No. 23-1361

IN THE UNITED STATES COURT OF APPEALS
FOR THE FIRST CIRCUIT

PUBLIC INTEREST LEGAL FOUNDATION, INC.,

Plaintiff-Appellee,

v.

SHENNA BELLOWS, in her official capacity as the Secretary of State for the State of Maine,

Defendant-Appellant.

On Appeal from the United States District Court
for the District of Maine
No. 1:20-cv-00061-GZS
The Honorable George Z. Singal, U.S. District Court Judge

BRIEF OF THE ELECTRONIC PRIVACY INFORMATION CENTER AS *AMICUS CURIAE* IN SUPPORT OF DEFENDANT-APPELLANT AND REVERSAL

Caitriona Fitzgerald (Bar # 1208080)
John Davisson
Tom McBrien
Suzanne Bernstein
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140
fitzgerald@epic.org

Attorneys for Amicus Curiae

June 16, 2023

CORPORATE DISCLOSURE STATEMENT

Pursuant to Fed. R. App. P. 26.1, *amicus curiae* Electronic Privacy Information Center states that it has no parent corporation and that no publicly held corporation owns 10% or more of its stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Regulations

Other Authorities

INTEREST OF THE *AMICUS CURIAE*[1]

The Electronic Privacy Information Center (EPIC) is a public interest research center in Washington, D.C., that focuses public attention on emerging privacy and civil liberties issues. EPIC routinely participates as *amicus curiae* in cases concerning emerging privacy issues, including voter privacy and the right of informational privacy. *See, e.g.*, Brief of *Amici Curiae* EPIC *et al*., *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008) (No. 07-21) (opposing voter photo-ID requirements as infringing on citizens' right to cast a secret ballot); Brief of *Amicus Curiae* EPIC, *Veasey v. Abbott*, 830 F.3d 216, 225 (5th Cir. 2016) (No. 14–41127) (arguing that Texas photo identification requirements violates voter privacy); Brief of *Amicus Curiae* EPIC, *National Coalition on Black Civic Participation v. Wohl*, 2023 WL 2403012 (S.D.N.Y. Mar. 8, 2023) (No. 20-8668) (arguing that intimidating robocalls violated voter privacy); Brief of *Amicus Curiae* EPIC, *Curling v. Raffensperger*, 403 F. Supp. 3d 1311 (N.D. Ga. 2019) (No. 17-2989) (explaining that ballot secrecy and voter privacy are critical to election integrity).

[1] The parties consent to the filing of this *amicus curiae* brief. In accordance with Rule 29, the undersigned states that 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.

SUMMARY OF ARGUMENT

Voter privacy is critical to election integrity in the United States. The secret ballot and legal safeguards on voter roll information protect voters from intimidation, bribery, and harassment. The district court's conclusion that the National Voter Registration Act preempts the reasonable use and transfer restrictions in 21-A M.R.S.A. § 196-A(1)(J) is both wrong on the law and a threat to these essential privacy protections. If allowed to stand, the decision could enable any individual or organization claiming to evaluate Maine's compliance with voter list maintenance obligations to broadly expose sensitive voter information. Such unrestricted republication of personal information—including a voter's name, address, birthdate, voter participation history, and party affiliation—risks undermining the ability of voters to freely exercise the franchise. Even if section 8(i) of the NVRA were held to require disclosure of the statewide Voter File, an assertion that Defendant-Appellant has convincingly disproven, it surely does not preempt commonsense use and transfer restrictions that still permit dissemination of information for the purpose of evaluating NVRA compliance.

Not only is the district court's interpretation dangerous to the democratic process, but it is also unsupported by the text and legislative history of the NVRA. Indeed, the record indicates that Congress sought to protect voter privacy even as it required states to make certain public disclosures. Nothing in the text or legislative

history of the NVRA suggests that Congress intended to preempt state laws that establish reasonable use and transfer limitations on personally identifiable voter data. These limitations are commonplace across legal frameworks governing the use and disclosure personal data and are necessary tools to protect sensitive personal information. Maine's reasonable use and transfer limitations for voter information are a lawful and effective means of safeguarding voter privacy. The Court should decline to hold them silently preempted by the NVRA.

