STATE OF SOUTH CAROLINA COUNTY OF RICHLAND ANNE CROOK, Plaintiff, v. SOUTH CAROLINA ELECTION COMMISSION A/K/A STATE ELECTION COMMISSION, Defendants.	IN THE COURT OF COMMON PLEAS **Civil Action No. 2025-CP-40- 06539** **NOTICE OF MOTION AND MOTION FOR TEMPORARY INJUNCTION**

TO: STATE ELECTION COMMISSION

PLEASE TAKE NOTICE THAT the Plaintiff in this matter, Anne Crook, pursuant to SC Code Sections 7-5-170, 7-5-186(B), 7-5-186(C), 30-2-20 et seq., South Carolina Constitution, Article 1, Section 10, and Rule 65, SCRCP, moves for a temporary injunction enjoining Defendant State Election Commission ("Defendant") from distributing the Statewide Voter Registration List, in full, to the Department of Justice.

Pursuant to the current Scheduling Order in this matter, Plaintiff moves for a hearing on this motion to be conducted at 2pm on Friday, September 26, 2025.

FACTUAL AND PROCEDURAL BACKGROUND

Defendant is, by statute, authorized to collect the information of persons registering to vote in the State of South Carolina. On August 6 and 14, Defendant received two letters demanding the Statewide Voter Registration List from the Department of Justice ("DOJ"). Affidavit of Howard

Knapp, Exhibit 1. Defendant began conversations with the DOJ about what information could be shared and how, including a discussion of a data sharing agreement and a memorandum of understanding ("MOU"). *Id*.

DOJ's letters to Defendant demanded more than what is available in the salable precinct list; the full Statewide Voter Registration List additionally contains information such as phone numbers, social security numbers, and state-issued identification numbers. *Id*.

Upon information and belief, no data sharing agreement or memorandum of understanding has been reached between the DOJ and Defendant, both of which Defendant considered necessary for "securely sharing such information and data." *Id*.

As a result, Plaintiff filed a Complaint with a request for injunctive relief and a declaratory judgment prior to the expiration of the deadline set by DOJ to Defendant to produce the Statewide Voter Registration List. A Temporary Restraining Order was granted preventing Defendant from complying with DOJ until a hearing could be held, and a hearing was set for the following Wednesday, September 10. Rather than having said hearing, both Defendant and proposed intervenor, Governor McMaster, filed with the appellate courts to reverse the Temporary Restraining Order; these motions were successful, as the State Supreme Court found that the Circuit Court Order lacked sufficient detail. However, no ruling on the merits resulted from the South Carolina Supreme Court.

Venue was transferred to Richland, and the matter was assigned to the Chief Administrative Judge, Judge Coble.

PARTIES

Defendant is the State Election Commission, the body tasked with impartially conducting the business of elections in South Carolina; among its duties is voter registration.

Plaintiff is Dr. Anne Crook, a registered voter from Calhoun County, SC. Dr. Crook has objected to her protected personally identifiable information ("PII") such as her partial social security number and her state-issued identification number from being shared with the DOJ.

DEFENDANT'S RESPONSIBILITIES UNDER THE LAW

Plaintiff outlines herein SEC's responsibilities and general restrictions on PII under state law. These arguments are incorporated by reference into Plaintiff's likelihood to succeed on the merits. In summary, state law prohibits the disclosure of certain PII, and at a minimum, a confidentiality agreement and restrictions are required before PII can be disclosed outside of the SEC. SC Code Sections 7-5-170, 7-5-186, 30-2-20 et seq., and the State Constitution. Furthermore, as discussed *infra*, these laws are not pre-empted by federal law.

SC Code Section 7-5-170 and Voter Registration

This statute sets forth the PII to be collected when someone is registering to vote. It includes the applicant's social security number but does not include state-issued identification number (driver's license number). In fact, the voter registration application does not request the applicant's identification number. The application also provides the following disclaimer: "SSN is required by the SC Code of Laws 7-5-170. This number is used for internal purposes only and eliminates multiple registration by a single individual. Your Social Security Number is not released to any unauthorized individual." Voter Registration Application, Exhibit 2.

SC Code Section 7-5-186(B)

The General Assembly enacted SC Code Section 7-5-186 titled "Statewide Voter Registration Database." SC Code Section 7-5-186 requires the SEC to "establish and maintain a statewide voter registration database." It allows for this database to be available to County Boards

of Voter Registration and "other agencies as authorized by law."[1]

SC Code Section 7-5-186(B) expressly states that the SEC shall "ensure that any information or data provided to [SEC], which is confidential in the possession of the entity providing the data, remains confidential while in the possession of the [SEC]." Importantly, in SC Code Section 7-5-186 there is an explicit statutory authority as to when this information may be shared.

