IN THE COMMONWEALTH COURT OF PENNSYLVANIA

SENATOR JAY COSTA, SENATOR ANTHONY H. WILLIAMS, SENATOR VINCENT J. HUGHES, SENATOR STEVEN J. SANTARSIERO, AND SENATE DEMOCRATIC CAUCUS,	:	CASES CONSOLIDATED
Petitioners,	:	No. 310 MD 2021
vs.	:	
SENATOR JACOB CORMAN III, SENATE PRESIDENT PRO TEMPORE, SENATOR CRIS DUSH, AND SENATE SECRETARY-PARLIAMENTARIAN MEGAN MARTIN,	:	
Respondents.	:	
COMMONWEALTH OF PENNSYLVANIA, PENNSYLVANIA DEPARTMENT OF STATE And VERONICA DEGRAFFENREID, Acting Secretary of the Commonwealth of Pennsylvania,	:	
Petitioners,	:	No. 322 MD 2021
vs.	:	
SENATOR CRIS DUSH, SENATOR JAKE CORMAN, and THE PENNSYLVANIA STATE SENATE INTERGOVERNMENTAL OPERATIONS COMMITTEE,	:	
Respondents.	:	
ARTHUR HAYWOOD JULIE HAYWOOD,	:	

Petitioners,	:	
vs.	:	No. 323 MD 2021
VERONICA DEGRAFFENREID, ACTING SECRETARY OF STATE, COMMONWEALTH OF PENNSYLVANIA,	:	
Respondents.	:	

BRIEF IN SUPPORT OF
MOTION FOR SUMMARY RELIEF PURSUANT TO Pa.R.A.P. 1532(b)
FILED BY PETITIONER-INTERVENORS
ROBERTA WINTERS, NICHITA SANDRU, KATHY FOSTER-SANDRU, ROBIN ROBERTS, KIERSTYN ZOLFO, MICHAEL ZOLFO, PHYLLIS HILLEY, BEN BOWENS, THE LEAGUE OF WOMEN VOTERS OF PENNSYLVANIA, COMMON CAUSE PENNSYLVANIA AND MAKE THE ROAD PENNSYLVANIA

TABLE OF CONTENTS

TABLE OF AUTHORITIES

CASES

STATUTES

OTHER AUTHORITIES

RULES

TREATISES

REGULATIONS

BRIEF IN SUPPORT OF
MOTION FOR SUMMARY RELIEF PURSUANT TO Pa.R.A.P. 1532(b)
FILED BY PETITIONER-INTERVENORS
ROBERTA WINTERS, NICHITA SANDRU, KATHY FOSTER-SANDRU, ROBIN ROBERTS, KIERSTYN ZOLFO, MICHAEL ZOLFO, PHYLLIS HILLEY, BEN BOWENS, THE LEAGUE OF WOMEN VOTERS OF PENNSYLVANIA, COMMON CAUSE PENNSYLVANIA AND MAKE THE ROAD PENNSYLVANIA

INTRODUCTION

The issue in this important case is whether under the Pennsylvania Constitution's robust protection for informational privacy the Pennsylvania Senate's Intergovernmental Operations Committee ("Committee") can enforce a legislative subpoena to acquire nine-million Pennsylvania voters' personally-identifying information without a clear, demonstrated need for the data and an explanation of how it will use it. The Committee, which has no history of election oversight, has made vague claims that it needs to investigate "allegations" about the November 2020 election and the May 2021 primary election. These elections, and especially the November 2020 election, have in the past year been scrutinized in dozens of lawsuits and investigated by multiple government bodies, including by professionals in state and county election bureaus and legislative committees that have issued reports. Those lawsuits and investigations have uncovered no major problems. In short, this Committee has embarked on a fishing expedition, but one with potentially dangerous consequences.

Conducting a baseless investigation is one thing, but doing so in a way that exposes the private personal data of nine million Pennsylvanians to unnecessary and significant financial and identity fraud risks is a bridge too far. Pennsylvania's historically strong protection for residents' constitutional right of informational privacy imposes a formidable check on the Committee's effort. Absent, in the first instance, a clear demonstration of why the Committee needs the data and why it is essential to promoting a compelling governmental interest, this Court must enjoin enforcement of the Subpoena.

Even if the Committee were able to satisfy this stringent test to justify the massive and intrusive data request, the Committee would still need to demonstrate that it has the technical expertise and has adopted appropriate safeguards to control transfer, storage and access to the highly-sensitive data to prevent breaches and thereby protect nine million voters' constitutional privacy rights. Respondents have not met their burden to demonstrate a legitimate, compelling interest in the personally-identifying information of all registered voters, and that the demand for this information, especially driver's license and social security numbers, is narrowly tailored for a legitimate purpose. And they certainly have not established

that they can protect this information if they receive it. Petitioner-Intervenors[1] are entitled to relief under Pa.R.A.P. 1532(b).

I. Factual Background

A. The Subpoena and its Purported Purpose

On September 15, 2021, Senator Dush, in his capacity as Chair of the Committee, issued a subpoena *duces tecum* to Veronica Degraffenreid, Acting Secretary of the Commonwealth ("Subpoena," attached to the accompanying Motion as Exhibit A). The Subpoena "ordered" the Secretary to "supply the following documents listed below" no later than October 1, 2021. The Subpoena then listed the various documents and other information it required, including:

> A complete list containing the name, date of birth, driver's license number, last four digits of Social Security number, address, and date of last voting activity of all registered voters within the Commonwealth of Pennsylvania as of May 1, 2021, by County.

(Exhibit A, ¶4). The Subpoena further requested additional lists of the same information, broken down by individuals who voted in the November 2020 election and the May 2021 primary, further broken down by the type of vote cast, i.e., in-person, mail-in ballot, absentee ballot or provisional ballot (Exhibit A, ¶¶6-

[1] The Court has not yet ruled upon Intervenor-Petitioners' Application for Leave to Intervene. Intervenor-Petitioners nevertheless file this Motion and Brief now to comply with the expedited schedule agreed upon by the Parties, and so as not to cause any delay in the expedited proceedings.

13). Thus, the Subpoena on its face seeks personally-identifying information, including date of birth, driver's license number and partial Social Security number, of every registered voter in the Commonwealth.

As of December 31, 2020, there were approximately nine million registered voters in the Commonwealth (The Administration of Voter Registration in Pennsylvania, 2020 Report to the General Assembly (Department of State, June 2021), attached to the accompanying Motion as Exhibit B).

The Subpoena itself does not describe its purpose or the reasons why the Committee needs personally-identifying information of any particular set of voters, let alone all registered voters in the Commonwealth. At a September 15, 2021, Committee hearing, when asked the purpose of the Subpoena, Senator Dush responded:

> Those documents are part of any audit that the auditor general would conduct or anybody who is ***looking to verify the identity of individuals and their place of residence and their eligibility to vote.***

(Transcript of 9/15/21 Hearing, attached to the accompanying Motion as Exhibit C, at 17:4-8 (emphasis added)). *See also* Exhibit C, at 19:12-13 ("Again, it is to verify the individuals"). When asked why it was necessary to verify the identity of individual voters, Senator Dush responded as follows:

> Because ***there have been questions*** regarding the validity of people who have voted, whether or not they exist. ***Again, we are not responding to proven allegations. We are investigating the allegations to determine whether or not they are factual***.

(Exhibit C, 17:15-20 (emphasis added)). Senator Dush was asked on several occasions why these "questions" warranted an investigation when testimony at prior hearings revealed no issues regarding voter identity, and the transcript does not show any response to those queries (Exhibit C, pp. 18-20).