ARGUMENT

I. USE AND TRANSFER LIMITATIONS ON PERSONAL VOTER DATA DO NOT OBSTRUCT CONGRESS'S PURPOSE IN ENACTING THE NVRA AND ARE CRUCIAL FOR ELECTION INTEGRITY.

A. Voter privacy helps ensure that voters are willing to exercise the franchise and willing to vote for the causes and candidates of their choice.

The history of voting in the United States shows the ongoing recognition of the importance of privacy to election integrity. The right to a secret ballot evolved as a response to intimidation and coercion.

Voting was not always done in secret. During the colonial period, voters used myriad public displays to cast their votes—from raising voices to stamping feet to casting beans. *See Burson v. Freeman*, 504 U.S. 191, 201 (1992). Although most states had adopted voting by paper ballots by the early 1800s, it remained easy for interested persons to determine who was voting for whom because the

parties, which created the ballots with their candidates' names pre-marked, made the ballots large and conspicuously colored. *See id.*

A lack of privacy in voting led to widespread bribery and intimidation. Voters were sometimes threatened with economic ruin, joblessness, or violence if they voted against the will of their employer, landlord, creditor, or party benefactor. *See* Eldon Cobb Evans, *A History of the Australian Ballot System in the United States* 12–13, 22 (1917). Members of the military were subject to heightened voter coercion. Significant pressure was put on military rank-and-file to vote for specific candidates, with servicemen sometimes demoted or relieved of duty if they refused or expressed their preference for another politician. *See* Jonathan W. White, Opinion, *How Lincoln Won the Soldier Vote*, N.Y. Times (Nov. 7, 2014).[2] These issues grew after the Civil War, as Northern party bosses aimed to consolidate and maintain their political hegemony and Southern Whites engaged in a widespread campaign of violence to discourage newly freed slaves from voting or attaining political power. *See* Eldon Cobb Evans, *A History of the Australian Ballot System in the United States* 7 (1917); Ben Cady & Tom Glazer, *Voters Strike Back: Litigating Against Modern Voter Intimidation*, 39 N.Y.U. Rev. L. & Soc. Change 173, 184–85 (2015).

[2] http://opinionator.blogs.nytimes.com/2014/11/07/how-lincoln-won-the-soldier-vote/.

Maine was the first state to take a major step towards the secret ballot, and it did so to protect voters from the fear of economic and physical reprisal for voting their conscience. *See* Evans, *supra*, at 7–8; Caitriona Fitzgerald, Susannah Goodman & Pamela Smith, *The Secret Ballot at Risk: Recommendations for Protecting Democracy* (Aug. 2016).[3] In 1831, Maine required that voting take place on a white paper ballot with black ink, fully 36 years before a second state would adopt such a law. However, the requirement was not as effective as hoped because political parties, which were still in charge of printing ballots, found ways to use different shades of white for their ballots so it was still possible to tell how a voter voted. Evans, *supra*, at 7–8. So, in the early 1890s, the minority party in Maine fought for a secret ballot printed by the government. *Ballot Reform in Maine*, N.Y. Times (Mar. 31, 1891).[4] They were met with fierce resistance because voter coercion was such an important tool for gaining and retaining power. The New York Times reported at the time that "A strong lobby had been at work against the bill from the day the session began — probably the most influential that has ever been seen in Augusta." *Id.* The Times further noted:

> The Republican ascendency in Maine for years has been maintained by bribery and intimidation. It is, of course, uncertain to what extent the new system will repress bribery. Many believe that this great evil will become in a short time almost unknown. In Maine the seller is not paid

[3] https://secretballotatrisk.org.
[4] https://www.nytimes.com/1891/03/31/archives/ballot-reform-in-maine-a-bitter-fight-that-was-gloriously-won-the.html.

