnected to any alleged violation of federal law.

The 2005 SORN does not remedy this lack of adequate notice. It merely adds a new routine use to the 2003 SORN, allowing for “the disclosure of information explaining the Department’s decision to close a criminal matter to the local community or public” under certain circumstances. 70 Fed. Reg. at 43904. Like the 2003 SORN, this SORN

does not in any way put the public on notice that the DOJ may collect and potentially disclose data from unredacted VRLs. The 2017 SORN fares no better—it only further modifies the original system of records described in the 2003 SORN to add necessary disclosure of records in response to a data breach as an additional routine use. 82 Fed. Reg. at 24151. The DOJ's demand thus violates the Privacy Act because the agency failed to publish an adequate SORN. 5 U.S.C. §552a(e)(4).

II. THE DOJ'S DEMAND VIOLATES THE E-GOVERNMENT ACT

This Court should additionally refuse to enforce the DOJ's demand because the DOJ failed to conduct a Privacy Impact Assessment (PIA) under the E-Government Act. In 2002, Congress enacted the E-Government Act, Pub. L. No. 107-347, §208, 116 Stat. 2899 (2002), to “promote better informed decisionmaking by policy makers” and “more transparent and accountable” government. 44 U.S.C. §§3601(5)(b)(7), (9). The Act requires federal agencies to conduct a PIA *before* initiating a new collection of personally identifiable information. Pub. L. No. 107-347, §208(b), 116 Stat. at 2921; *see also Electronic Priv. Info. Ctr. v. Presidential Advisory Comm'n on Election Integrity*, 878 F.3d 371, 378 (D.C. Cir. 2017) (“[Section 208] is intended to protect *individuals* ... by

requiring an agency to fully consider their privacy before collecting their personal information.”).

The DOJ does not claim that it ever carried out a PIA or intends to in the future. *See* U.S. Mem. In Opp. to Mot. to Dismiss 31, *United States v. Wisconsin Elections Commission*, No. 25-1036 (W.D. Wis. Mar. 2, 2026). The DOJ instead argues that it was not required to complete a PIA because merely gathering existing VRLs does not *itself* initiate a “new process” of information collection. *Id.* at 32. If adopted, DOJ’s narrow reading of the Act would degrade privacy rights by encouraging agencies to target existing databases to avoid completing a PIA.

Moreover, the Office of Management and Budget—which “oversees the implementation of the privacy impact assessment process,” Pub. L. No. 107-347, §208(b)(3)(A), 116 Stat. at 2921—has made it clear that “[a]gencies should commence a PIA when they begin to develop a new *or significantly modified* IT system or information collection,” Bolten, Dir., OMB, Executive Office of the President, M03-22, Memorandum for Heads of Executive Departments and Agencies, attachment A §II.C.2 (Sept. 26, 2003) (emphasis added), and that “a PIA shall be considered a living document that agencies are required to update whenever changes

to the information technology, changes to the agency's practices, or other factors alter the privacy risks," Office of Management & Budget, *OMB Circular A-130: Managing Information as a Strategic Resource* (2016), app. II at 10 (July 28, 2016).²³ So even under the DOJ's untenably narrow reading of §208, the agency would still be obligated to conduct and publish a new PIA before it could proceed with the radically expanded scope of data collection it intends.

And even if the DOJ decided to complete a PIA now, it would still be in violation of §208, which makes clear that PIAs must take place *before* collection. Pub. L. No. 107-347, §208(b), 116 Stat. at 2921. If agencies can collect personal data before completing the analysis required by §208, the requirement that agencies "assess" privacy impacts becomes meaningless. *Doe v. Office of Pers. Mgmt.*, 2025 WL 513268, at *1 (D.D.C. Feb. 17, 2025) (raising concerns that an agency's rushed, post-filing PIA was insufficient under §208). Thus, the DOJ violated the E-Government Act and can no longer remedy the violation.

²³ Available at <https://www.federalregister.gov/documents/2016/07/28/2016-17872/revision-of-omb-circular-no-a-130-managing-information-as-a-strategic-resource>.

CONCLUSION

For the foregoing reasons, this Court should affirm the district court's judgment.

Respectfully submitted,

/s/ Christopher T. Casamassima

CHRISTOPHER T. CASAMASSIMA

MAIREAD C. AHLBACH

SARA R. ORTON

WILMER CUTLER PICKERING

HALE AND DORR LLP

350 South Grand Avenue

Suite 2400

Los Angeles, CA 90071

(213) 443-5300

chris.casamassima@wilmerhale.com

mairead.ahlbach@wilmerhale.com

sara.orton@wilmerhale.com

Counsel for Amicus Curiae Electronic Privacy Information Center

August 24, 2026

CERTIFICATE OF COMPLIANCE

The brief complies with the type-volume limitations of Seventh Circuit Rules 29 because it contains 6,373 words, excluding the parts exempted by Federal Rule of Appellate Procedure 32(f). This brief complies with the typeface requirements and type-style requirements of Federal Rule of Appellate Procedure 32(a), as amended by Seventh Circuit Rule 32(b), because it has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point Century Schoolbook font.

/s/ Christopher T. Casamassima
CHRISTOPHER T. CASAMASSIMA

August 24, 2026

CERTIFICATE OF SERVICE

I hereby certify that on this 24th day of August 2026, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the Seventh Circuit using the appellate CM/ECF system. Counsel for all parties to the case are registered CM/ECF users and will be served by the appellate CM/ECF system.

/s/ Christopher T. Casamassima
CHRISTOPHER T. CASAMASSIMA