Separately, the Committee has asserted that Social Security numbers and driver's license numbers are "necessary to help identify any duplicate registrations, fake registrations, and any votes resulting from those ineligible registrations." Home - Pennsylvania Election Investigation, found at: https://paelectioninvestigation.com/. (printout as of October 11, 2021, attached to the accompanying motion as Exhibit E). *See also* https://www.pasenategop.com/blog/intergovernmental-operations-committee-announces-new-election-integrity-investigation-website/ (printout as of October 11, 2021, attached to the accompanying motion as Exhibit E-1, confirming this is the Committee's website). The Committee's website does not provide any factual basis for its speculation that there were any "votes resulting from . . . ineligible registrations" and, in any event, does not explain why Social Security numbers and driver's licenses numbers are necessary for such a process.

B. <u>The Lack of Factual Basis for the Subpoena</u>

Before issuing its Subpoena, the Committee held a hearing on September 9, 2021 (Transcript of September 9, 2021 Hearing, attached to the accompanying Motion as Exhibit D). According to Senator Dush, the purpose of the September 9 hearing was to examine "Act 77[2] and how the regulatory issues of the last-minute guidances [sic] came down that impacted it" (Exhibit D, at 61:18-24). *See also* Exhibit D, at 70:17-22 ("the actions that led up to and during the last-minute guidance from the Secretary"). Because the hearing was limited to Act 77 and last minute guidance on its implementation from the Department of State, and was not intended to address any problems regarding voter identity, no testimony was received, or other evidence presented, regarding any duplicate registrations, fake registrations or voter identity irregularities or anomalies. Although not the intended subject of the hearing, the sole witness at that hearing, Fulton County Commissioner Stuart Ulsh, testified that the County conducted an investigation earlier this year that reported no instances of voting irregularities (Exhibit D, 62:24 to 63:12).

Three separate legislative and joint government committees already have examined the November 2020 election and found no voter identity irregularities or

[2] Act of October 31, 2019, P.L. 552, No. 77 (which provided for expanded mail-in voting, among other election reforms)

anomalies. The House State Government Committee, which typically oversees the Department of State and elections generally, held ten hearings and heard from 52 testifiers, as part of an investigation into Pennsylvania's election laws. On May 10, 2021, that committee issued a report with its findings (A COMPREHENSIVE REVIEW OF PENNSYLVANIA'S ELECTION LAWS: HOW PENNSYLVANIA CAN GUARANTEE RIGHTS AND INTEGRITY IN OUR ELECTION SYSTEM, attached to the accompanying Motion as Exhibit F). Separately, the Senate Special Committee on Election Integrity and Reform conducted its own investigation into the 2020 election, holding three public hearings and hosting an online survey. That committee published its report in June 2021 (REPORT ON THE SPECIAL COMMITTEE'S FINDINGS AND RECOMMENDATIONS TO THE SENATE AND THE SENATE STATE GOVERNMENT COMMITTEE, attached to the accompanying Motion as Exhibit G). Finally, a Joint State Government Commission, created by the General Assembly, conducted yet another investigation and issued a report in June 2021 (ELECTION LAW IN PENNSYLVANIA: REPORT OF THE ELECTION LAW ADVISORY BOARD FOR THE FISCAL YEAR 2020-2021, attached to the accompanying Motion as Exhibit H). The Reports of these Committees and Commissions do not reflect any findings of irregularities or anomalies in voter identity or eligibility during the November 2020 election or May 2021 primary.

Litigants made allegations of voting irregularities in numerous lawsuits both before and after the November 2020 election. None of those lawsuits, uncovered evidence of fake or duplicate registrations, or any issues with voter identity. Rather, the courts routinely dismissed such allegations for lack of evidence. *See, e.g.*, *Bolus v. Boockvar*, No. 3:20-CV-1882-RDM, 2020 U.S. Dist. LEXIS 219337 (M.D. Pa. 2020) (denying injunction and dismissing complaint for failure to show likelihood of success on the merits, adopting a report and recommendation (2020 U.S. Dist. LEXIS 200373) that found: "Wholly lacking is any allegation that collecting ballots in locations other than the office of the County Election Board results in fraudulent ballots"); *Donald J. Trump for President, Inc. v. Boockvar*, 502 F. Supp.3d 899, 906 (M.D. Pa. 2020) (granting motion to dismiss claims, finding "One might expect that when seeking such a startling outcome, a plaintiff would come formidably armed with compelling legal arguments and factual proof of rampant corruption, . . . That has not happened. Instead, this Court has been presented with strained legal arguments without merit and speculative accusations, unpled in the operative complaint and unsupported by evidence."), *aff'd*, 830 Fed. Appx. 377 (3d Cir. 2020); *Donald J. Trump for President, Inc. v. Boockvar*, 493 F. Supp.3d 331, 342, 373 (W.D. Pa. 2020) (granting summary judgment to defendants after "extensive discovery" and finding, "While Plaintiffs may not need to prove actual voter fraud [prior to the election], they must at least prove that such fraud is

'certainly impending.' They haven't met that burden. At most, they have pieced together a sequence of uncertain assumptions . . ."") (opinions collectively attached to the accompanying Motion as Exhibit J).

Thus, while Senator Dush referenced "questions" or "allegations" to support the issuance of the Subpoena, many different governmental bodies comprising officials from both major political parties and from all three of Pennsylvania's branches of government, county elections departments, and many federal and state courts have already considered these same issues. None have identified any factual support for these so-called questions or allegations that underlie the Committee's highly intrusive demand for 9 million voters' personally identifying information.

C. Lack of Security Preparations for the Subpoenaed Information

When asked about security for the personally-identifying information that the Subpoena seeks, the Committee has provided only general statements that the information will be "stored securely" and that any third party vendor personnel would sign a non-disclosure agreement (Exhibit E). Senator Dush stated during the September 15, 2021, hearing that documents and data responsive to the subpoena would be "held in legal counsel's office until such time as we have a finalized agreement and a contract for the investigator" (Exhibit C, 24:10-12). He further stated that the data responsive to the Subpoena would be secured "just like any other legal documents are secured within the senate legal offices" (Exhibit C,

24:16-20). The records of nine million Pennsylvania voters containing highly sensitive personally-identifying information, however, are not the same "as any other legal document" (Declaration of J. Alex Haldeman, attached to the accompanying Motion as Exhibit I, at ¶17).

Dr. Haldeman is Professor of Computer Science and Engineering, Director of the Center for Computer Security and Society, and Director of the Software Systems Laboratory at the University of Michigan in Ann Arbor. An important part of his scholarship has been election security and techniques for conducting rigorous post-election audits. He is Co-Chair of the State of Michigan's Election Security Advisory Commission, and has performed security testing of electronic voting systems in California. Dr. Halderman is greatly concerned about the Committee's Subpoena, and has submitted a Declaration discussing those concerns (Exhibit I).

At the September 15, 2021 Committee hearing, Senator Dush could not explain who would have access to the information except noting that those with access would include his staff, his legal counsel, Senate Republication legal counsel, possibly unidentified outside counsel, and unidentified third party vendors (Exhibit C, p. 20-21). With respect to vendors, Senator Dush noted "there is going to be a need to have multiple investigators, multiple areas of expertise," but those vendors have not yet been identified (Exhibit C, p. 39:16-17). It is not known

whether other members of the Committee and their staffs and counsel also would have access.