> until he has voted. A man who sells cannot be trusted, and under the new system he will have no way of proving that he has delivered his goods. The Republican bosses take a very gloomy view of the situation. When asked if it was not possible that the next Legislature would repeal the law, a well-known Republican leader replied: "The Republicans will not be in control the next Legislature!"

Id. The secret ballot and other voter privacy measures have since protected voters from harassment as a result of their vote.

But the unrestricted republication of voter registration information online is a dangerous threat to voter privacy. The publication of a voter's party affiliation and voting history online is particularly harmful as it is highly indicative of the individuals the voters cast their ballots for. Since the 2004 election, Democratic and Republican voters have consistently voted for their party's presidential candidate over 89% of the time. Am. Nat'l Election Studies, *The Anes Guide to Public Opinion And Electoral Behavior: Presidential Vote: 2 Major Parties*.[5] And indeed, the district court's determination that the NVRA preempts the reasonable use and transfer restrictions in 21-A M.R.S.A. § 196-A(1)(J)—though not Exception (J) as a whole—would enable individuals and organizations assertedly "evaluating the State's compliance with its voter list maintenance obligations" to obtain and publish voters' party affiliations and voting history. 21-A M.R.S.A. § 196-A(1)(B); *see also* ECF No. 80 at 7 (noting that enrollment status includes

[5] https://electionstudies.org/data-tools/anes-guide/anes-guide.html?chart=vote_for_president_2_parties.

political party affiliation). Allowing organizations to widely publish voters' party affiliation and voting history is tantamount to disclosing who they voted for.

The harms of this erosion of voter privacy are real. While ballot secrecy protects individuals from the worst consequences of employer-employee political coercion, attempts to coerce employees into voting for their employer's favored candidates are commonplace. *See* Lee Fang & David Dayen, *How Companies Pressure Workers to Vote for Corporate Interests Over Their Own*, The Intercept (Nov. 6, 2018);[6] Alexander Hertel-Fernandez, *Employer Political Coercion: A Growing Threat*, American Prospect (Nov. 23, 2015).[7] Thanks to the secret ballot, employers cannot lawfully go so far as to verify how an employee actually voted. But an erosion of voter privacy via the widespread publication of political party affiliation and voter history could further empower employers to threaten and pressure employees to vote in line with the employers' interests, or even change party affiliation, preventing the employee from voting in their desired primary in some states. *See* 21-A M.R.S.A. § 441(2) ("voters enrolled in a political party may only vote in that party's presidential primary election"). This would threaten the freedom and fairness of our democracy.

[6] https://theintercept.com/2018/11/06/midterms-2018-voting-coercion-bosses-employees/.
[7] http://prospect.org/article/employer-political-coercion-growing-threat.

B. Nothing in the text or legislative history of the NVRA suggests that Congress intended to preempt use and transfer limitations on personal voter data.

The text and legislative history of the NVRA evince no Congressional intent to prohibit states from placing reasonable use and transfer limitations on personal voter data made available for public inspection. The district court concluded that the NVRA preempts Exception J because (on its interpretation) Congress intended for voter roll information to be publicly disclosed. ECF No. 87 at 12. But even if that were a correct reading of Congress's intent, the district court's holding overlooks a key point: reasonable use restrictions are entirely compatible with ensuring the public availability of records pursuant to 52 U.S.C. § 20507(i)(1). *See* Part II, *infra*. Indeed, were states required to make voter roll information available for public inspection under the NVRA, use limitations would enable states to comply with that mandate while still mitigating the "privacy concerns related to the disclosure of sensitive information[.]" ECF No. 87 at 15. Had Congress meant to strip states of their authority to regulate the use and transfer of voter roll information, that purpose would presumably be reflected somewhere in the voluminous legislative history of the NVRA. Yet the record yields no indication that Congress intended such a result. This Court should decline to interpret Congress's silence as hostility toward the use limitations established by the Maine

legislature, let alone as a basis to declare the limitations of Exception J preempted by the NVRA.

