

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

VOTER REFERENCE FOUNDATION LLC,
PLAINTIFF-APPELLANT,

v.

ALBERT SCHMIDT, IN HIS OFFICIAL CAPACITY AS
SECRETARY OF THE COMMONWEALTH OF PENNSYLVANIA,

DEFENDANT-APPELLEE.

On Appeal from the Order of the United States District Court for the
Middle District of Pennsylvania, Case No. 1:24-CV-00294

**BRIEF OF *AMICUS CURIAE* ELECTRONIC PRIVACY
INFORMATION CENTER (EPIC) IN SUPPORT OF APPELLEE**

Alan Butler
Counsel of Record
Tom McBrien
Abigail Kunkler
Kabbas Azhar
Electronic Privacy Information Center
1519 New Hampshire Ave. NW
Washington, DC 20036
(202) 483-1140

September 23, 2026

CORPORATE DISCLOSURE STATEMENT

Pursuant to Federal Rule of Appellate Procedure 26.1 and 29(c), *amicus curiae* Electronic Privacy Information Center (“EPIC”) certifies that it is a District of Columbia corporation with no parent corporation. No publicly held company owns 10% or more of EPIC stock.

TABLE OF CONTENTS

TABLE OF AUTHORITIES	iii
INTEREST OF THE AMICUS CURIAE	1
SUMMARY OF THE ARGUMENT	1
ARGUMENT	3
I. Access, use, and transfer limitations for personal data are common and necessary tools to protect privacy in other similarly sensitive contexts.....	3
II. The First Amendment and information privacy rights work together to secure the fundamental right to vote and bolster democratic participation.....	12
III. The Internet Sharing Ban protects voter privacy without restricting speech.	17
CONCLUSION	27

TABLE OF AUTHORITIES

CASES

<i>Buckley v. Am. Const. L. Found.</i> , 525 U.S. 182 (1999).....	13
<i>Burson v. Freeman</i> , 504 U.S. 191 (1992).....	14, 17
<i>Cohen v. Cowles Media Co.</i> , 501 U.S. 663 (1991).....	24
<i>Dahlstrom v. Sun-Times Media, LLC</i> , 777 F.3d 937 (7th Cir. 2015)	8
<i>Federal Election Commission v. Political Contributions Data, Inc.</i> , 943 F.2d 190 (2d Cir. 1991)	7
<i>Los Angeles Police Dep’t v. United Reporting Publ’g Corp.</i> , 528 U.S. 32 (1999) (Ginsburg, J., concurring)	24
<i>Los Angeles Police Dep’t v. United Reporting Publ’g Corp.</i> , 528 U.S. 32 (1999).....	10
<i>McIntyre v. Ohio</i> , 514 US 334 (1995).....	17
<i>Mills v. Alabama</i> , 384 U.S. 214 (1966).....	13
<i>Sorrell v. IMS Health, Inc.</i> , 564 U.S. 552 (2011).....	24
<i>Travis v. Reno</i> , 163 F.3d 1000 (7th Cir. 1998)	8
<i>United States v. Schmidt</i> , 835 F. Supp. 3d 697 (W.D. Pa. 2026).....	16
<i>United States v. Weber</i> , 816 F. Supp. 3d 1168 (C.D. Cal. 2026)	16, 17
<i>Whiteland Woods, L.P v. Twp. of W. Whiteland</i> , 193 F.3d 177 (3d Cir. 1999)	23, 25
<i>Whitney v. California</i> , 274 U.S. 357 (1927) (Brandeis, J., concurring)	13
<i>Yick Wo v. Hopkins</i> , 118 U.S. 356 (1886).....	18

STATUTES

25 Pa. C.S.A. § 1222(a).....	3
25 Pa. C.S.A. § 1404	3
26 U.S.C. § 6103	11
National Voter Registration Act of 1993	
52 U.S.C. § 20507.....	2
Cal. Gov't Code § 7923.620	10
Confidential Information Protection and Statistical Efficiency Act, Pub. L. No. 107-347, 116 Stat. 2962 (2002).....	10
Driver's Privacy Protection Act	
18 U.S.C. § 2721(a)	8
18 U.S.C. § 2721(c)	8
18 U.S.C. §§ 2722–24.....	8
Federal Election Campaign Act, Pub. L. No. 92-225, 86 Stat. 3 (1972).....	7
Freedom of Information Act	
5 U.S.C. § 552.....	9
Help America Vote Act	
Pub. L. 107-252, 116 Stat. 1666 (2002).....	2
Idaho Code § 74-120(1)	11
K.S.A. 45-220(c)(2)(A)–(B).....	11
Md. Code Ann. Gen. Prov § 4-308(b).....	11
Md. Code Ann. Gen. Prov. § 4-312(b)(2)	11
Md. Code Ann. Gen. Prov. § 4-315(b).....	11
Privacy Act of 1974, 5 U.S.C. § 552a	6