SC Code Section 7-5-186(C)

SC Code Section 7-5-186(C) states:

> The State Election Commission may enter into agreements to share information or data with **other states or groups of states**, as the commission considers necessary, **in order to maintain the statewide voter registration database** established pursuant to this section. Except as otherwise provided in this subsection, **the commission shall ensure that any information or data provided to the commission that is confidential in the possession of the state providing the data remains confidential** while in the possession of the commission. The commission may provide such otherwise confidential information or data to persons or organizations that are **engaging in legitimate governmental purposes related to the maintenance of the statewide voter registration database**. (emphasis added).

There can be a considered a four pronged test set forth by SC Code Section 7-5-186(C) for the sharing of information: 1) the proposed recipient must be a qualified entity, 2) the SEC must find that the sharing is necessary to maintain the voter registration database, 3) the SEC must have assurances of confidentiality, and 4) that the entity receiving the information must be engaging in

[1] DOJ is not an agency expressly authorized to receive this information in any part of the SC Code of Laws.

maintenance of the voter registration database. The demand by DOJ fails on all four fronts. Briefly, 1) DOJ is not a state or a group of states. 2) DOJ is not purporting to maintain the statewide voter registration database and has no role in doing so. 3) SEC is required to keep this information confidential and to date, no security agreement has been produced. 4) DOJ has not claimed to be engaging in a purpose "related to the maintenance of the statewide voter registration database." *See* Exhibits filed with Plaintiff's Complaint, letters from DOJ dated August 6 and 14.

SC Code Section 30-2-20 (Privacy policies and procedures required of all state entities), et seq.

This portion of SC Code requires all state agencies, which includes Defendant, to "develop privacy policies and procedures to ensure that the collection of personal information pertaining to citizens of the State is limited to such personal information required by any such agency, board, commission, institution, department, or other state entity and necessary to fulfill a legitimate public purpose."

SC Code Section 30-2-30(1) defines personal information to include Social Security Number and Driver's Identification Number (state-issued identification number). As to this PII, the General Assembly made the following express findings:

> (1) The social security number can be used as a tool to perpetuate fraud against an individual and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to the individual. While the social security number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes and other legitimate consensual purposes.

(2) Although there are legitimate reasons for state and local government entities to collect social security numbers and other personal identifying information from individuals, government entities should collect the information only for legitimate purposes or when required by law. An entity that provides employee benefits has a legitimate need to collect and use social security numbers and personal identifying information as part of its administration and provision of employee benefits programs.

(3) When state and local government entities possess social security numbers or other personal identifying information, the governments should minimize the instances this information is disseminated either internally within government or externally with the general public.

SC Code Section 30-2-300.[2] Not only has the General Assembly made these findings expressly, but Plaintiff shares the same concern as outlined in her Affidavit. Exhibit 3, Crook Affidavit.

South Carolina Constitution, Article 1, Section 10

The South Carolina Constitution states: "The right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures and **unreasonable invasions of privacy shall not be violated**." S.C. Const. art. I, § 10 (emphasis added). "Right to privacy" protected by South Carolina constitution is individual's right to be let alone and to live life free from unwarranted publicity. *Bauer v. Summey*, 2021, 568 F.Supp.3d 573. The South Carolina Constitution, with an express right to privacy provision included in the article prohibiting

[2] SC Code Section 30-2-310 goes on to state the numerous prohibitions placed on State Agencies with respect to SSNs, including that they may not "use the social security number or a portion of it containing six digits or more for any purpose other than the purpose stated." *Id*. (d).

unreasonable searches and seizures, favors an interpretation offering a higher level of privacy protection than the Fourth Amendment. *State v. Key* (S.C. 2020) 431 S.C. 336, 848 S.E.2d 315.

As we have seen in recent years, the State's Right to Privacy extends beyond criminal matters. *See e.g.*, *Planned Parenthood S. Atl. v. State*, 438 S.C. 188, 882 S.E.2d 770 (2023), reh'g denied (Feb. 8, 2023); *see also*, *Singleton v. State*, 313 S.C. 75, 437 S.E.2d 53 (1993). In each of these cases, privacy is recognized as a more expansive right under the South Carolina Constitutional provision.