Though the legislative record pertaining to 52 U.S.C. § 20507(i)(1) is scant, two relevant lessons may be drawn from the text and history of the NVRA. First, it is clear that Congress understood the central role voter privacy plays in election integrity and that it meant for the NVRA to enhance—not diminish—privacy protections. For example, section 7 of the NVRA imposed a new requirement that voter registration agencies provide voters with a form stating as follows:

> If you believe that someone has interfered with your right to register or to decline to register to vote, *your right to privacy in deciding whether to register or in applying to register to vote*, or your right to choose your own political party or other political preference, you may file a complaint with [the appropriate official in the relevant jurisdiction].

52 U.S.C. § 20506(a)(6)(B)(v) (emphasis added). This provision was added to the NVRA "to ensure that in enabling people to register to vote we do not open them up to coercion, pressure, or invasion of their privacy, in the offices where they have gone basically for help." 139 Cong. Rec. S2988-01 (daily ed. Mar. 17, 1993), 1993 WL 75574 (statement of Sen. David Durenberger); *see also* 139 Cong. Rec. S5746-03 (daily ed. May 11, 1993), 1993 WL 151575 ("Under my compromise, applicants in State agencies would be provided with a form that advises them . . . that they have the right to privacy or assistance while they register[.]").

Further, in the same provision that requires states to make records concerning voter roll maintenance available for public inspection, Congress was careful to exempt from disclosure "records relat[ing] 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. § 20507(i)(1). True, this disclosure exemption does not apply to the wider universe of voter roll data in dispute in this case, but it does illustrate that Congress was mindful of the risks imposed by the disclosure of voters' personally identifiable information. It would be a curious thing for Congress to expressly recognize the necessity of voter privacy protections one minute while silently overriding states' authority to impose even the most basic use and transfer limitations the next. Yet that is the tenuous conclusion compelled by Plaintiff-Appellee's reading of the NVRA.

Second, it is apparent from the legislative history of the NVRA that Congress was simply not concerned with regulating states' authority to impose use limitations on voter roll data. The record is devoid of any suggestion that, in requiring "public inspection" of records pertaining to voter roll maintenance, Congress also meant to upend the ability of states to protect the privacy of registered voters through reasonable use restrictions. 52 U.S.C. § 20507(i)(1). It is particularly implausible that Congress meant to protect the right of third parties to expose personally identifiable voter information online to "the general public," the

use prohibited by 21-A M.R.S.A. § 196-A(1)(J)(2). Leaving voters vulnerable to such exposure—indeed, rendering states powerless to stop it—would be directly at odds with the NVRA's stated purposes of "enhanc[ing] the participation of eligible citizens as voters" and "protect[ing] the integrity of the electoral process." 52 U.S.C. § 20501(b). *See* Part I.A, *supra*.

The district court rightly noted that "the purpose of Congress is the ultimate touchstone in every pre-emption case." *Wyeth v. Levine*, 555 U.S. 555, 565 (2009). Yet here, neither "the statutory language" of 52 U.S.C. § 20507(i)(1) nor the "purpose, history, and the surrounding statutory scheme" indicate that Congress had as its purpose the preemption of reasonable use limitations on voter roll information. *Massachusetts Delivery Ass'n v. Coakley*, 769 F.3d 11, 17 (1st Cir. 2014). Mindful that Congress does not "hide elephants in mouseholes," *Whitman v. Am. Trucking Ass'ns, Inc.*, 531 U.S. 457, 468 (2001), the Court should reject a reading of § 20507(i)(1) that rests on illusory claims of Congressional intent.

