IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; KRIS KOBACH, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES; GENERAL SERVICES ADMINISTRATION Defendants.	Civil Action No. _____

PLAINTIFF'S EMERGENCY MOTION FOR A TEMPORARY RESTRAINING ORDER

Pursuant to Rules 7 and 65 of the Federal Rules of Civil Procedure and Local Civil Rule 65.1, Plaintiff Electronic Privacy Information Center ("EPIC") hereby moves this Court for a Temporary Restraining Order prohibiting Defendants from collecting voter roll data from state election officials prior to the completion and public release of a required Privacy Impact Assessment, E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note), and prior to the resolution of EPIC's constitutional privacy claims.

The collection and aggregation of state voter roll data by a federal commission is without precedent. The Commission's pending action would increase the risks to the privacy of millions of registered voters—including in particular military families whose home addresses would be revealed—and would undermine the integrity of the federal election system. Further, the request

for partial Social Security Numbers that are often used as default passwords for commercial services, coupled with the Commission's plan to make such information "publicly available," is both without precedent and crazy.

The Commission's failure to fulfill its statutory obligation to undertake a Privacy Impact Assessment prior to sending requests to state election officials underscores the urgent need for relief. EPIC accordingly requests, as an immediate remedy, that the Court safeguard the privacy interests of registered voters and maintain the *status quo* while more permanent solutions may be considered. EPIC also requests that the Court set an expedited hearing to determine whether such order should remain in place.

This motion is supported by the attached Memorandum in Support of Plaintiff's Emergency Motion for a Temporary Restraining Order, accompanying declarations, exhibits, and any additional submissions that may be considered by the Court.

Respectfully Submitted,

/s/ Marc Rotenberg
Marc Rotenberg, D.C. Bar # 422825
EPIC President and Executive Director

Alan Butler, D.C. Bar # 1012128
EPIC Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: July 3, 2017

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; KRIS KOBACH, in his official capacity as Vice Chair of the Presidential Advisory Commission on Election Integrity; EXECUTIVE OFFICE OF THE PRESIDENT OF THE UNITED STATES; OFFICE OF THE VICE PRESIDENT OF THE UNITED STATES; GENERAL SERVICES ADMINISTRATION

Defendants.

Civil Action No. _____

MEMORANDUM IN SUPPORT OF PLAINTIFF'S EMERGENCY MOTION FOR A TEMPORARY RESTRAINING ORDER

INTRODUCTION

The failure to safeguard personal data gathered by government agencies is a national crisis. In 2015, the personal records of 22 million Americans, including 5 million digitized fingerprints and sensitive background records, were breached. Federal agencies are, understandably, required to take steps to safeguard personal information before collecting new data. Yet the Presidential Advisory Commission on Election Integrity ("PACEI" or the "Commission") has initiated an unprecedented effort to collect millions of state voter records without any effort to protect the privacy interests of those voters. More than two dozen states have already refused to comply. The action is as brazen as it is unlawful.

The Commission has ignored entirely the rules Congress established in the E-Government Act of 2002 and the Federal Advisory Committee Act that would safeguard the personal data sought by the Commission. The Commission was required to prepare and publish a Privacy Impact Assessment that would have addressed the types of information to be collected and the purpose of the collection, as well as how the information would be secured and whether it would be disclosed to others. The Commission's actions also threaten the informational privacy rights guaranteed under the Fifth Amendment and violate the Due Process Clause.

The Commission has already committed two egregious acts: (1) directing state election officials to transmit state voter records to an insecure website and (2) announcing that it will make publicly available the last four digits of the Social Security Numbers of millions of registered voters. Those four numbers are the default passwords for many commercial services and could lead almost immediately to an increase in financial fraud and identity theft.

Registered voters, EPIC, and EPIC's members face immediate and irreparable injury as a result of these violations of law.

EPIC respectfully asks this Court to enter a temporary restraining order prohibiting the Commission from collecting any voter data. The requirements for such an order have been met: EPIC is likely to succeed on the merits of its claim that the collection is unlawful. EPIC's members will be irreparably harmed by the collection of their personal information by the Commission without adequate safeguards. The Commission has not identified any interest that would outweigh those harms, and the public interest clearly favors preserving the status quo pending proper review and the establishment of voter privacy safeguards.