OTHER AUTHORITIES

Advisory Comm. on Automated Pers. Data Sys., U.S. Dep't of Health, Educ., & Welfare, <i>Records, Computers and the Rights of Citizens</i> (1973).....	5
Alexander Hertel-Fernandez, <i>Employer Political Coercion: A Growing Threat</i> , American Prospect (Nov. 23, 2015).....	19
Alfred Ng, <i>Some States Are Fighting to Protect Voters from Doxxing. They're Losing</i> , Politico (Mar. 17, 2024)	21
Alice Clapman & Andrew Garber, <i>A New Antidemocracy Tool</i> , Brennan Center for Justice (Sep. 5, 2023).....	22

Am. Nat'l Election Studies, <i>The Anes Guide to Public Opinion and Electoral Behavior: Presidential Vote: 2 Major Parties</i>	19
Amy Rolph, <i>Voting Can Be Dangerous for Domestic Violence Survivors in Washington State</i> , KUOW (Oct. 9, 2018)	21
Ben Cady & Tom Glazer, <i>Voters Strike Back: Litigating Against Modern Voter Intimidation</i> , 39 N.Y.U. Rev. L. & Soc. Change 173 (2015)	14, 15
Caitriona Fitzgerald & Suzy Bernstein, EPIC, <i>Full of Holes: Federal Law Leaves Americans' Personal Data Exposed</i> (Apr. 27, 2013)	12
Caitriona Fitzgerald <i>et al.</i> , <i>The Secret Ballot at Risk: Recommendations for Protecting Democracy</i> (2016).....	14
Commonwealth of Pennsylvania, <i>Types of Elections</i>	20
Commonwealth of Pennsylvania, <i>Voting & Election Statistics</i>	25
Danielle Root, <i>Obstacles to Voting for Survivors of Intimate Partner Violence</i> , Center for American Program (Nov. 1, 2018)	20
Data.gov, <i>Federal Data Strategy: Data Governance Playbook</i> (July 2020)	7
David Gilbert, <i>ICE Plans to Pay \$5 Million to Create National Voting Database</i> , Wired (Sept. 2, 2026)	17
Electronic Privacy Information Center, <i>The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record</i>	8
Federal Trade Commission, <i>Privacy and Security Enforcement</i>	11
Ira S. Rubenstein, <i>Voter Privacy in the Age of Big Data</i> , 2014 Wisc. L. Rev. 861	14, 15, 16
Jack Balkin, <i>Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society</i> , 79 N.Y.U. L. Rev. 1 (2004)	14
Jack M. Balkin, <i>Technology and Constitutional Rot</i> (2026).....	17
Julie E. Cohen, <i>What Privacy Is For</i> , 126 Harv. L. Rev. 1904 (2013)	14
Kaylie Martinez-Ochoa <i>et al.</i> , Brennan Center for Justice, <i>Tracker of Justice Department Requests for Voter Information</i>	16
Kevin Herms, <i>How to Respect Privacy: A Constellation of Principles</i> , Federal Privacy Council.....	6
Lee Fang & David Dayen, <i>How Companies Pressure Workers to Vote for Corporate Interests Over Their Own</i> , The Intercept (Nov. 6, 2018).....	19
Micah Altman <i>et al.</i> , <i>Towards A Modern Approach to Privacy-Aware Government Data Releases</i> , 30 Berkeley Tech. L. J. 1967 (2015).....	4

Morgan Lee & Anthony Izaguirre, <i>Voter Rolls Are Becoming the New Battleground over Secure Elections as Amateur Sleuths Hunt Fraud</i> , Associated Press (Oct. 6, 2023)	22
Neil M. Richards, <i>Reconciling Data Privacy and The First Amendment</i> , 52 UCLA L. Rev. 1149 (2005)	24
Noor Al-Sibai, <i>If You Voted, Now Your Address and Party Registration Are Publicly Available Online</i> , Futurism (Nov. 8, 2024)	21
Pew Research Center, <i>Why Are Millions of Citizens Not Registered to Vote?</i> (June 21, 2017)	22
Scottie Andrew, <i>For Abuse Victims, Registering to Vote Brings a Dangerous Tradeoff</i> , CNN (Oct. 27, 2020)	20
Thorin Klosowski, <i>The State of US Consumer Data Privacy Laws in the US (and Why It Matters)</i> , N.Y. Times (Sept. 6, 2021)	12
U.S. Dep’t of Justice, Office of Information Policy, <i>OIP Guidance: The Interface Between the FOIA and Privacy Act</i>	9, 10
Xiaofeng Liu et al, <i>Fingerprinting Web Browser for Tracing Anonymous Web Attackers</i> , 2026 IEEE First International Conference on Data Science in Cyberspace (2016)	23

INTEREST OF THE AMICUS CURIAE¹

The Electronic Privacy Information Center (“EPIC”) is a public interest research center in Washington, D.C., established in 1994 to secure the fundamental right to privacy in the digital age for all people. EPIC routinely participates as *amicus curiae* in cases concerning voter privacy protections. *See, e.g.*, Brief of *Amici Curiae* EPIC *et al.*, *Crawford v. Marion County Election Board*, 128 S. Ct. 1610 (2008) (opposing voter photo-ID requirements on basis of citizens’ right to cast a secret ballot); Brief of *Amicus Curiae* EPIC, *PILF v. Bellows*, 92 F.4th 36 (1st Cir. 2023) (arguing that Maine’s voter privacy protections were consistent with federal law). EPIC also regularly participates as *amicus curiae* in cases concerning the First Amendment implications of data protection regulations. *See* EPIC, *The First Amendment* (2024).²

SUMMARY OF THE ARGUMENT

The digitization of government records concerning citizens creates significant political, constitutional, and moral risks that have been the subject of countless hearings, investigations, debates, and reports over the last 60 years. The

¹ Voter Reference Foundation LLC did not consent to the filing of this amicus brief. In accordance with Rule 29(A)(4)(E), the undersigned states that no monetary contributions were made for the preparation or submission of this brief. This brief was not authored, in whole or in part, by counsel for a party.