Transferring, storing and sharing a large data set of sensitive, personally-identifying information without employing industry-recognized best practices to protect that information creates substantial risk (Exhibit I, ¶22). Widely recognized standards exist to protect such information (Exhibit I, ¶¶25-28). *See also* House State Government Committee Report (Exhibit F), p. 60-61 (With respect to election security, expert testified that "there must be a strong access control to the database to know who has access at any time" and "cyber-attacks can be mounted to the system by an adversary impersonating an individual through their Social Security number, found on the dark web"). But the Committee has not indicated that it will, or demonstrated that it can, comply with such standards (Exhibit I, ¶24).

D. <u>The Owners of the Subpoenaed Information</u>

Intervenor-Petitioners include eight registered voters who reside throughout the Commonwealth, and who cast votes in the November 2020 election and/or the May 2021 primary. The Subpoena seeks information about, and belonging to, Intervenor-Petitioners and other registered voters in the Commonwealth. All of the individual Intervenor-Petitioners are concerned about the disclosure of their

personally-identifying information (Verified Petition, ¶5-43). Each has particularized concerns set forth in the Verified Petition for Review. *Id.*

The organizational Intervenor-Petitioners (the "Organizations") expend considerable resources for the purpose of registering voters and ensuring that eligible voters can exercise their right to vote (Verified Petition, ¶¶44-74; Verified Application for Leave to Intervene, ¶35). Their members and constituents registered to vote and chose to participate in elections based on the reasonable expectation that their highly sensitive private personal information would be kept confidential. Disclosure of voters' private personal information works against the mission of these organizations and would require the organizations to divert resources and expend additional sums in an effort to try to protect that information, educating their members and constituents regarding the risk to their personal information, and encouraging them to participate in the process (Verified Application for Leave to Intervene, ¶35). In particular, these organizations encounter resistance from voters who are wary of providing their driver's license number or last four digits of their Social Security number because they fear misuse of that private information (Verified Petition, ¶¶52, 61).

As discussed below, Intervenor-Petitioners have a reasonable expectation of privacy in their personally-identifying information, and in fact, have a constitutional right to maintain the privacy of that information.

E. The Risks of Unauthorized Disclosure of Personally-Identifying Information

The unauthorized disclosure of voters' highly sensitive personal information would violate their constitutional right to privacy as explained below. Moreover, disclosure poses significant risk above and beyond the infringement of voters' constitutional right to privacy, and the adverse impact on the voters' constitutional right to vote.

The risk from disclosure of sensitive personally-identifying information is that thieves can create false accounts in individuals' names, access bank accounts or medical records, incur debt in a person's name, and cause other severe disruptions to an individual's life (Exhibit I, ¶18). An individual's name and address coupled with the last four digits of their Social Security number and/or driver's license number is enough to allow criminals to pose as the individual and engage in various activities to enrich themselves at the expense of the individual (Exhibit I, ¶18). In particular, a criminal could use one's name address, zip code and last 4 digits of his or her Social Security number to access credit card information and bank accounts. (Exhibit I, ¶19)

Several Intervenor-Petitioners previously have been victims of identity theft, and are especially attuned to the risk of disclosure of their personally-identifying information. Roberta Winters has twice had her private information disclosed

through data breaches, and her husband's bank account was drained of all funds (Verified Petition, ¶6). Nichita Sandru's debit card was hacked and used to make illegal purchases (Verified Petition, ¶14). Kathy Foster-Sandru's debit card also was hacked recently and used to make illegal purchases (Verified Petition, ¶18). Robin Roberts' husband bank card similarly was used to make unauthorized online purchases (Verified Petition, ¶22).

According to some estimates, it can take between 100 and 200 hours of an individual's time to recover from a stolen identity, especially when an impostor has opened new accounts, applied for government benefits or taken other actions in the name of the individual. The Identity Theft Resource Center reports that identity theft victims suffer financial, emotional and physical impacts from identity misuse. While the financial impacts vary, more than 21% of victims report that they lost more than $20,000 to identity criminals (Exhibit I, ¶20).

Voters' private information can be disclosed through numerous mechanisms, including hacking, phishing or other Social engineering methods, breaches of physical security, bribery, extortion, or insider attacks (Exhibit I, ¶22). All of these mechanisms could be used to access voters' personally-identifying information. Sharing this large dataset with many people, as yet unidentified, who have no announced plans to reliably safeguard the information, creates a high risk of a data breach (Exhibit I, ¶¶28-31). Given the Committee's inability (or unwillingness) to

detail their security precautions around data transfer, storage and access, enforcing the Subpoena would be "extremely risky" (Exhibit I, ¶22).

II. Argument

A. Pennsylvania Law Zealously Guards the Right to Privacy, and Plainly Protects Personally-Identifying Information Against Legislative Subpoenas.

Pennsylvania's "Constitution has historically been interpreted to incorporate a strong right of privacy…." *Commonwealth v. Alexander*, 243 A.3d 177, 204 (Pa. 2020) (*quoting Commonwealth v. Edmunds*, 586 A.2d 887, 899 (Pa. 1991)). *See also Commonwealth v. Gindlesperger*, 743 A.2d 898, 899 n.3 (Pa. 1999) ("strong notion of privacy" in Pennsylvania); *Commonwealth v. Waltson*, 724 A.2d 289, 292 (Pa. 1998) ("notion of enhanced privacy rights" in Pennsylvania); *Commonwealth v. Matos*, 672 A.2d 769, 773 (Pa. 1996) ("strong right of privacy"). Another decision characterized privacy as "the most comprehensive of rights and the right most valued by civilized [people]." *Denoncourt v. Commonwealth State Ethics Comm'n*, 470 A.2d 945, 948-49 (Pa. 1983) (*quoting Olmstead v. United States*, 277 U.S. 438, 478 (1928) (dissenting opinion of J. Brandeis)). In Pennsylvania, therefore, this "right to privacy is as much property of the individual as the land to which he holds title and the clothing he wears on his back." *Pennsylvania State Educ. Ass'n v. Commonwealth Dep't of*

Cmty. & Econ. Dev., 148 A.3d 142, 151 (Pa. 2016) ("*PSEA*") (*citing Commonwealth v. Murray*, 223 A.2d 102, 109 (Pa. 1966)).

This decades-long commitment to safeguarding Pennsylvanians' privacy is rooted in the common law, the protection of "inherent and indefeasible rights" in Article 1, Section 1 of the Pennsylvania Constitution, and the protection against unreasonable searches and seizures in Article 1, Section 8. *See, e.g., Stenger v. Lehigh Valley Hops. Ctr.*, 609 A.2d 796, 800-02 (Pa. 1992); *Murray*, 223 A.2d at 109-10. The fact that this right emanates from multiple sources "is a recognition that the constitution of our Commonwealth embodies a commitment to principles that manifest themselves in a coherent pattern of protection of individual privacy." Seth F. Kreimer, *The Right to Privacy in the Pennsylvania Constitution*, THE PENNSYLVANIA CONSTITUTION: A TREATISE ON RIGHTS AND LIBERTIES (Gormley, Ed. 2020), at 788-89.

Pennsylvania's longstanding commitment to safeguarding individuals' privacy is stronger than protections under the U.S. Constitution. The Pennsylvania Supreme court recently reaffirmed that, "Article 1, Section 1 of the Pennsylvania Constitution provides even 'more rigorous and explicit protection for a person's right to privacy'" than does the U.S. Constitution. *PSEA*, 148 A.3d at 151 (citation omitted). *See also Alexander*, 243 A.3d at 206 ("Article I, Section 8 affords greater

protection to our citizens than the Fourth Amendment" and, referring also to Article I, Section I, "[w]e must consider our charter as a whole . . .").