C. Voter file use and transfer restrictions are common and non-controversial across the United States.

The district court's holding that section 8(i) of the NVRA preempts the use and transfer restrictions of Exemption J interprets the NVRA's preemption too broadly. If adopted widely, the court's interpretation would invalidate dozens of important state election privacy laws that protect voters. The district court held that the NVRA preempts Exception J's use and transfer restrictions because the NVRA

"plainly requires disclosure of completed voter registration applications," ECF No. 87 at 16 (quoting *Project Vote/Voting for Am., Inc. v. Long*, 682 F.3d 331, 339 (4th Cir. 2012)), which include, at minimum, a voter's full name, residential address, mailing address, and birth date, *see* ECF No. 87 at 16 n.22. This interpretation clashes with transfer and use limitations on statewide voter registries that are common across the United States. States routinely redact sensitive categories of data from registries, restrict who can request the registries, impose limitations on the ways in which people can use information they have received from voter registries, and permit citizens to remove their records from public voter registries for safety and privacy reasons. All of these commonsense measures would be preempted under the district court's interpretation of the NVRA.

The district court's interpretation of section 8(i), if widely adopted, would preempt almost every state's use of privacy safeguards known as "Address Confidentiality Programs" (ACPs). These laws protect victims of stalking, domestic violence, sexual assault, human trafficking, and other crimes by providing them with a false address to be used for official government business so that members of the public do not learn their real addresses. *See* Victim Connect Resource Center, *Address Confidentiality* (2023).[8] In almost every state, a person enrolled in an ACP program will have their personal information removed from

[8] https://victimconnect.org/learn/address-confidentiality/.

any statewide voter registry shared with the public. *See* National Conference of State Legislatures, *Access to and Use of Voter Registration Lists* (2023).[9] In Massachusetts, for example, any participant in an ACP program will have their name and address removed from any voter registration list provided to the public. Mass. Gen. Laws ch. 51, §§ 4(d), 44 (2023). Many states also extend the same protections to law enforcement officers, abortion providers, judges, prosecutors, legislators, public defenders, and anybody else who demonstrates a substantial need for privacy. *See, e.g.*, Ala. Code §§ 17-4-33(b)(1)(a)–(c) (2022); Cal. Elec. Code §§ 2166(a)–(b), 2166.5(a)–(b) (West 2022); Conn. Gen. Stat. § 54-240(g) (2022).

Recently, many state and federal statutes have sought to protect judges by allowing them to remove or redact their personal information from public records in ways that the district court's opinion would prohibit. The U.S. Marshals Service has reported thousands of threats or inappropriate communications against the judiciary per year. *Judges Targeted Fast Facts*, CNN (May 10, 2023).[10] In response to these threats and actual tragedies involving judges and their families, the federal government and state governments have considered and enacted legislation protecting the confidentiality of judges' personal information. *See, e.g.*,

[9] https://www.ncsl.org/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.
[10] https://www.cnn.com/2013/11/04/us/judges-targeted-fast-facts/index.html.

U.S. Courts, *Congress Passes the Daniel Anderl Judicial Security and Privacy Act* (Dec. 16, 2022) (describing the passage of a federal judicial privacy law);[11] State of New Jersey, *Governor Murphy Signs "Daniel's Law"* (Nov. 20, 2020) (describing the passage of a state judicial privacy law).[12] If section 8(i) were to preempt state and federal statutes that impair the dissemination of information contained in the Voter File, these important protections would disappear.

Many states also redact sensitive information before disclosing voter registration lists, a practice that would be impermissible if section 8(i) preempted state voter privacy laws. Many states redact some of the categories that the district court held as necessary to disclose. For example, states such as Hawaii keep voters' birth dates confidential, among other sensitive categories. Haw. Code R. § 3-177-160(c) (LexisNexis 2023) (prohibiting public disclosure of "the voter's full or last four digits of the social security number, driver, license number, state identification card number, electronic mail address, telephone number, or date of birth"). Other states keep voters' gender, telephone number, and voting history confidential. *See, e.g.*, Ind. Code § 3-7-26.4-8(c) (2021). There are valid reasons to apply heightened privacy safeguards to sensitive information despite the benefits of transparency, as courts have recognized when holding that the NVRA's