² <https://epic.org/issues/platform-accountability-governance/the-first-amendment-and-platform-regulation/>.

response to these risks has been the enactment of laws and regulations (along with related executive actions) to protect privacy while also ensuring the integrity and transparency of government records. Not all of these laws and regulations are perfect, but they all serve an important purpose in protecting the rights of citizens against the numerous and evolving risks to their personal information. Many operate by placing access, use, and transfer restrictions on personal information held in government control, which ensures government transparency without needlessly endangering individuals' privacy rights.

The National Voter Registration Act of 1993 (“NVRA”), 52 U.S.C. § 20507, includes a public disclosure provision that requires states to make certain voter records available to the public for inspection. *Id.* § 20507(i). A decade after the NVRA was passed, Congress enacted the Help America Vote Act (“HAVA”), Pub. L. 107-252, 116 Stat. 1666 (2002), to establish standards for computerized voter registration systems. The goal of both of these laws was to ensure the accuracy and integrity of the voter registration process and to increase participation in federal elections by eligible citizens. Notably, neither of these laws obligated states to provide unfettered access to voter data to anyone who requested it.

Pennsylvania, like other states, created an electronic database to maintain voter records pursuant to HAVA. *See* 25 Pa. C.S.A. § 1222(a). This system is called the Statewide Uniform Registry of Electors (or “SURE”), and the data in

that system is used to generate “public information lists” that can be accessed for purposes related to “elections, political activities, or law enforcement” pursuant to 25 Pa. C.S.A. § 1404 and the implementing regulations 4 Pa. Code. § 183.14. One of the rules included in the implementing regulations of the public information lists is the Internet Sharing Ban, a simple rule that states “the list may not be published on the internet.” *Id.* § 183.14(k). The Internet Sharing Ban is an example of an access, use, and disclosure restriction.

Privacy laws and rules restricting access to government records at the state and federal level have been in force and upheld under a range of legal challenges for decades. And that is not surprising because these rules are in harmony with the individual rights enshrined in the Constitution including the right to freedom of speech, the right to privacy, and the right to vote. The Court should reject Plaintiff-Appellant’s overbroad argument that a commonplace privacy protection for individual data represents government censorship.

ARGUMENT

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

The Internet Sharing Ban is an access, use, and transfer restriction, which is a privacy-protecting rule common across a wide variety of statutory and regulatory

frameworks. These disclosure policies facilitate information-sharing by placing conditions that prevent recipients from misusing the information.

When government actors decide to share individuals' personal information with the public, they often turn to these conditions to protect the privacy and safety of individuals whose information is disclosed. 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). The government's decision to grant access to data often does not imply a right to unrestricted use or transfer of that 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. While it is possible to conceive of an access, use, and transfer limitation that violates the First Amendment, the Internet Sharing Ban is not such a limitation. *See* Section III, *infra*.

Federal, state, and local governments necessarily keep databases of records on individual people in order to carry out their essential functions and serve the needs of their citizens. In the 1960s and 70s, advancing computer technologies enabled agencies to cross-reference and identify individuals' personal data, raising

alarm bells for citizens and legislators alike about the risk of abuses 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).³ The report recommended the adoption of the Fair Information Practices (“FIPs”) to govern such systems. *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 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).⁴

The year after the HEW Report, Congress passed the Privacy Act of 1974. The Privacy Act places use, transfer, and access limitations on how federal agencies can share an individual’s data with third parties and other agencies,

³ <https://www.justice.gov/opcl/docs/rec-com-rights.pdf>.

⁴ <https://www.fpc.gov/data-privacy-day/respect-privacy/>.

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).⁵ 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).⁶ Under the Privacy Act, certain personal information cannot be disclosed 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).⁷ For example, the Federal Election Campaign Act (“FECA”) incorporates use and

⁵ <https://archive.epic.org/foia/21/appendixb.html>.

⁶ <https://archive.epic.org/foia/21/appendixb.html>.

⁷ <https://resources.data.gov/assets/documents/fds-data-governance-playbook.pdf>.

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 imposes a use limitation on recipients of this information, prohibiting the sale of any personal information about the donors or the use of the information for soliciting donations or any other commercial purpose. *Id.* § 308(a)(4). In a First Amendment challenge to FECA, the Second Circuit found its privacy-based use restrictions to be fully consonant with the First Amendment, *see Federal Election Commission v. Political Contributions Data, Inc.*, 943 F.2d 190, 197–98 (2d Cir. 1991), despite the fact that soliciting business is generally considered protected speech.