The right to privacy includes what is referred to as the "right of informational privacy," described as "the right of the individual to control access to, or the dissemination of, personal information about himself or herself." *PSEA*, 148 A.3d at 150. *See also In re T.R.*, 731 A.2d 1276, 1279 (Pa. 1999) (plurality) ("There is no longer any question that the United States Constitution and the Pennsylvania Constitution provide protections for an individual's right to privacy . . . [including] . . . the individual's interest in avoiding disclosure of personal matters . . ."). As discussed further below, personal information subject to constitutional protection includes the personally identifying information subpoenaed by the Committee.

Pennsylvania's constitutional privacy rights indisputably apply to legislative subpoenas. Pennsylvania courts, going back decades, have applied the constitutional right of privacy to protect individuals from unjustified and overbroad legislative subpoenas. *See, e.g., Lunderstadt v. Pennsylvania House of Representatives Select Comm.*, 519 A.2d 408, 415 (Pa. 1986); *Commonwealth ex. Rel. Carcaci v. Brandamore*, 327 A.2d 1, 4 (Pa. 1974) ("Broad as it is, however, the legislature's investigative role, like any other governmental activity, is subject to the limitations placed by the Constitution on governmental encroachments on

individual freedom and privacy"); *McGinley v. Scott*, 164 A.2d 424, 431 (Pa. 1960) ("[L]egislative investigations must be kept strictly within their proper bounds if the orderly and long-established processes of our coordinate branches of government are to be maintained"); *Annenberg v. Roberts*, 2 A.2d 612, 617-18 (Pa. 1938) ("None of the rights of the individual citizen has been more eloquently depicted and defended in the decisions of the Supreme Court of the United States than the right of personal privacy as against unlimited and unreasonable legislative or other governmental investigations….").

1. Social Security Numbers and Driver's License Numbers, In Particular, Are Included Within the Right of Privacy

The Pennsylvania Supreme Court recently recognized that there are "certain types of information whose disclosure, by their very nature, would operate to the prejudice or impairment of a person's privacy, reputation, or personal security, and thus intrinsically possess a palpable weight that can be balanced by a court against those competing factors that favor disclosure." *PSEA*, 148 A.3d at 155. The Court referenced earlier decisions protecting the personal information of constituents who contacted elected officials as examples where "patently strong privacy interests" outweighed the "weak, perhaps non-existent" public interest in favor of disclosure. *Id*. (*citing Sapp Roofing Co. v. Sheet Metal Workers' Int'l Ass'n, Local Union No. 12*, 713 A.2d 627 (Pa. 1998) (plurality), and *Tribune–Review Publ. Co. v. Bodack*, 961 A.2d 110 (Pa. 2008)). Driver's license and Social Security

numbers are particularly sensitive private information that merit heightened protection.

Pennsylvania law protects individuals' privacy in Social Security numbers. *See PSEA*, 148 A.3d at 158 (*citing Times Publ'g Co. v. Michel*, 633 A.2d 1233, 1237-38 (Pa. Commw. 1993), and *Sapp Roofing*, 713 A.2d 627 (refusing request for names, addresses, Social Security numbers and phone numbers)). *See also Governor's Office of Admin. v. Purcell*, 35 A.3d 811, 813 (Pa. Commw. 2011) (Social Security number part of the "holy trinity" for identity theft and deserves special protection); *Cypress Media, Inc. v. Hazleton Area Sch. Dist.*, 708 A.2d 866, 870 (Pa. Commw. 1998) ("[T]his Court has held that a person's [personally-identifying information including] Social Security number are not subject to disclosure under the [previous Right-to-Know] Act because the benefits of disclosing such information are outweighed by a person's privacy interests in that information.") (citations omitted)). *cf. Pa. State Univ. v. State Emples. Ret. Bd.*, 935 A.2d 530, 539 (Pa. 2007) ("With regard to the right to privacy in one's Social Security number, . . . , we would have greater difficulty concluding that the public interest asserted here outweighs those basic rights to privacy").

Even partial Social Security numbers, i.e., the last four digits, are sufficient to enable breaches of sensitive private data. Social Security numbers have been called the "skeleton key" for identity theft criminals. Jonathan J. Darrow &

Stephen Lichtenstein, *Do you Really Need My Social Security Number? Data Collection Practices in the Digital Age*, 10 N.C.J.L. & Tech. 1, 4 (2008). The first five numbers are relatively easy to recreate. For example, the first three digits represent an "area number," which identify a geographic area. Knowing where an individual lives can help narrow down the possible combinations. In fact, using "fairly standard computer algorithms," investigators have been able to predict the first five digits of Social Security numbers with alarming accuracy. "Social Security Numbers are Easy to Guess," Science Magazine, July 6, 2009, found at https://www.science.org/content/article/Social-Security-numbers-are-easy-guess (predicted first five digits on the first try 44% of the time). Thus, protecting the last four digits of the Social Security number is of extreme importance in assuring privacy (Exhibit I, ¶19).

Courts across the country, in other contexts, have recognized the highly sensitive nature of just the last four digits of Social Security numbers.[3]

[3] *See, e.g., Curphey v. F&S Mgmt., LLC*, 2021 U.S. Dist. LEXIS 25829, at *14 (D. Az. 2021) ("The Court will not ask Defendants to violate their employees' informational privacy unnecessarily. Defendants are not required to produce the last four digits of employees' Social Security number."); *Watt v. Fox Rest. Venture, LLC*, 2019 U.S. Dist. LEXIS 26959, at *24 (C.D. Ill. 2019) ("Because the last four digits of Social Security numbers is of marginal use in locating putative collective members and the marginal use is outweighed by the privacy concerns of putative collective members, the Court will not order Defendants to provide such information"); *Figueroa v. Harris Cuisine LLC*, 2019 U.S. Dist. LEXIS 12271, at *19 (E.D. La. 2019) ("The disclosure of dates of birth and the last four digits of

Pennsylvania's Right to Know Law also recognizes this, providing that "a record containing ***all or part of*** a person's Social Security number. . ." constitutes "personal identification information" that is exempt from disclosure. 65 P.S. §67.708(b)(6)(k)(A) (emphasis added).

Federal and state law likewise recognize the need to maintain the privacy of driver's license numbers because they can be used to identify particular individuals just as easily as can Social Security numbers. Driver's license numbers are considered "personal information" that the government may not disclose under the Drivers Protection Privacy Act, 18 U.S.C. §§2721, 2725(3). State law similarly prohibits the disclosure of records relating to the driving record of any person, 75

Social Security numbers raises significant privacy and Security concerns that outweigh the plaintiff's risk of failing to contact the potential class in this case, where notice will be provided via mail, email, and text message."); *Firneno v. Radner Law Grp., PPLC*, 2016 U.S. Dist. LEXIS 142907, at *10-11 (E.D. Mich. 2016) ("Plaintiffs persuasively argue that "the invasion of privacy caused by the unauthorized viewing and retention of their personal credit and other information" — including the last four digits of their Social Security number, their address, and the exact amount of debt owed to creditors — is a de facto injury that satisfies the injury-in-fact requirement."); *Acevedo v. WorkFit Med, LLC*, 2014 U.S. Dist. LEXIS 131269, at *30 (W.D.N.Y. 2014) ("Plaintiffs argue that they need the last four digits of the potential plaintiffs' Social Security numbers in order to locate potential plaintiffs if notices are returned as undeliverable. The Court is not persuaded that this rationale justifies disclosure of such sensitive information, particularly given that the Court has no way of knowing if and/or how many notices will be returned as undeliverable."); *White v. Integrated Elec. Techs., Inc.*, 2013 U.S. Dist. LEXIS 83298, at *41 (E.D. La. 2013) ("the Court recognizes the significant privacy and security concerns inherent in disclosing the last four digits of class members' Social Security numbers.").