[11] https://www.uscourts.gov/news/2022/12/16/congress-passes-daniel-anderl-judicial-security-and-privacy-act.
[12] https://www.nj.gov/governor/news/news/562020/20201120b.shtml.

preemption has limits. *See, e.g., Project Vote/Voting for Am., Inc. v. Long*, 682 F.3d 331, 339 (4th Cir. 2012) (recognizing that social security numbers should be redacted to comply with the Privacy Act); *Pub. Int. Legal Found., Inc.. v. Boockvar*, 431 F. Supp. 3d 553, 563 (M.D. Pa. 2019) (holding that the privacy protections of the Driver's Privacy Protection Act are not preempted by the NVRA); *Pub. Int. Legal Found., Inc. v. Dahlstrom*, No. 1:22-CV-00001-SLG, 2023 WL 3498044, at *10 (D. Alaska May 17, 2023) (ruling that the NVRA did not preempt the redaction of sensitive information protected by the Bipartisan Budget Act of 2013).

An overly broad interpretation of section 8(i) preemption would also prohibit important use and transfer limitations that other states have placed on people who access statewide voter rolls. For example, almost every state prohibits the public to use or transfer the voter list for commercial purposes. *See* National Conference of State Legislatures, *Access to and Use of Voter Registration Lists* (2023);[13] 10 ILCS 5/4 §8 (2022); Iowa Code § 48A.39 (2022). California prohibits using its statewide voter list for a host of purposes including harassment, advertising, or reproducing the list on the internet. Cal. Elec. Code § 2194 (West 2019). Hawaii permits the public to view a voter's name, district and precinct

[13] https://www.ncsl.org/elections-and-campaigns/access-to-and-use-of-voter-registration-lists.

designation, and voter status for any purpose but restricts the use of all other information to election or governmental purposes. Haw. Rev. Stat. § 11-97 (2022). South Dakota only allows dissemination of statewide voter roll information for election purposes and prohibits providing unrestricted access to the information on the internet. S.D. Codified Laws § 12-4-41 (2022). In Virginia, members of the public who receive the list must agree that they are only using the list to promote voter participation and registration by means of a communication or mailing without intimidation or pressure exerted on the recipient. Va. Code Ann. § 24.2-406 (2022). These various restrictions on the ways Voter File data may be used illustrate the widespread understanding that election integrity and voter privacy protection are complementary, not conflicting.

II. ACCESS, USE, AND TRANSFER LIMITATIONS FOR PERSONAL DATA ARE COMMON AND NECESSSARY TOOLS TO PROTECT PRIVACY IN OTHER SIMILARLY SENSITIVE CONTEXTS.

Access, use, and transfer limitations are common across statutory and regulatory frameworks that shape government data management of personal information. These limitations are necessary to protect the confidentiality of personal information. Disclosure policies for government information are context-specific and can be "based on the type of information released, the agency releasing it, and the mechanism of release." Micah Altman *et al.*, *Towards A Modern Approach to Privacy-Aware Government Data Releases*, 30 Berkeley

Tech. L. J. 1967, 1972 (2015). Access often does not imply unrestricted use or the ability to transfer data. Because disclosure mechanisms and conditions are directly related to the sensitivity of the information, they are crafted to protect individual privacy by balancing the interests for and against disclosure. *Id*. at 2009.