When reading each of these statutes and provisions in concert, it is apparent that the State of South Carolina places a high value on personal information and privacy. The Plaintiff agrees and has therefore filed this action.

LACK OF FEDERAL AUTHORITY TO SUBMIT INFORMATION

The DOJ's letters to the SEC posit that they are owed South Carolina's voter PII under three avenues: Section 8(i) of the National Voter Registration Act ("NVRA"), the Help America Vote Act ("HAVA"), and the Civil Rights Act of 1960. None apply, and as such, SEC is under no obligation to comply with these demands, particularly when they are in opposition to State Law.

NVRA

DOJ claims that it is entitled to South Carolina's unredacted voter roll (plus driver's license and social security information) under the NVRA's "public disclosure provision." DOJ Letters, August 6. But courts have routinely held the opposite. The First Circuit, for example, recently explained that "nothing in the text of the NVRA prohibits the appropriate redaction of uniquely or highly sensitive personal information in the Voter File." *Pub. Int. Legal Found., Inc. v. Bellows*, 92 F.4th 36, 56 (1st Cir. 2024) (collecting cases). In fact, courts have specifically authorized the redaction of social security numbers, which "are uniquely sensitive and vulnerable to abuse,"

Project Vote/Voting for Am., Inc. v. Long, 752 F. Supp. 2d 697, 711–12 (E.D. Va. 2010), and driver's license information, *Pub. Int. Legal Found., Inc. v. Boockvar*, 431 F. Supp. 3d 553, 563–64 (M.D. Pa. 2019).[3]

The DOJ's citation of NVRA also creates a problematic implication and outcome. The NVRA is for *public* disclosures. Under the DOJ's logic concerning NVRA, the public, writ large, would be entitled to social security numbers, phone numbers, driver's license numbers, etc. That is a stark reversal of DOJ's longstanding position on the issue, *see, e.g.*, U.S. Br. as Amicus Curiae at 27–28, *Public Int. Legal Found. v. Bellows*, No. 23-1361 (1st Cir. July 25, 2023), https://perma.cc/ML4S-5V4S; U.S. Br. as Amicus Curiae at 24–26, *Project Vote*, 682 F.3d 331 (No. 11-1809), https://perma.cc/HSM3-U964, and is incompatible with the Fourth Circuit's holding that "a statute that conditions voting on public release of a voter's Social Security number 'creates an intolerable burden on that right as protected by the First and Fourteenth Amendment,'" *Project Vote/Voting for Am., Inc. v. Long*, 682 F.3d 331, 339 (4th Cir. 2012) (quoting *Greidinger v. Davis*, 988 F.2d 1344, 1355 (4th Cir. 1993)). Moreover, if NVRA were to apply in such a fashion, other organizations could demand a disclosure from DOJ of this protected PII since it would have been turned over to the DOJ on the grounds of that it was sent to the public for inspection.

HAVA

HAVA simply does not apply to this type of request from the DOJ. Unlike the NVRA,

[3] Under the NVRA's public disclosure provision, courts have also blocked access to voters' dates of birth, *True the Vote v. Hosemann*, 43 F. Supp. 3d 693, 735–39 (S.D. Miss. 2014); telephone numbers, *Project Vote, Inc. v. Kemp*, 208 F. Supp. 3d 1320, 1343 (N.D. Ga.); email addresses, *id.*, and information bearing on citizenship status, *Pub. Int. Legal Found., Inc. v. N. Carolina St. Bd. of Elect.*, 996 F.3d 257, 266–68 (4th Cir. 2021).

HAVA has no disclosure provision.[4] Thus, DOJ has no authority under HAVA to demand documents outside of its ordinary subpoena or discovery powers. HAVA, and the Attorney General's related enforcement authority, primarily concerns list *maintenance—i.e.*, the procedures employed by states to clean and maintain their voter lists by, for example, removing duplicate and ineligible voters. *See* 52 U.S.C. § 21083. Given that purpose, the Attorney General could argue that she has implicit authority under HAVA to demand information about how South Carolina updates, cleans, and otherwise manages its voter rolls. But because access to unredacted voter *data* does not further that purpose (and is mentioned nowhere in the statute), HAVA provides no basis for DOJ's present demand. Finally, even if HAVA implicitly created a novel investigative tool for reviewing a state's voter list (it did not), that disclosure would be subject to the same redaction and privacy concerns that apply to Section 8(i) of the NVRA. *See supra*.