Pa.C.S. §6114, and this Court has held that information included in a driver's license falls within this protection. *Advancement Project v. Pennsylvania Dep't of Transp*., 60 A.3d 891, 895-97 (Pa. Commw. 2013). In a recent case, the trial court found driver's license numbers to fall within the constitutional right of privacy and prohibited disclosure, a point conceded by the appellant on appeal. *Lancaster County District Attorney's Office v. Walker*, 245 A.3d 1197, 1205, 1206 (Pa. Commw. 2021) (Leavitt, J) ("the driver's license and address information should be redacted").

Other state laws and security protocols buttress Pennsylvanians' expectation that Social Security numbers and driver's license numbers will be kept confidential and exempt from disclosure requirements. For example, Pennsylvania's Right to Know Law protects from disclosure Social Security numbers or driver's license numbers, among other information. 65 P.S. §67.708(b)(6)(k)(A). Similarly, the Commonwealth's Information Technology Policy includes both pieces of information in its definition of personally-identifiable information (Pennsylvania Information Technology Policy No. ITP-SEC025 (March 19, 2010), https://www.oa.pa.gov/Policies/Documents/itp_sec025.pdf, attached to the accompanying motion as Exhibit K). *See also* Breach of Personal Information Notification Act, 73 P.S. 2301, 2302 (defining personal information to mean last name, first name or initial, and any of the following: Social Security number,

driver's license number, financial account number, and credit or debit card number).

Indeed, the security protocols for filing documents in Pennsylvania courts, including this Court, acknowledge the importance of maintaining the confidentiality of driver's license and Social Security numbers. Each time an attorney files a document in this Court, the attorney must verify that he or she has redacted personally-identifying information. Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of Appellate and Trial Courts, attached hereto as Exhibit L. That Policy specifically identifies Social Security numbers and driver's license numbers as "Confidential Information" that must be redacted (Exhibit L, Section 7.0(A)). *See also* Exhibit M (Login page for PACFile).

As a matter of law, driver's license and partial Social Security numbers are confidential and thereby protected by the constitutional right of informational privacy.

2. Large Collections of Data Pose Heightened Levels of Concern

While Social Security numbers and driver's license numbers are, in and of themselves, highly confidential personally-identifying information, that information is even more sensitive when combined with other personally-

identifying information such as name, address and date of birth. Together, those five pieces of information make it easy for a bad actor to steal one's identity or commit financial fraud (Exhibit I, ¶18 ("An individual's name and address coupled with the last four digits of their Social Security number and/or driver's license number is enough to allow criminals to pose as the individual and engage in various activities to enrich themselves at the expense of the individual.")). *Accord Purcell*, 35 A.3d 811, 813 (noting that theft experts consider name, date of birth and Social Security as the "Holy Trinity," because together they can be used to commit financial fraud). For example, with just the name, address, zip code and last four digits of the Social Security number, criminals can access credit card information and bank accounts (Exhibit I, ¶ 19).

When that same information is packaged together for multiple people, rather than just one person, it is especially attractive to identity thieves (Exhibit I, ¶16). And where that information is available for nine million voters in one dataset, it becomes an irresistible target. The Pennsylvania Supreme Court recently acknowledged "the threat to privacy implicit in the accumulation of vast amounts of personal information in computerized data banks or other massive government files." *PSEA*, 148 A.3d at 150, citing *Whalen v. Roe*, 429 U.S. 589, 605 (1977). As Dr. Halderman explains:

> The database of nine million Pennsylvania voters including driver's license and the last four digits of Social Security numbers is an attractive target for many reasons, not least its financial value. This data has a monetary value proportional to the number of people it represents, and it could command an even higher price because of the number of records that have multiple data points per individual. Voter registration records with name, address, date of birth, last four digits of Social Security number and driver's license number would be a treasure trove of neatly packaged information that could command a high price on the "Dark Web."

(Exhibit I, ¶21). *See also* Darrow & Lichtenstein, *Do you Really Need My Social Security Number?*, 10 N.C.J.L. & Tech. at 13 ("Unfortunately, the aggregation of vast amounts of data is like the hoarding of treasure: while few will bother to pick up a penny lying on the sidewalk, a bank vault full of cash will draw thieves and imposters from far afield.").

The Committee does not appear to understand, let alone have anywhere near the appropriate level of security for this massive collection of private information. The National Institute for Standards and Technology, the Commonwealth and the Federal Trade Commission all have issued guidance for creating security protocols to secure personally-identifying information (Exhibit I, ¶¶25-27), and all indications are that the Committee does not have the expertise or capacity to implement any of these measures (Exhibit I, ¶24). Without such security protocols, the risk that further disclosure will compound the initial privacy violation (disclosure of personally-identifying information to the Committee) is substantial (Exhibit I, ¶28 ("There is no evidence that the Committee has

implemented or is in a position to adopt these measures, and until and unless they do, voters' private data turned over to the Committee would be highly vulnerable")).

3. Registering to Vote Does Not Waive this Privacy Interest

Pennsylvania voters have no choice except to provide to the Secretary of State personally-identifying information if they want to exercise their constitutional right to vote. 52 U.S.C. §21083(a)(5)(i). *See also* 4 Pa. Code §183.1 (definition of personal information); Voter Registration Application, https://www.pavoterservices.pa.gov/pages/VoterRegistrationApplication.aspx. To the extent Respondents would argue that voters waive any right to privacy in this information when registering to vote, that argument is misplaced for several reasons.

First, waiver of the constitutional right of privacy, like waiver of any other constitutional right, occurs only where the waiver is "knowing, intelligent and voluntary." *Chester Hous. Auth. v. Polaha*, 173 A.3d 1240, 1250 (Pa. Commw. 2017) (*quoting Commonwealth v. Goodwin*, 333 A.2d 892, 894 (Pa. 1975)). Where voters have no choice but to provide this information, it cannot reasonably be argued that they voluntarily waived the right of privacy.

Second, voters are assured through numerous laws and regulations that their Social Security numbers and driver's license numbers will remain confidential upon registering to vote. Pursuant to Title 25, this private information is available only to the Secretary and any employees or agents she assigns to administer the Statewide Uniform Registry of Electors (SURE) system, as well as elected officials in the relevant county. 25 Pa. C.S. §1222(c)). Indeed, Pennsylvania law imposes criminal sanctions for accessing the SURE system without lawful authority. 25 Pa.C.S. §1707.

Although Pennsylvania statutes and regulations permit production of some information in certain voters' registration applications for certain purposes, these statutes and regulations do NOT allow access to Social Security numbers or driver's license numbers. For example, upon an authorized request, the Department of State may provide the name, address, date of birth and voting history of a voter, 4 Pa. Code §183.14, but voters' unique identifiers, driver's license number or Social Security number are ***specifically excluded*** from any such production. §183.14(c). Further, for certain categories of voters, home addresses likewise are excluded. §183.14(c)(4) and (5). *See also* 25 Pa.C.S. §1404. Street lists (lists of voters arranged by street or house number or alphabetically by surname) may be compiled for individual districts, limited to names and addresses, 4 Pa. Code §183.13(a), and even this limited information is subject to safeguards.

§183.13(c). This regulation specifies that a voter's signature, unique identifier, driver's license number and the last four digits of his/her Social Security number ***shall not be made available***. §183.13(c)(5). *See also* 25 Pa.C.S. §1403. Indeed, although the Department of State allows individuals to purchase the "Full Voter Export List," Social Security numbers and driver's license numbers are excluded from that list. See https://www.pavoterservices.pa.gov/Pages/PurchasePAFULLVoterExport.aspx. Thus, voters are routinely assured, and have a reasonable expectation, that their private information will remain private.