The Driver’s Privacy Protection Act (“DPPA”) imposes similar disclosure and use restrictions on motor vehicle records to protect drivers’ privacy. Congress passed the DPPA in response to a series of murders, robberies, and other crimes facilitated by criminals’ obtaining victims’ motor vehicle records. Electronic Privacy Information Center, *The Drivers Privacy Protection Act (DPPA) and the Privacy of Your State Motor Vehicle Record*.⁸ The DPPA protects driver privacy by imposing access, use, and transfer restrictions. Nobody may access the

⁸ <https://epic.org/dppa/>.

information unless they seek it for specific permissible uses, and nobody may access highly restricted personal information for any reason without express consent. 18 U.S.C. §§ 2721(a)(1)–(2). Recipients who use or republish information in any way inconsistent with the listed permissible uses face civil liability, fines, and potential criminal penalties. 18 U.S.C. §§ 2721(c), 2722–24. Notably, the Seventh Circuit has twice found the DPPA consistent with the First Amendment. *See Dahlstrom v. Sun-Times Media, LLC*, 777 F.3d 937, 946–54 (7th Cir. 2015); *Travis v. Reno*, 163 F.3d 1000, 1007 (7th Cir. 1998).

The Freedom of Information Act (“FOIA”) presumes public access to government records, but it also empowers agencies to withhold personal information where disclosure would represent an unwarranted violation of privacy. The FOIA requires an agency to make certain records available to the public, 5 U.S.C. § 552(a)(2), but it permits agencies to withhold information that triggers one of nine different exemptions, two of which relate directly to privacy, *see id.* §§ (b)(6)–(7). The Privacy Act itself created special rules that work in tandem with the FOIA when a person requests records containing personal information. *See* U.S. Dep’t of Justice, Office of Information Policy, *OIP Guidance: The Interface Between the FOIA and Privacy Act* (last updated Feb. 7, 2025).⁹ In combination, the two statutes permit maximal access to government records without needlessly

⁹ <https://www.justice.gov/oip/oip-guidance-interface-between-foia-and-privacy-act>.

violating individuals' privacy. When a person requests a government record containing personal information, an agency must evaluate the request under both laws. *See id.* The statutes are as permissive as possible when a person requests a record containing information about the requestor because a person represents no privacy risk to themselves. Both statutes presume disclosure, and neither statute's exemptions can prohibit disclosure due to a requestor under the other statute. *See id.* (citing 5 U.S.C. § 552(a)(1)–(2)). Meanwhile, a person requesting a record about a third party has no rights under the Privacy Act but enjoys a presumption of disclosure under the FOIA unless an exemption—such as a privacy exemption—applies. *See id.* If a person requests data about themselves under the Privacy Act that contains information identifying third parties who have not consented to disclosure, both statutes contemplate circumstances in which the third party's information may or may not be shared based on privacy considerations. *Id.* This statutory framework carefully manages both privacy and transparency considerations.

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 (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. It prevents data collected by a government agency for statistical purposes from being used or disclosed for any other purpose. 44 U.S.C. §§ 3572(a)(1)–(2).

A variety of state open records laws impose access and use restrictions to protect residents' privacy. The California Public Records Act prevents individuals from obtaining the address of arrestees or victims of crimes unless they declare under penalty of perjury that the request is for approved purposes. Cal. Gov't Code § 7923.620; *see Los Angeles Police Dep't v. United Reporting Publ'g Corp.*, 528 U.S. 32 (1999). Idaho's Public Records Act generally prohibits the sale or distribution of any list of persons contained in public records for use as a mailing or phone number list unless consent is obtained from each person on the list. Idaho Code § 74-120(1). Kansas's Open Records Act requires requesters to attest that they will not use personal information for commercial purposes before getting access to public records containing that information. K.S.A. 45-220(c)(2)(A)–(B). The Maryland Public Information Act places a variety of restrictions on use of personal information in public records. *See, e.g.*, Md. Code Ann. Gen. Prov § 4-308(b) (only permitting inspection of public libraries' circulation records in narrow circumstances); § 4-312(b)(2) (prohibiting disclosure of any information that would identify a person in interest when county auditors access former or current

employees' retirement records); § 4-315(b) (prohibiting the use of criminal records and reports to solicit or market legal services).

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.

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. *See generally* Fed. Trade Comm'n, *Privacy and Security Enforcement* (listing privacy and data security enforcement actions).¹⁰ 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

¹⁰ <https://www.ftc.gov/news-events/topics/protecting-consumer-privacy-security/privacy-security-enforcement> (last visited September 23, 2026).

laws);¹¹ *see also* Caitriona Fitzgerald & Suzy Bernstein, EPIC, *Full of Holes: Federal Law Leaves Americans' Personal Data Exposed* (Apr. 27, 2013).¹²

Federal and state governments have developed a framework that, for decades, has promoted both government transparency and individual privacy protections. *Amicus* believes the Internet Sharing Ban falls comfortably within this framework. As the Court considers the Internet Sharing Ban's constitutionality, it must keep in mind how its rule will impact the broader framework of statutes and regulations that underpin U.S. data protection.