FACTUAL BACKGROUND

A. The Privacy Threat of Massive Voter Databases

Computer experts have long raised concerns about the collection of sensitive voter information in insecure databases. *E.g.*, Barbara Simons, *Voter Registration and Privacy* (2005);[1] EPIC, Comment Letter on U.S. Election Assistance Commission Proposed Information Collection Activity (Feb. 25, 2005).[2] Election officials "face many technical challenges in implementing [voter registration] databases in a secure, accurate, and reliable manner, while protecting sensitive information and minimizing the risk of identity theft." Simons, *supra*, at 10. Voter registration databases "are complex systems," and "[i]t is likely that one or more aspects of the technology will fail at some point." Ass'n for Comput. Machinery, *Statewide Databases of Registered Voters: Study of Accuracy, Privacy, Usability, Security, and Reliability Issues* 6 (Feb. 2006).[3] Moreover, merging data from multiple sources "can, if not properly handled, undermine the accuracy of the voter registration data." Simons, *supra*, at 12.

Recent events underscore the privacy risks inherent in assembling a nationwide voter database. In June 2017, political consulting firm Deep Root Analytics was found to have left

[1] https://epic.org/events/id/resources/simons.ppt.
[2] https://epic.org/privacy/voting/register/eac_comments_022505.html.
[3] https://people.eecs.berkeley.edu/~daw/papers/vrd-acm06.pdf.

198,000,000 voter files unprotected on the Internet for weeks. Brian Fung et al., *A Republican Contractor's Database of Nearly Every Voter Was Left Exposed on the Internet for 12 Days, Researcher Says*, Wash. Post (June 19, 2017).[4] The files included "billions of data points" such as names, addresses, birth dates, phone numbers, and voting histories. *Id.* The researcher who discovered the cache described the alarming implications of exposing such a large accumulation of voter information to the public: "With this data you can target neighborhoods, individuals, people of all sorts of persuasions . . . . I could give you the home address of every person the RNC believes voted for Trump." *Id.*

B. The Establishment of the Commission

The Presidential Advisory Commission on Election Integrity was established by executive order on May 11, 2017. Exec. Order No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017), Ex. 1. The Vice President is named as the Chair of the Commission, "which shall be composed [sic] of not more than 15 additional members." *Id*. Additional members are appointed by the President, and the Vice President may select a Vice Chair of the Commission from among the members. *Id*. Vice President Pence has named Kansas Secretary of State Kris Kobach to serve as Vice Chair of the Commission.

The Commission was asked to "*study* the registration and voting processes used in Federal elections." *Id.* (emphasis added). The Commission was further asked to identify "(a) those laws, rules, policies, activities, strategies, and practices that enhance the American people's confidence in the integrity of the voting processes used in Federal elections; (b) those laws, rules, policies, activities, strategies, and practices that undermine the American people's confidence in the integrity of the voting processes used in Federal elections; and (c) those vulnerabilities in

[4] https://www.washingtonpost.com/news/the-switch/wp/2017/06/19/republican-contractor-database-every-voter-exposed-internet-12-days-researcher-says/.

voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting, including fraudulent voter registrations and fraudulent voting." *Id*.

There is no authority in the Executive Order to subpoena records, to undertake investigations, or to demand the production of state voter records from state election officials.

C. The Commission's Request/Demand for State Voter Records

On June 28, 2017, the Vice Chair of the Commission undertook to collect detailed voter histories from all fifty states and the District of Columbia. Such a request to state election officials had never been made by any federal official before. The Vice Chair stated during a phone call with PACEI members that "a letter w[ould] be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls . . . ." Ex. 2. One of these letters, dated June 28, 2017, was sent to North Carolina Secretary of State Elaine Marshall. Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017), Ex. 3 ("Commission Letter"). In the letter, Kobach asked Marshall to provide to the Commission

> the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas citizen information.

Id. at 1–2.

The Commission sought from the states sensitive personal information. For example, the improper collection of Social Security Numbers ("SSNs") is a major contributor to identity theft in the United States. Soc. Sec. Admin., *Identity Theft and Your Social Security Number* (Feb.

2016).[5] "An estimated 17.6 million Americans—about 7% of U.S. residents age 16 or older—were victims of identity theft in 2014." Erika Harrell, Bureau of Justice Statistics, *Victims of Identity Theft, 2014* at 1 (Sept. 2015).[6] U.S. victims of identity theft lost a collective total of $15.4 billion in the same year. *Id.* at 7.