Indeed, any claim that submission of information for one purpose waives expectations of privacy regarding disclosures for other purposes would fly in the face of four decades of Pennsylvania law. For example, the Supreme Court rejected a state police argument that a criminal defendant waived any privacy interest he may have had in financial documents because he "voluntarily" conveyed them to his bank. *Commonwealth v. DeJohn*, 403 A.2d 1283, 1287-89 (Pa. 1979). The Court wrote that, "[f]or all practical purposes, the disclosure by individuals or business firms of their financial affairs to a bank is not entirely volitional, since it is impossible to participate in the economic life of contemporary society without maintaining a bank account." *Id.* at 1289 (*quoting Burrows v. Superior Court of San Bernardino County*, 13 Cal.3d 238, 118 Cal.Rptr. 166

(1974)). The Court thus refused to enforce the subpoena, finding that the defendant had a reasonable expectation of privacy in his financial documents. *Id.* at 1291. The Court has regularly reaffirmed this rule in other contexts. *See Commonwealth v. Melilli*, 555 A.2d 1254, 1258-59 (Pa. 1989) (sharing phone number dialed with telephone company does not void the privacy interest); *Commonwealth v. Shaw*, 770 A.2d 295, 299 (Pa. 2001) (blood test in possession of hospital does not void privacy interest). Similarly, voters' disclosure of their driver's license or Social Security numbers to elections officials in order to exercise their right to vote does not vitiate their expectation of privacy in the information.

Even as a matter of common law, the law of Pennsylvania requires custodians of personal information to avoid improper release of sensitive personal information. *Dittman v. UPMC*, 196 A.3d 1036, 1047 (Pa. 2018) (employer, who required employees to provide confidential information, including Social Security number, had a common law duty to exercise reasonable care to maintain the confidentiality of that data and not expose that information to others). The obligations on custodians of data that arise from Pennsylvania's right to privacy are even stronger. And the obligation to maintain the confidentiality of information applies equally to government entities and officers. As the Supreme Court has observed,

> [T]he citizens of this Commonwealth, pursuant to Article I, Section 1 of the Pennsylvania Constitution, have a right to informational privacy, namely the right of an individual to **control access to, and dissemination of, personal information** about himself or herself. Accordingly, we ruled that before the government may release personal information, it must first conduct a balancing test to determine whether the right of informational privacy outweighs the public's interest in dissemination. In so ruling, we were clear that …the PSEA balancing test is applicable to all government disclosures of personal information, including those not mandated by the RTKL or another statute.

Reese v. Pennsylvanians for Union Reform, 173 A.3d 1143, 1159 (Pa. 2017) (emphasis added, citations omitted). *See also City of Harrisburg*, 219 A.3d at 618 (requiring assessment of constitutional right of privacy in context of right to know request---which by definition is seeking information held by a public entity); *PSEA*, 148 A.3d at 146, 150-52 (same); *Denoncourt*, 470 A.2d at 947-48 (same).

Thus, not only does the Secretary of State have a duty to protect the confidentiality of voters' personally-identifying information, but voters are provided every assurance that she will do so. There can be no voluntary, knowing waiver of constitutional rights under such circumstances.

B. The Committee Has Not Demonstrated a Significant or Compelling Interest in the Requested Private Information, and Even if it Came Forward With Such Evidence, Any Such Interest Does Not Override Voters' Privacy Rights

Before any government entity discloses, or forces the disclosure of, any private, personal information, the Pennsylvania Constitution requires a balancing

of whether the right of informational privacy outweighs the public's interest in disclosure. *See, e.g.*, *Reese*, 173 A.3d at 1145-46. *See also PSEA*, 148 A.3d at 154; *City of Harrisburg*, 219 A.3d at 618. Given Pennsylvania's zealous protection of the right to privacy, the Committee bears a heavy burden:

> Privacy claims must be balanced against state interests. Our test of whether an individual may be compelled to disclose private matters, as we stated it in *Denoncourt*, is that "government's intrusion into a person's private affairs is constitutionally justified when the government interest is significant and there is no alternate reasonable method of lesser intrusiveness to accomplish the governmental purpose." 470 A.2d at 949. More recently, we have stated the test in terms of whether there is a compelling state interest. *Stenger*, 609 A.2d at 802. In reality, the two tests are not distinct. ***There must be both a compelling, i.e., "significant" state interest and no alternate reasonable method of lesser intrusiveness.***

In re T.R., 731 A.2d at 1280 (1999) (emphasis added) (citing *Denoncourt*, 470 A.2d at 949; *Stenger*, 609 A.2d at 802). This balancing test is in addition to any statutory restrictions such as those pursuant to the right to know law, and applies to any government disclosure of personal information. *Reese*, 173 A.3d at 1159 ("applicable to all government disclosures of personal information, including those not mandated by the [Right to Know Law] or another statute").

The Committee has not met its burden described above and, for the reasons outlined below, cannot do so. The Committee has not identified *any* legitimate interest, let alone one that outweighs voters' significant privacy interests, and has not established that there are no less-intrusive methods of satisfying any such

interest. As a result, the Court should grant Intervenor-Petitioners' Petition for Review, and enjoin Respondents from violating voters' privacy rights by obtaining the personally-identifying information requested in the Subpoena.

1. The Committee Cannot Satisfy Its Burden of Demonstrating Any Interest, Let Alone a Compelling or Significant Need for this Information.

The Committee has failed to advance a coherent justification for its electoral review, much less why it needs all 9 million voters' driver's license and partial Social Security numbers. When explaining the purpose of its investigation as a whole, Senator Dush stated: "to evaluate our election code is working and to confirm whether or not these things and their worth – if there were things that need to be changed in the law to make our elections run better for everyone" (Exhibit D, at 2:22 to 3:1). While an interest in improving our laws is laudatory, a general interest in examining whether the current law is working and whether changes can be made, cannot constitute a sufficient interest to override constitutional rights. Otherwise, constitutional rights would be illusory. Under such reasoning:

> -an interest in improving the tax laws would justify disclosure of every tax-paying citizen's tax returns and financial records
>
> -an interest in improving health care at state hospitals would justify disclosure of each patient's medical records
>
> -an interest in improving the way our justice system is administered would justify disclosure of internal court documents and communications.

In other words, the General Assembly would be entitled to any document it wanted as long as it purported to be seeking to improve the law. As demonstrated by the cases limiting legislative subpoenas discussed above at pp. 15-18, *supra*, the General Assembly's authority is not nearly so expansive.

Similarly, with respect specifically to the Subpoena's request for voters' constitutionally-protected personal information, Senator Dush stated that the Committee's purpose is to "verify the identity of individuals and their place of residence and their eligibility to vote" (Exhibit C, at 16:22-17:20). When asked why it was necessary to verify the identities of individual voters, Senator Dush responded by referring only to unsubstantiated allegations by unidentified individuals who supposedly had raised unspecified "questions":

> Because there have been questions regarding the validity of the people who have voted, whether or not they exist. Again, we are not responding to proven allegations. We are investigating the allegations to determine whether or not they are factual.

(*Id.*, at 17:15-20). No facts have been developed that would provide any substantiation to such "questions" or "allegations."