II. THE FIRST AMENDMENT AND INFORMATION PRIVACY RIGHTS WORK TOGETHER TO SECURE THE FUNDAMENTAL RIGHT TO VOTE AND BOLSTER DEMOCRATIC PARTICIPATION.

It is well understood that democratic self-governance is a core goal of the First Amendment. *See Whitney v. California*, 274 U.S. 357, 375–78 (1927) (Brandeis, J., concurring) (discussing the need for protected free speech to achieve deliberative self-government); *Mills v. Alabama*, 384 U.S. 214, 218 (1966) (finding that “a major purpose of [the First] Amendment was to protect the free discussion of governmental affairs”). By guaranteeing citizens the freedom to speak, associate, and access their government, the First Amendment ensures that the people can check government tyranny and enjoy free and frank political

¹¹ <https://www.nytimes.com/wirecutter/blog/state-of-privacy-laws-in-us/>.

¹² <https://epic.org/full-of-holes-federal-law-leaves-americans-personal-data-exposed/>.

participation. These democratic aims are most perfectly realized by the right to vote. When individuals register to vote or cast their ballots, they exercise not only their fundamental right to vote but also their rights to speech and association. *See Buckley v. Am. Const. L. Found.*, 525 U.S. 182, 195 (1999) (finding that voter registration implicates political thought and expression).

Voter privacy is necessary to achieve the First Amendment's purpose. As prominent constitutional and privacy law scholars have explained, meaningful democratic engagement requires that individuals have space to freely explore ideas, form conclusions, and speak without fear, coercion, or pressure to conform to social norms. *See* Jack Balkin, *Digital Speech and Democratic Culture: A Theory of Freedom of Expression for the Information Society*, 79 N.Y.U. L. Rev. 1, 3 (2004); Julie E. Cohen, *What Privacy Is For*, 126 Harv. L. Rev. 1904, 1912–18 (2013). Privacy provides such space. By limiting the collection, use, and disclosure of personal information, privacy protects uninhibited democratic participation at the ballot box. *See* Ira S. Rubenstein, *Voter Privacy in the Age of Big Data*, 2014 Wisc. L. Rev. 861, 887, 905–07.

Failing to adequately protect voter privacy is counterproductive to the task of democratic self-governance. First, voter privacy protects individual voters from intimidation and harassment based on how they exercise their voting rights. Voter intimidation has deep roots in the U.S. *See* Caitriona Fitzgerald *et al.*, *The Secret*

Ballot at Risk: Recommendations for Protecting Democracy 4 (2016).¹³ Indeed, the right to a secret ballot, now a cornerstone of American elections, evolved as a response to rampant intimidation and coercion by the government, employers, and neighbors threatening economic ruin, joblessness, or violence, particularly to silence black voters. See *Burson v. Freeman*, 504 U.S. 191, 200–06 (1992) (detailing the history of voter intimidation in the U.S.); Ben Cady & Tom Glazer, *Voters Strike Back: Litigating Against Modern Voter Intimidation*, 39 N.Y.U. Rev. L. & Soc. Change 173, 177, 188–91 (2015). While voter intimidation is certainly improved since the introduction of the secret ballot, these risks remain. Cady & Glazer, *supra*, at 177–78. The decision to register as a voter “implicates political thoughts and expression.” *Buckley v. Am. Const. L. Found.*, 525 U.S. 182, 195 (1999).

Pennsylvania’s voter registration list contains uniquely sensitive information, including an individual voter’s decision to register, association with a political party, and voter history. The broad republication of this information would be an effective tool to anyone seeking to exert pressure on individual voters and threaten free democratic participation. Maintaining sensible limits on the acquisition and disclosure of voter registration lists, therefore, helps ensure that voters are willing to exercise their right to vote for the causes and candidates of

¹³ <https://www.secretballotatrisk.org/Secret-Ballot-At-Risk.pdf>

their choice while also permitting important functions such as election integrity work, journalism, research, and other beneficial tasks.

Inadequate voter privacy protections perpetuate broad chilling effects on the right to vote. Pennsylvania’s voter registration list does not exist in a vacuum but may be combined by anyone with commercially available information to gain unprecedented insights about any one voter for targeted use. *See* Rubenstein, *supra*, at 895–97. Indeed, a 2005 survey of Californians found that 23 percent did not register to vote because of privacy concerns. *Id.* Similarly, Americans nationwide roundly reject tailored political advertising, and declare themselves unwilling to vote for candidates that harvest their data. *Id.* Motivated by their privacy concerns, voters will act to protect themselves by avoiding registration, providing incorrect information, or even refraining from political engagement altogether. *See id.* Regulations that facilitate government transparency without promoting indiscriminate dissemination of voters’ personal information is therefore necessary to maintain vital political discourse.