Federal, state, and local governments necessarily keep databases of records on individual people in order to function and provide services. In the 1960s and 70s, advancing computer technology began to enable agencies to cross-reference and identify individuals' personal data, sounding alarm bells for citizens and legislators alike about potential harms and abuse from compiling sensitive information. As a result, the landmark report *Records, Computers and the Rights of Citizens* was issued in 1973 by an advisory committee of the Department of Health Education and Welfare. Advisory Comm. on Automated Pers. Data Sys., U.S. Dep't of Health, Educ., & Welfare, *Records, Computers and the Rights of Citizens* (1973).[14] The report recommended the adoption of the Fair Information Practices (FIPs). *Id*. at 41. One practice focused uniquely on access, use, and transfer limitations of data: "Any organization creating, maintaining, using, or disseminating records of identifiable personal data must assure the reliability of the data for their intended use and must take reasonable precautions to prevent misuse of the data." *Id*. Various iterations of the FIPs and the practice of limiting use and

[14] https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

access have become central to disclosure policies and "have informed federal law and the laws of many U.S. states and foreign nations." Kevin Herms, *How to Respect Privacy: A Constellation of Principles*, Federal Privacy Council (last visited June 2, 2023).[15]

The year after the HEW Report, Congress passed the Privacy Act of 1974. The Privacy Act places use, transfer, and access limitations on how agencies can share an individual's data with third parties and other agencies, among other privacy safeguards. Privacy Act of 1974, 5 U.S.C. § 552a. The Privacy Act's congressional findings section states that "it is necessary and proper for the Congress to regulate the collection, maintenance, use, and dissemination of information by such agencies." *Id.* § (a)(5).[16] One of the Act's chief purposes was to safeguard personal privacy by requiring agencies to implement access and use limitations on personal data—for example, by mandating that agencies "collect, maintain, use, or disseminate any record of identifiable personal information in a manner that assures that such action is necessary and lawful purpose […] and that adequate safeguards are provided to prevent misuse of such information." *Id.* § (b)(4).[17] Under the Privacy Act, certain personal information cannot be disclosed

[15] https://www.fpc.gov/data-privacy-day/respect-privacy/.
[16] https://archive.epic.org/foia/21/appendixb.html.
[17] https://archive.epic.org/foia/21/appendixb.html.

without written consent. The twelve exceptions to that disclosure prohibition are largely dictated by the nature and purpose of the intended use. 5 U.S.C. § 552a(b).

The Privacy Act has influenced other statutes and regulations that have shaped government data management for decades. Use, transfer, and access limitations have become commonplace. *See* Data.gov, *Federal Data Strategy: Data Governance Playbook* 5 (July 2020) (strong federal data strategy includes data management policies for the integrity and use of data and information).[18] For example, the Federal Election Campaign Act (FECA) incorporates use and transfer limitations. *See* Federal Election Campaign Act, Pub. L. No. 92-225 § 308(a)(4), 86 Stat. 3, 17 (1972), *as amended*. FECA requires the Federal Election Commission to make campaign finance disclosure reports available for the public within 48 hours of receipt. *Id.* § 304(a). To protect the privacy of individual contributors, FECA prohibits the sale or use of any information about those donors—including their names and addresses—for commercial purposes or for soliciting contributions or charitable donations. *Id.* § 308(a)(4).

Another example is the Confidential Information Protection and Statistical Efficiency Act (CIPSEA), which was enacted in 2002 to regulate information technology practices across government agencies. Confidential Information Protection and Statistical Efficiency Act, Pub. L. No. 107-347, 116 Stat. 2962

[18] https://resources.data.gov/assets/documents/fds-data-governance-playbook.pdf.

(2002). A core objective of CIPSEA is to safeguard the privacy of individually identifiable information by controlling the use, transfer, and access of such information for statistical purposes. Other examples of use, transfer, and access limitations apply to individual agencies. The Internal Revenue Service is bound by disclosure laws that generally prohibit the release of tax return information with limited exceptions for specific groups and uses. *See* 26 U.S.C. § 6103.