Courts have cautioned against "fishing expeditions," where there is no evidentiary basis to intrude upon privacy rights:

> Anyone who respects the spirit as well as the letter of the 4th Amendment would be loath to believe that Congress intended to

> authorize one of its subordinate agencies to sweep all our traditions into the fire . . . and to direct *fishing expeditions* into private papers on the possibility that they may disclose evidence of crime . . . . It is contrary to the first principles of justice to allow a search through all the respondents' records, relevant or irrelevant, in the hope that something will turn up.
>
> . . . The analogies of the law do not allow the party wanting evidence to call for all documents in order to see if they do not contain it. Some ground must be shown for supposing that the documents called for do contain it . . . . Some evidence of the materiality of the papers demanded must be produced.
>
> . . . We assume for present purposes that even some part of the presumably large mass of papers . . . may be so connected with charges . . . as to be relevant . . ., but that possibility does not warrant a demand for the whole.

Lunderstadt, 519 A.2d at 413 (Opinion announcing Judgment of the Court) *(quoting FTC. v. American Tobacco Co.*, 264 U.S. 298, 305-307 (1924) (emphasis added in *Lunderstadt*)).

The Committee held one evidentiary hearing, and the sole witness testified that no irregularities or anomalies had been found (Exhibit D). As discussed above, two legislative committees and a Joint State Government Commission investigated the past two elections. *See* House Statement Government Committee (Exhibit F); Special Committee on Election Integrity and Reform (Exhibit G); and Joint State Government Commission created by the General Assembly (Exhibit H). None of them produced evidence to support allegations of systematic voter fraud.

Moreover, litigants (including some Committee members) raised allegations of fraud and other election improprieties in dozens of lawsuits in 2020, none of which resulted in findings sustaining the allegations. In rejecting one of the last election challenges, Judge Bibas of the U.S Third Circuit Court of Appeals observed that, "calling an election unfair does not make it so." *Donald J. Trump for President, Inc. v. Secretary, Com. Of Pennsylvania*, 830 Fed. Appx. 377, 381 (3d Cir. 2020). That observation also summarizes the outcome of the approximately 30 lawsuits challenging different aspects of the Pennsylvania 2020 election that were filed before, during and immediately after Election Day. *See* Exhibit J, and discussion on pp. 8-9, *supra*, of this Brief.

Again, if allegations were sufficient to overcome constitutional rights, then constitutional rights would be illusory. Anyone can make an allegation. Indeed, one who wanted to conduct an investigation could himself make or provoke such allegations in order to justify the investigation he seeks. An allegation by itself does not justify intrusion of a single person's constitutional rights, let alone the constitutional rights of nine million Pennsylvania voters. Where the requesting entity fails to present evidence supporting its interest in constitutionally-protected information, this Court has not hesitated to prevent the disclosure of that information. *See Pennsylvania State Education Ass'n by Wilson v. Commonwealth*, 981 A.2d 383, 386 (Pa. Commw. 2009).

Nor has the Committee offered any evidence to explain why voters' constitutionally-protected personal information is necessary for any such investigation. In prior investigations, the investigating bodies did not seek the information now sought by the Committee. Moreover, any purported explanation falls flat. If the purpose is to look for duplicate registrations, that comparison can be done without transferring the information outside of the SURE system, where it currently is securely housed (Exhibit I, ¶29). Therefore, this purpose does not justify the Subpoena. If the purpose is to look for fake registrations, that would entail an investigation into specific voters. Unless the Committee intends to investigate each and every voter, then the Subpoena is overbroad. And if the Committee is serious about investigating all, or even a portion of, Pennsylvania's nine million registered voters, the effort would require a massive amount of staff, and for that reason alone would expose voter's private information to great risk of further disclosure (Exhibit I, ¶29).

The mere fact that others have conducted investigations into the November 2020 election and May 2021 primary cuts against any legitimate interest in yet another investigation. And the fact that these prior investigations did not require the subpoenaed information undermines any legitimate need for that information. At least one court already has found that Social Security numbers were unnecessary for a similar investigation. *Greidinger v. Davis*, 988 F.2d 1344, 1354

n.19 (4th Cir. 1993) ("Virginia's interest in preventing voter fraud and participation could easily be met without the disclosure of SSN and the attendant possibility of a serious invasion of privacy that could result from that disclosure. Most assuredly, an address or DOB would sufficiently distinguish among voters that share a common name.").

Because the Committee has no factual basis for its purported interest, and cannot establish that the subpoenaed information is necessary, the Committee fails to meet the exacting standard to justify access to this private information. The Committee has not demonstrated and cannot demonstrate ANY legitimate interest, let alone a compelling interest.

2. Voters' Interests Significantly Outweigh Any Interest of the Committee

Because the Committee fails to meet its burden of showing a compelling or significant interest in the information--indeed it has shown no legitimate interest at all--no balancing of interests is even necessary. However, even if the Committee could demonstrate some minimal interest, such interest is far outweighed by the voters' privacy interests in their personally-identifying information.

The interest of the Intervenor-Petitioners and their members and constituents is significant--"the most comprehensive of rights and the right most valued by civilized [people]." *Denoncourt*, 470 A.2d at 948-49 (Pa. 1983) (*quoting Olmstead*

v. United States, 277 U.S. 438, 478 (1928) (dissenting opinion of J. Brandeis)). Pennsylvania courts repeatedly have referenced the "strong" privacy right in Pennsylvania, even stronger than that provided by the U.S. Constitution. *See, supra*, section II(A) of this Brief.

The disclosure of the subpoenaed information carries significant risks. Voters' private information can be disclosed through numerous mechanisms, including hacking, phishing or other Social engineering methods, breaches of physical security, bribery, extortion, or insider attacks (Exhibit I, ¶22). The risk to individuals from disclosure of sensitive personally-identifying information is that thieves can create false accounts in individuals' names, access bank accounts or medical records, incur debt in a person's name, and cause other severe disruptions to an individual's life. The subpoenaed information allows criminals to pose as the individual and assume their identity, thus creating havoc (Exhibit I, ¶18). In particular, a criminal could use the name address, zip code and last 4 digits of your Social Security number to access credit card information and bank accounts (Exhibit I, ¶19). The Committee has provided no assurances that it can comply with standards for protecting this sensitive information (Exhibit I, ¶¶24, 28). Further, the Committee's failure to clearly identify who would have access to this information, and its stated intention to use third party contractors, makes the risks even greater (Exhibit I, ¶30). *See also* Darrow & Lichtenstein, *Do you Really Need*

My Social Security Number?, 10 N.C.J.L. & Tech. at 17 (discussing dangers of outsourcing to contractors and business partners).

In the face of these privacy rights and risks, the Committee must come forward with something more than unsubstantiated allegations. It has not done so. A general interest in improving election law or preventing fraud, without any factual basis to show that fraud is occurring, cannot outweigh, and is not a basis for infringing, constitutional rights.

3. Even if the Committee Musters Some Evidence to Support a Legitimate Interest, the Subpoenas Are Not Narrowly Tailored, and There are Reasonable, Less-Intrusive Means That Serve Any Such Interest.

The Committee purportedly is requesting the personally-identifying information of all nine million registered voters in Pennsylvania in order to "verify the identity" of unidentified voters about whom it has unspecified "questions." Even if there were a factual basis (rather than just "questions") to believe that ineligible voters cast votes in certain voting precincts, the collection of personal information for every registered voter in the Commonwealth would be a grossly overbroad method of identifying those supposed voters. *Lunderstadt*, 519 A.2d at 413 ("We assume for present purposes that even some part of the presumably large mass of papers . . . may be so connected with charges . . . as to be relevant . . ., but that possibility does not warrant a demand for the whole", *quoting FTC. v. American*

Tobacco Co., 264 U.S. 298, 305-307 (1924)). *See also Chester Hous. Auth.*, 173 A.3d at 1252 (providing information in a less intrusive manner and finding further response "not constitutionally justified").