The harms that flow from disregarding voter privacy are not hypothetical. As this Court knows, since May 2025, the Department of Justice has attempted to obtain unredacted voter registration lists from nearly every state based on unfounded claims of voter fraud. *See* Kaylie Martinez-Ochoa *et al.*, Brennan Center for Justice, Tracker of Justice Department Requests for Voter Information

(last updated Sep. 18, 2026).¹⁴ To date, 23 courts have roundly rejected these attempts as baseless, invasive, and pretextual. In its decision dismissing DOJ’s bid in California, the court in *United States v. Weber* noted the Justice Department’s intent to create an illegal national database to pursue immigration enforcement. 816 F. Supp. 3d 1168, 1185–1186 (C.D. Cal. 2026) (appeal filed); *see also United States v. Schmidt*, 835 F. Supp. 3d 697, 699–700 (W.D. Pa. 2026) (appeal filed) (documenting evidence that the federal government intended to weaponize voter rolls in elections, engage in fishing expeditions, and for immigration enforcement). At the same time, the Department of Homeland Security and Immigration and Customs Enforcement have directed their agents and third-party contractors to collect and analyze voter registration and history data directly. *See* David Gilbert, *ICE Plans to Pay \$5 Million to Create National Voting Database*, *Wired* (Sept. 2, 2026).¹⁵ As the *Weber* court noted, these violations of voter privacy will inevitably chill democratic participation and diminish public trust as people rightfully fear their information being misused in unpredictable and illegal ways. 816 F. Supp. 3d. at 1175–76, 1195–96.

¹⁴ <https://www.brennancenter.org/our-work/research-reports/tracker-justice-department-requests-voter-information>.

¹⁵ <https://www.wired.com/story/ice-plans-to-pay-5-million-to-create-national-voting-database/>.

Protecting voter privacy is essential to protect the free exercise of the right to vote. The Supreme Court has recognized the value of rules that promote both privacy and free-speech values in tandem. *See McIntyre v. Ohio*, 514 US 334, 357 (1995) (holding that requiring disclosure of one’s name on campaign materials had potential chilling effect on citizens and infringed on anonymous speech); *Burson v. Freeman*, 504 U.S. 191, 207–08 (1992) (recognizing voter privacy at polling places as necessary to protect against undue coercion). To find the two in conflict would undermine the free exercise of the franchise and, thus, free speech itself. *See* Jack M. Balkin, *Technology and Constitutional Rot* 27–28 (2026).

III. THE INTERNET SHARING BAN PROTECTS VOTER PRIVACY WITHOUT RESTRICTING SPEECH.

The Internet Sharing Ban is a targeted commonsense use and transfer restriction—specifically a disclosure rule—that protects voter privacy without restricting protected speech. The Internet Sharing Ban permits dissemination of information for evaluating NVRA compliance while protecting the secret ballot and ensuring that stalkers, harassers, and other malevolent actors cannot easily target or intimidate voters by accessing a public centralized list of highly sensitive personal information. Voter privacy is constitutive of the right to vote, *see supra* Section II, and the ban ensures the individuals can safely exercise this right, a fundamental right “preservative of all rights.” *Yick Wo v. Hopkins*, 118 U.S. 356, 370 (1886). Without the ban, the right to vote would be further imperiled.

Furthermore, any claimed burden on First Amendment speech on Appellant's part is overstated. The Internet Sharing Ban is a viewpoint-neutral disclosure condition on information that the government controls. VRF cannot claim a First Amendment injury when its expression is not affected and its views are not disfavored.

A. The Internet Sharing Ban protects voter privacy.

The unrestricted republication of voter registration information online is a dangerous threat to voter privacy. The Internet Sharing Ban is a commonsense disclosure rule that allows for NVRA compliance while still vindicating the secret ballot and preventing voter intimidation and harassment.

While voter registration lists do not themselves list who voters cast a ballot for, party affiliation can be highly indicative of the individuals that voters cast ballots for. Since the 2004 election, Democratic and Republican voters have consistently voted for their party's presidential candidate over 89 percent of the time. Am. Nat'l Election Studies, *The Anes Guide to Public Opinion and Electoral Behavior: Presidential Vote: 2 Major Parties*.¹⁶ Publishing voters' party affiliation and voting history online would effectively disclose who they voted for to anyone with an internet connection. The harms of this erosion of voter privacy are all too

¹⁶ https://electionstudies.org/data-tools/anes-guide/anes-guide.html?chart=vote_for_president_2_parties

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);¹⁷ Alexander Hertel-Fernandez, *Employer Political Coercion: A Growing Threat*, *American Prospect* (Nov. 23, 2015).¹⁸

While employers cannot verify how an employee actually voted, wholesale publication of voter 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 employees from voting in their desired primary. *See* Commonwealth of Pennsylvania, *Types of Elections* (accessed Sept. 21, 2026) (Pennsylvania has a closed primary system).¹⁹

Aside from ameliorating potential voter coercion, the Internet Sharing Ban protects voters from potential harassment, doxing, and intimidation. All too often, individuals are harassed and stalked because their personal information can be gleaned from publicly posted voter registration lists. Scottie Andrew, *For Abuse*

¹⁷ <https://theintercept.com/2018/11/06/midterms-2018-voting-coercion-bosses-employees/>