Where government agencies collect, maintain, and use vast amounts of sensitive personal information, there are typically heightened disclosure safeguards. Public access to and disclosure of such information is typically limited to anonymized or aggregate data sets. For example, federal law establishes strict confidentiality and privacy requirements for personally identifiable information collected and used by the U.S. Census Bureau. 13 U.S.C. § 9 (2023). There are similarly strict safeguards in place for reports on mortgage activity published pursuant to the Home Mortgage Disclosure Act (HDMA). Home Mortgage Disclosure Act of 1975, Pub. L. No. 94-200, 89 Stat. 1125. Although there are not "direct personal identifiers" in the system, access to the HMDA Data Repository System is still restricted to certain authorized users to prevent indirect identification of borrowers. Federal Reserve, *Privacy Impact Assessment of the HMDA Repository System* 8 (2022).[19]

[19] https://www.federalreserve.gov/files/pia_hmda.pdf.

Use, transfer, and access limitations for personal data are also widely found in or derived from statutes regulating the private sector. The Federal Trade Commission has brought enforcement actions under its Section 5 authority against businesses for failing to impose adequate use, transfer, and access limitations.[20] *See generally* Fed. Trade Comm'n, *Privacy and Security Enforcement* (last visited June 2, 2023) (listing privacy and data security enforcement actions). Other sectoral privacy laws like the Gramm-Leach-Bliley Act, Family Educational Rights and Privacy Act, Children's Online Privacy Protection Act, and the Health Insurance Portability and Accountability Act regulate how entities use, collect, retain and transfer personal data. *See* Thorin Klosowski, *The State of US Consumer Data Privacy Laws in the US (and Why It Matters)*, N.Y. Times (Sept. 6, 2021) (survey of sectoral privacy laws);[21] *see also* Caitriona Fitzgerald & Suzy Bernstein, EPIC, *Full of Holes: Federal Law Leaves Americans' Personal Data Exposed* (Apr. 27, 2013).[22]

Use, access, and transfer limitations are commonly employed to balance information privacy and public disclosure based on the sensitivity of the data involved. In other words: a requirement for government to make certain

[20] https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.
[21] https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/.
[22] https://epic.org/full-of-holes-federal-law-leaves-americans-personal-data-exposed/.

information available for inspection does not automatically foreclose limits on the use or transfer of such information. And while Congress established certain disclosure obligations in the NVRA, it was silent on use, access, and transfer limitations. Given the ubiquity of such privacy safeguards in the management of personal data, Congress would not have stripped states of their power to impose reasonable use and transfer restrictions with nary a mention in the text or legislative history of the NVRA. The use and transfer restrictions on voter information in 21-A M.R.S.A. § 196-A(1)(J) do not conflict with the NVRA and are aligned with common government data management practices concerning personally identifiable information.

CONCLUSION

For the foregoing reasons, *amicus* respectfully urges the Court to reverse the district court's grant of summary judgment in favor of Plaintiff-Appellee and remand the case with instructions to enter summary judgment for Defendant-Appellant.

Date: June 16, 2023

/s/ Caitriona Fitzgerald
Caitriona Fitzgerald
John Davisson
Tom McBrien
Suzanne Bernstein
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center

CERTIFICATE OF COMPLIANCE

I am the attorney or self-represented party.

1. This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(4) because this brief contains 4793 words, excluding the parts of the brief exempted by Fed. R. App. P. 32(f); and

2. This brief complies with the typeface requirements of Fed. R. App. P. 32(a)(5) and the type-style requirements of Fed. R. App. P. 32(a)(6) because this brief has been prepared in a proportionally spaced typeface using Microsoft Word in 14-point font in Times New Roman font.

Signature: *<u>/s/ Caitriona Fitzgerald</u>* **Date:** June 16, 2023

CERTIFICATE OF SERVICE

I certify that on June 16, 2023, this brief was e-filed through the CM/ECF System of the U.S. Court of Appeals for the First Circuit. I certify that all participants in the case are registered CM/ECF users and that service will be accomplished by the CM/ECF system.

Date: June 16, 2023

/s/ Caitriona Fitzgerald

Caitriona Fitzgerald (Bar # 1208080)
John Davisson
Tom McBrien
Suzanne Bernstein
ELECTRONIC PRIVACY
INFORMATION CENTER
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

Attorneys for Amicus Curiae
Electronic Privacy Information Center