If the Committee were to offer evidence of voting irregularities in, for example, Precinct 1 of Dauphin County, then depending on the level of evidence presented, perhaps the Committee could argue that it had a legitimate interest in accessing private information of certain voters within that precinct. The Committee has not even tried to make such a showing. But even in that hypothetical, the Committee could pursue its purposes through less intrusive means—for example, by collecting names, addresses and dates of birth only, or by asking the Department of State to investigate.

The Committee offers no basis for assessing whether the Subpoena is narrowly tailored to any purported interest. Instead, it ignores the voters' interests altogether, and has assumed blindly that it is entitled to the private information of every single registered voter in the Commonwealth. This dramatic overreach is unparalleled.

This overreach is all the more concerning because of the lack of factual basis for the allegations. The Committee should be required to produce the factual basis for the Subpoena. Assuming the Committee can establish some factual basis, only

then can the parties and the Court determine if the Subpoena is appropriately tailored to serve that interest and does not outweigh voters' constitutional rights.

III. Conclusion

If the Attorney General were to allege that the Committee is conducting this "investigation" for purely partisan purposes, and not for any legitimate legislative purpose, would the Attorney General be entitled to commence an investigation and access the private communications of each Committee member to assess the truth of that allegation? Would the Committee not demand that the Attorney General provide some "probable cause" or other evidence beyond a mere allegation before his request could be granted? Allowing investigations into highly sensitive personal information based on nothing more than unsubstantiated allegations would set a dangerous precedent, and would undercut substantially well-recognized and highly valued individual liberties. The precedent this Subpoena would establish cannot be overstated.

The Committee has not met, and cannot meet, its burden of showing a significant or compelling interest in the constitutionally-protected personal information of nine million Pennsylvanians. The Committee has not identified any factual basis for its asserted interest, offering instead only unsubstantiated allegations, which, as a matter of law, cannot overcome constitutional rights. Nor

can the Committee satisfy its burden of showing that its Subpoena is narrowly tailored to meet any legitimate interest. Summary relief is appropriate, and Intervenor-Petitioners request that the Court grant the relief requested in their Petition for Review.

Dated: October 13, 2021

Witold J. Walczak (PA I.D. No. 62976)
AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA
P.O. Box 23058
Pittsburgh, PA 15222
Tel: (412) 681-7736
vwalczak@aclupa.org

Marian K. Schneider (Pa. I.D. No. 50337)
AMERICAN CIVIL LIBERTIES UNION OF PENNSYLVANIA
P.O. Box 60173
Philadelphia, PA 19102
mschneider@aclupa.org

Sophia Lin Lakin*
AMERICAN CIVIL LIBERTIES UNION FOUNDATION
125 Broad Street, 18th Floor
New York, NY 10004
Tel.: (212) 549-2500
slakin@aclu.org

/s/ Keith E. Whitson
Keith E. Whitson (Pa. I.D. No. 69656)
SCHNADER HARRISON SEGAL & LEWIS LLP
2700 Fifth Avenue Place
120 Fifth Avenue
Pittsburgh, PA 15222
Telephone: (412) 577-5220
Facsimile: (412) 577-5190
kwhitson@schnader.com

/s/ Stephen J. Shapiro
Stephen J. Shapiro (Pa. I.D. No. 83961)
SCHNADER HARRISON SEGAL & LEWIS LLP
1600 Market Street, Suite 3600
Philadelphia, PA 19103-7286
(215) 751-2000
sshapiro@schnader.com

Counsel for Roberta Winters, Nichita Sandru, Kathy Foster-Sandru, Robin Roberts, Kierstyn Zolfo, Michael Zolko, Phyllis Hilley, Ben Bowens, League of Women Voters of Pennsylvania; Common Cause Pennsylvania and Make the Road Pennsylvania

**Pro hac vice* forthcoming

CONFIDENTIAL DOCUMENTS CERTIFICATION

I certify that this filing complies with the provisions of the *Public Access Policy of the Unified Judicial System of Pennsylvania: Case Records of the Appellate and Trial Courts* that require filing confidential information and documents differently than non-confidential information and documents.

/s/ Keith E. Whitson
Keith E. Whitson

CERTIFICATE OF COMPLIANCE

I hereby certify that the Brief in Support of Motion for Summary Relief was filed (or attempted to be filed) with the Commonwealth Court of Pennsylvania's PACFile System and is an accurate and complete representation of the paper version of the Brief filed by Intervenor-Petitioners. I further certify that the foregoing Brief complies with the length requirements set forth in Rule 2135(a) of the Pennsylvania Rules of Appellate Procedure as the Brief contains 9,281 words, not including the supplementary matter identified in Rule 2135(b), based on the word count of Microsoft Word 2010, the word processing system used to prepare the brief. It has been prepared in 14-point font.

Respectfully submitted,

SCHNADER HARRISON SEGAL
& LEWIS LLP

By: /s/ Keith E. Whitson
Keith E. Whitson
PA ID No. 69656
E-mail: kwhitson@schnader.com

Fifth Avenue Place, Suite 2700
120 Fifth Avenue
Pittsburgh, PA 15222
Telephone: (412) 577-5220

CERTIFICATE OF SERVICE

I hereby certify that a true and correct copy of the foregoing document was served via PACFile and/or email, this 13th day of October, 2021, upon the following:

Michael J. Fischer
Aimee D. Thompson
Jacob B. Boyer
Stephen R. Kovatis
Pennsylvania Office of Attorney General
1600 Arch Street, Suite 300
Philadelphia, PA 19103
mfischer@attorneygeneral.gov
athomson@attorneygeneral.gov
jboyer@attorneygeneral.gov

Keli M. Neary
Karen M. Romano
Stephen Moniak
Pennsylvania Office of Attorney General
15th floor, Strawberry Square
Harrisburg, PA 17120

John C. Dodds
Morgan, Lewis & Bockius LLP
1701 Market Place
Philadelphia, PA 19103
John.dodds@morganlewis.com

Susan Baker Manning
Morgan, Lewis & Bockius LLP
1111 Pennsylvania Avenue, NW
Washington, DC 20004
Susan.manning@morganlewis.com

Aaron Scherzer
Christine P. Sun
States United Democracy Center
572 Valley Road, No. 43592
Montclair, NJ 07043
aaron@statesuniteddemocracy.org
christine@statesuniteddemocracy.org

Counsel for Petitioners in 322 MD 2021

Matthew H. Haverstick
Joshua J. Voss
Shohin H. Vance
Samantha G. Zimmer
Kleinbard LLC
Three Logan Square
1717 Arch Street, 5th floor.
Philadelphia, PA 19103
mhaverstick@kleinbard.com
jvoss@kleinbard.com
svance@kleinbard.com
szimmer@kleinbard.com

Counsel for Respondents

Tamika N. Washington
LEGIS GROUP LLC
3900 Ford Road, suite B
Philadelphia, PA 19131
twashington@legislawyers.com

Counsel for Petitioners in 323 MD 2021

Clifford B. Levine
Emma Shoucair
Matthew R. Barnes
Dentons Cohen & Grigsby P.C.
625 Liberty Avenue

Pittsburgh, PA 15222-3152
Clifford.Levine@dentons.com
Emma.Shoucair@dentons.com
Matthew.Barnes@dentons.com

Claude J. Hafner, II
Ronald N. Jumper
Shannon A. Sollenberger
Democratic Caucus
Senate of Pennsylvania
Room 535, Main Capitol Building
Harrisburgh, PA 17120
Cj.hafner@pasenate.com
Ron.jumper@pasenate.com
Shannon.sollenberger@pasenate.com

Counsel for Petitioners in 310 MD 2021

/s/ Keith E. Whitson
Keith E. Whitson