¹⁸ <https://prospect.org/2015/11/23/employer-political-coercion-growing-threat/>

¹⁹ <https://www.pa.gov/agencies/vote/elections/types-of-elections>

Victims, Registering to Vote Brings a Dangerous Tradeoff, CNN (Oct. 27, 2020).²⁰

Domestic abuse victims in particular face a daunting choice between preserving their privacy and safety, and exercising their right to vote. While research on domestic violence and its impact on voting is sparse due to complex methodological issues, numerous survivors have spoken publicly about how wide dissemination of public voter registration lists deters them from participating in elections. Danielle Root, *Obstacles to Voting for Survivors of Intimate Partner Violence*, Center for American Program (Nov. 1, 2018);²¹ Amy Rolph, *Voting Can Be Dangerous for Domestic Violence Survivors in Washington State*, KUOW (Oct. 9, 2018).²²

In other cases, easy access to voter registration lists helps malicious actors dox and intimidate voters. A POLITICO review of forums dedicated to coordinated online harassment found multiple instances where harassers used publicly posted voter registration records to identify victim's addresses. Alfred Ng, *Some States Are Fighting to Protect Voters from Doxxing. They're Losing*, Politico

²⁰ <https://www.cnn.com/2020/10/27/us/domestic-violence-voting-election-privacy-trnd/index.html>

²¹ <https://www.americanprogress.org/article/obstacles-voting-survivors-intimate-partner-violence/>.

²² <https://www.kuow.org/governing/2018-10-09/for-domestic-violence-survivors-voting-can-be-dangerous>

(Mar. 17, 2024).²³ Harassment tactics include repeatedly calling to the victim's home based on false alarms. *Id.* VRF's own online lists have already been misused in precisely that way. In one example, online posters used VRF's online lists to dox a reporter. Noor Al-Sibai, *If You Voted, Now Your Address and Party Registration Are Publicly Available Online*, Futurism (Nov. 8, 2024).²⁴ Malicious actors have also used online lists to harass and intimidate voters, impersonating government officials while falsely intimating that voters have committed fraud. Morgan Lee & Anthony Izaguirre, *Voter Rolls Are Becoming the New Battleground over Secure Elections as Amateur Sleuths Hunt Fraud*, Associated Press (Oct. 6, 2023).²⁵ In New York, voters in 13 different counties were approached at their homes in a coordinated effort by individuals from a group called the New York Citizens Audit. *Id.* Group members accused residents of voter fraud while impersonating election officials. *Id.* These incidents are deleterious towards our democracy and prevent citizens from exercising their right to vote. As a 2016 Pew survey of unregistered eligible voters highlighted, eleven percent of unregistered voters did not register because of privacy and security

²³ <https://www.politico.com/news/2024/03/17/the-losing-fight-to-keep-your-voter-registration-data-private-00147401>.

²⁴ <https://futurism.com/the-byte/voter-registration-address-site>.

²⁵ <https://apnews.com/article/elections-voter-rolls-access-trump-fraud-claims-7bf841f66cf6e0731ca6322e08de737c>.

concerns. Pew Research Center, *Why Are Millions of Citizens Not Registered to Vote?* (June 21, 2017).²⁶

While bad actors might still misuse voter registration lists with the Internet Access Ban in place, posting these lists online dramatically increases the ease with which the lists can be misused. A public online list can be accessed by anyone, at any time, for any reason, and for any purpose. Public lists can easily be scraped at will by tools such as EagleAI NETwork, an oft-inaccurate matching software that is currently being used for mass voting challenges which can disenfranchise voters. Alice Clapman & Andrew Garber, *A New Antidemocracy Tool*, Brennan Center for Justice (Sep. 5, 2023).²⁷ Meanwhile, use and transfer restrictions enable States to more easily enforce voter intimidation and protection laws. The restrictions ensure that there is a viable chain of custody that can be used for investigatory purposes if the voter registration lists are misused. But without the Internet Sharing Ban, it becomes all too easy for malicious actors to anonymously scrape a publicly posted list. See e.g., Xiaofeng Liu et al., *Fingerprinting Web Browser for Tracing Anonymous Web Attackers*, 2026 IEEE First International Conference on Data Science in Cyberspace (2016) (detailing difficulty of tracing attackers using multi-

²⁶ <https://www.pew.org/en/research-and-analysis/issue-briefs/2017/06/why-are-millions-of-citizens-not-registered-to-vote>

²⁷ <https://www.brennancenter.org/our-work/analysis-opinion/new-antidemocracy-tool>

step proxies or anonymous networks).²⁸ Thus, the ban is crucial to ensuring voter privacy and empowering citizens to exercise their right to vote.

B. The Internet Sharing Ban does not restrict protected speech.

The Internet Sharing Ban conditions access to information already under government control that the government voluntarily discloses. As this Court has recognized, the First Amendment does not require “unfettered access to government information.” *Whiteland Woods, L.P v. Twp. of W. Whiteland*, 193 F.3d 177, 182 (3d Cir. 1999) (holding that right to access planning commission meeting was not meaningfully restricted by ban on videotaping). And while the Government may not condition access to information based “on illegitimate criterion such as viewpoint,” it is free to support “some speech without supporting other speech.” *Los Angeles Police Dep’t v. United Reporting Publ’g Corp.*, 528 U.S. 32, 43 (1999) (Ginsburg, J., concurring).