It is important to note, however, that the DOJ has never publicly stated what this requested disclosure is for - what end it intends to seek. Without such a stated purpose or objective, it is impossible Plaintiff, Defendant, or the Court to attempt to determine if the disclosure is appropriate even if it is permissible on some yet unshown legal grounds.

Civil Rights Act of 1960

The purpose of the Civil Rights Act of 1960 is not to manage the transfer of data simply because the DOJ requests it. Its purpose, in relevant portion, is to ensure fair and free elections. The Civil Rights Act of 1960 requires state election officers to preserve, "for a period of twenty-

[4] DOJ blithely asserts that "Congress plainly intended that DOJ be able to conduct an independent review of each state's list." DOJ Letters (Aug. 14, 2025). But no court has ever said so, and Congress only speaks through the text of statutes. On this issue, HAVA's textual silence is deafening.

two months" following "any general, special or primary election," "all records and papers which come into [their] possession." 52 U.S.C. § 20701. The statute goes on to require the states to make those documents available for inspection, "upon demand in writing by the Attorney General," with one condition: "This demand shall contain a statement of the basis and the purpose therefore." 52 U.S.C. § 20703. Again, given that DOJ has not yet ventured a basis or purpose for its unprecedented quest for state voter list data (aside from a vague interest in investigating list maintenance under the NVRA and HAVA, which is not furthered by reviewing a state's unredacted voter list, *see supra*), it has not yet met the statutory qualifications for invoking the Civil Rights Act.

GROUNDS FOR TEMPORARY INJUNCTION

"To obtain an injunction, the plaintiff must allege facts sufficient to constitute a cause of action for injunction and demonstrate the injunction is reasonably necessary to protect the legal rights pending in the litigation." *Levine v. Spartanburg Regional Services District, Inc*., 367 S.C. 458, 464, 626 S.E.2d 38, 41 (Ct. App. 2005). Obtaining an injunction requires the plaintiff to show that (1) it would suffer irreparable harm if the injunction is not granted; (2) it will likely succeed on the merits of the litigation; and (3) there is an inadequate remedy at law. *Grosshuesch v. Cramer*, 367 S.C. l, 4, 623 S.E.2d 833, 834 (2005). In considering whether to grant an injunction, the court should balance the equities of the opposing parties on the particular facts of the case to determine which side is more entitled to relief. *Levine*, supra.

A. PLAINTIFF HAS DEMONSTRATED THAT IRREPARABLE HARM WILL RESULT IF AN INJUNCTION IS NOT GRANTED.

Once personal information is shared, there is no getting it back. "**The disclosure of private, confidential information 'is the quintessential type of irreparable harm that cannot**

be compensated or undone by money damages.'" *Airbnb, Inc. v. City of New York*, 373 F. Supp. 3d 467, 499 (S.D.N.Y. 2019) (granting preliminary injunction) (quoting *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000)). "Many [courts] have found that ongoing unauthorized disclosure, and even the mere unauthorized retention, of sensitive personal information is irreparable harm that money damage cannot remedy." *Am. Fed'n of Tchrs. v. Bessent*, 772 F. Supp. 3d 608, 657 (D. Md. 2025) (collecting cases), *vacated and remanded on other grounds,* No. 25-1282, 2025 WL 2313244 (4th Cir. Aug. 12, 2025) (only discussing likelihood of success on the merits).

Plaintiff has posited that such sharing would violate her rights under South Carolina laws and invite outcomes such as identity theft. Of note, the federal agencies very recently lacked security in maintaining citizens' personal information. *See*, *e.g.*, Letter from Dana L. Gold and Andrea Meza to Hon. Rand Paul, et al. (August 26,2025), b181d62a-full.pdf; *see also* Jenna McLaughlin, *A whistleblower's disclosure details how DOGE may have taken sensitive labor data*, NPR (Apr. 15, 2025) (available at: https://www.npr.org/2025/04/15/nx-s1-5355896/doge-nlrb-elon-musk-spacex-security).

Plaintiff would suffer harm for which there would be no remedy if either 1) more of her PII is shared than is permissible under the law or 2) the information is shared without adequate protection.

B. PLAINTIFF HAS SHOWN A LIKELIHOOD OF SUCCESS ON THE MERITS.

Plaintiff has set forth numerous applicable statutes and provisions that affect her position as a South Carolina voter with PII in the hands of the SEC. Pursuant to the statues and State Constitution, outlined *supra*, she has every right to expect that the SEC will treat her PII with the

utmost security and confidentiality as required by law.