The Internet Sharing Ban is on its face an information disclosure rule. Information disclosure rules regulate the ability of persons that possess information to communicate, sell, or otherwise transfer that information to others. Neil M. Richards, *Reconciling Data Privacy and The First Amendment*, 52 UCLA L. Rev. 1149, 1195 (2005). And “American law is replete with legal obligations placed on one person not to disclose information about another.” *Id.* Such obligations can

²⁸ <https://ieeexplore.ieee.org/document/7866130>.

find their basis in contract, where two parties may agree to keep information secret. *Id.* at 1201; *see Cohen v. Cowles Media Co.*, 501 U.S. 663, 670 (1991) (upholding promissory estoppel principles to allow a plaintiff to recover against a newspaper for its breach of a promise of confidentiality). They can also find their basis in generally applicable laws, *see supra* Section I, that impose obligations that do not place a burden upon protected, expressive conduct. Richards, *supra* at 1205. While limitations on disclosure may trigger First Amendment scrutiny if they “are based on the contents of the speech and are aimed at a particular viewpoint,” *Sorrell v. IMS Health, Inc.*, 564 U.S. 552, 565 (2011), there is no general rule that disclosure rules automatically implicate or run afoul of the First Amendment.

The Internet Sharing Ban is precisely the sort of viewpoint-neutral rule that avoids First Amendment scrutiny. It regulates access to certain government information conditioned on acceptance of an information disclosure rule that Pennsylvania believes is helpful for voter privacy. Pennsylvania is completely agnostic in its application of the Internet Sharing Ban, as even VRF admits. Appx. 280, 288. No one, no matter their party affiliation (or viewpoint) may upload the voter registration file to the Internet. Nor does the ban prohibit VRF from “express[ing] its views” as to what it learns from the voter registration list. *See White Woods, L.P.*, 193 F.3d at 183. VRF is free to make whatever arguments it would like based on what it learns from the file. And others are free to obtain the

file to ascertain whether VRF's arguments have merit. The only obstacle is that VRF cannot post the personal details of the nearly 7 million Pennsylvania voters online, for all to peruse. Commonwealth of Pennsylvania, *Voting & Election Statistics* (last updated Sep. 14, 2026).²⁹ But that by itself does not constitute protected speech.

The Internet Sharing Ban does not implicate the First Amendment. It is a commonsense information disclosure that ensures voter privacy while not discriminating among favored or disfavored speakers.

* * *

Pennsylvania law and the regulations governing the handling of voter records properly balance the public interests in promoting election integrity, protecting voter privacy, and ensuring that individuals can speak and inquire freely about these government systems. The Public Information Lists regulations ensure that individuals have access to information necessary to review and report on the Commonwealth's management of voter registration and records, and the prohibition on republishing the entire Voter File online is a reasonable use limitation necessary to protect the privacy of Pennsylvania voters. Allowing such publication would not provide any marginal improvement to transparency. The

²⁹ <https://www.pa.gov/agencies/dos/resources/voting-and-elections-resources/voting-and-election-statistics>

Internet Sharing Ban is similar in nature to other access, use, and transfer conditions that restrict access to personal data and other sensitive information in state and federal laws across the country. In addition, these regulations only limit access to government information for which there is no First-Amendment-based right of access, and they are broadly applicable, viewpoint-neutral, and firmly rooted in important privacy justifications. The Court should hold that these regulations are constitutional and serve the important dual purposes of protecting Pennsylvanians' privacy and for the integrity of the overall data protection regime.

CONCLUSION

Amicus respectfully request this Court affirm the lower court's order granting Appellee's motion for summary judgment.

/s/ Alan Butler_____

Alan Butler

Counsel of Record

Tom McBrien

Abigail Kunkler

Kabbas Azhar

Electronic Privacy Information Center

1519 New Hampshire Ave. NW

Washington, DC 20036

(202) 483-1140

butler@epic.org

COMBINED CERTIFICATES

1. **Type-Volume:** This brief complies with the type-volume limitation of Fed. R. App. P. 29(a)(5) and 32(a)(7)(B) because it contains 5,442 words according to the word-counting function of Microsoft Word for Mac, Version 16.96.2, excluding the parts of the brief exempted by Rule 32(f). This brief also complies with the typeface requirements of Rule 32(a)(5) and the type style requirements of Rule 32(a)(6) because this brief has been prepared in a proportionally spaced typeface of 14-point Times New Roman.
2. **Bar Membership:** Pursuant to L.A.R. 28.3(d), I certify that I am a member of good standing of the Bar of the United States Court of Appeals for the Third Circuit.
3. **Paper Copies:** I certify that the text of the electronic brief filed via ECF is identical to the text of the paper copies mailed to this Court.
4. **Virus Check:** Pursuant to L.A.R. 31.1(c), I certify that electronic copy of this brief was scanned with VirusTotal, and no virus was detected.
5. **Service:** I certify that on this date, I am filing the foregoing Brief of *Amicus Curiae* Electronic Privacy Information Center Support of Appellee with the Clerk of the United States Court of Appeals for the Third Circuit using the CM/ECF system. All parties are to this case will be served via the CM/ECF system.

Dated: September 23, 2026

/s/ Alan Butler

Alan Butler

Counsel of Record

Electronic Privacy Information Center

1519 New Hampshire Ave. NW

Washington, DC 20036

(202) 483-1140

butler@epic.org