"When seeking a preliminary injunction, the plaintiff need not prove an absolute legal right; the plaintiff need only present a fair question to raise as to the existence of such a right." *Levine*, 367 S.C. at 465, 626 S.E.2d at 42 (internal quotations omitted). A court "may consider the merits of a case to the extent necessary to determine whether a temporary injunction is appropriate." *Helsel v. City of North Myrtle Beach*, 307 S.C. 29, 32, 413 S.E.2d 824, 826 (1992). "Once a *prima facie* showing has been made entitling the plaintiff to injunctive relief, a temporary injunction will be granted without regard to the ultimate termination of the case on the merits." *Id.*

Defendant, by its own admission and actions, has created an interesting paradox which outlines the tension herein and underscores the likelihood that Plaintiff will succeed on the merits. On one hand, Defendant has stated that it would like to work on a security agreement and MOU to share the information. However, if no state law or other privacy concern existed, the SEC could have simply sent the information in early August. Defendant knows it has a privacy responsibility. Even if a cobbled together reading of the statutes might allow Defendant to share Plaintiff's protected PII with the DOJ, that can only happen if it is for an explicit and legitimate reason related to maintaining the state voter rolls. DOJ's failure to state a reason gives rise to suspicion that the PII will be misused. Nowhere is it anticipated in State Law that a person's PII will be turned over by the State to the federal government, in fact, the Governor himself expressed concerns about this type of data accumulation when he was Attorney General. SC Atty Gen Op. Mar. 24, 2008 (McMaster) (explaining how South Carolina might respect South Carolinians' reluctance to "turn our state driver's licenses into national ID cards" without violating the federal Real ID Act of 2005).

There is little balancing required by the Court between the interests of the parties. Numerous other States have refused to send their data to the DOJ without repercussion.[5]

C. PLAINTIFF LACKS AN ADEQUATE REMEDY AT LAW.

Plaintiff invokes the old 'Horses out of the Barn' adage. Plaintiff further notes the tale of the 'Camel's Nose Under the Tent.' In general, Plaintiff will have no remedy once her information is transmitted. *See e.g.*, *Hirschfeld v. Stone*, 193 F.R.D. 175, 187 (S.D.N.Y. 2000). Furthermore, if Plaintiff's information is not shared securely, she will have little adequate remedy if her PII is exploited by a bad actor. While Defendant could argue that this damage is repairable, in that the DOJ could destroy the information at a future date, Plaintiff would have no remedy under South Carolina law for such remediation, as State Courts would have little ability to bind a federal agency, and her remedies would be limited to those contemplated by federal law, which, as Plaintiff has outlined *supra*, may be more permissive that South Carolina's guarantees to its citizens.

RELIEF REQUESTED

Plaintiff asks that the court issue a temporary injunction (1) enjoining Defendant from releasing the protected PII of South Carolina voters to DOJ, (2) enjoining Defendant from releasing any information without a data sharing agreement and MOU which adequately protects her rights, and (3) that such an agreement and MOU be subject to review by this Court.

Plaintiff requests that such injunction be binding upon the Defendant, their officers, agents, servants, employees, and attorneys, and upon those persons in active concert or participation with

[5] See Kevin Miller, *Maine's top election official tells DOJ to 'jump in the Gulf of Maine' over voter data request*, Maine Public Radio (July 29, 2025) (available at: https://www.mainepublic.org/politics/2025-07-29/maines-top-elections-official-tells-doj-to-jump-in-the-gulf-of-maine-over-voter-data-request). *See also*, Brennan Center Tracker (Sept. 8, 2025) (available at: https://www.brennancenter.org/our-work/research-reports/tracker-justice-department-requests-voter-information).

them who receive actual notice of the order for temporary injunction by personal service or otherwise.

Plaintiff moves for this temporary injunction by posting of minimal or no security as there is no danger of an adverse effect on Defendant. Rule 65(c), SCRCP.

WE SO MOVE:

s/ Skyler B. Hutto
C. Bradley Hutto, S.C. Bar No. 6436
Skyler B. Hutto , S.C. Bar No.102741
WILLIAMS & WILLIAMS
ATTORNEYS AT LAW
Post Office Box 1084
Orangeburg, SC 29116
Tel: (803) 534-5218
cbhutto@williamsattys.com
skyler williamsattys.com

Date: September 22, 2025
Orangeburg, South Carolina