Collecting and publishing the home addresses of current and former military personnel also poses privacy and security risks. The U.S. Military routinely redacts "names, social security numbers, personal telephone numbers, home addresses and personal email addresses" of military personnel in published documents, "since release would constitute a clearly unwarranted invasion of their personal privacy." U.S. Pacific Fleet, *Report of the Court of Inquiry* (2001);[7] *see also* Def. Logistics Agency, *Defense Logistics Agency Instruction 6303* at 9, 14 (2009)[8] (noting that military home addresses are "For Official Use Only" and must be redacted prior to public release of documents); Jason Molinet, *ISIS hackers call for homegrown 'jihad' against U.S. military, posts names and addresses of 100 service members*, N.Y. Daily News (Mar. 21, 2015).[9]

In the Commission Letter, the Vice Chair warned that "any documents that are submitted to the full Commission w[ould] also be made available to the public." Commission Letter 2. The Vice Chair expected a response from the states by July 14, 2017—approximately ten business days after the date of the request—and instructed that the State Secretary could submit her responses "electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange" system. *Id*. Neither the email address nor the file exchange system proposed by

[5] https://www.ssa.gov/pubs/EN-05-10064.pdf.
[6] https://www.bjs.gov/content/pub/pdf/vit14.pdf.
[7] http://www.cpf.navy.mil/subsite/ehimemaru/legal/GREENEVILLE_FOIA_exemption.pdf.
[8] http://www.dla.mil/Portals/104/Documents/J5StrategicPlansPolicy/PublicIssuances/i6303.pdf.
[9] http://www.nydailynews.com/news/national/isis-hackers-call-jihad-u-s-military-article-1.2157749.

the Commission provides a secure mechanism for transferring sensitive personal information. In fact, an attempt to access the File Exchange system linked in the letter leads to a warning screen with a notification that the site is insecure. *See* Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Site (July 3, 2017 12:02 AM), Ex. 6.

Similar letters were sent to election officials in the other 49 states and the District of Columbia.

D. The States Have Opposed the Commission's Request

Officials in at least two dozen states have partially or fully refused to comply with the Commission Letter. Philip Bump & Christopher Ingraham, *Trump Says States Are 'Trying to Hide' Things from His Voter Fraud Commission. Here's What They Actually Say*, Wash. Post (July 1, 2017).[10] California Secretary of State Alex Padilla stated on June 29, 2017, that he would "not provide sensitive voter information to a committee that has already inaccurately passed judgment that millions of Californians voted illegally. California's participation would only serve to legitimize the false and already debunked claims of massive voter fraud." Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017).[11] Kentucky Secretary of State Alison Lundergan Grimes stated on June 29, 2017, that "Kentucky w[ould] not aid a commission that is at best a waste of taxpayer money and at worst an attempt to legitimize voter suppression efforts across the country." Bradford Queen, Secretary Grimes Statement on Presidential Election

[10] https://www.washingtonpost.com/news/wonk/wp/2017/07/01/trump-says-states-are-trying-to-hide-things-from-his-voter-fraud-commission-heres-what-they-actually-say/.
[11] http://www.sos.ca.gov/administration/news-releases-and-advisories/2017-news-releases-and-advisories/secretary-state-alex-padilla-responds-presidential-election-commission-request-personal-data-california-voters/.

Commission's Request for Voters' Personal Information, Kentucky (last accessed July 3, 2017).[12] Virginia Governor Terry McAuliffe stated on June 29, 2017, that he had "no intention of honoring [Kobach's] request." Terry McAuliffe, *Governor McAuliffe Statement on Request from Trump Elections Commission* (June 29, 2017).[13]

E. The Commission's Failure to Conduct a Privacy Impact Assessment

Under the E-Government Act of 2002, any agency "initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual" is required to complete a privacy impact assessment ("PIA") before initiating such collection. Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note). The agency must:

> (i) [C]onduct a privacy impact assessment; (ii) ensure the review of the privacy impact assessment by the Chief Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means.

Id. Under the Federal Advisory Committee Act:

> [R]ecords, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by each advisory committee shall be available for public inspection and copying at a single location in the offices of the advisory committee or the agency to which the advisory committee reports until the advisory committee ceases to exist.

5 U.S.C. app. 2 § 10(b). The Commission has not conducted a privacy impact assessment for its collection of state voter data. The Commission has not ensured review of a PIA by any Chief

[12] http://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prId=129.
[13] https://governor.virginia.gov/newsroom/newsarticle?articleId=20595.

Information Officer or equivalent official. The Commission has not made such a PIA available to the public. Complaint ¶¶ 32–34.

STANDARD OF REVIEW

In order to obtain a temporary restraining order or preliminary injunction, a plaintiff must show that (1) they are likely to succeed on the merits, (2) they are likely to suffer irreparable harm in the absence of preliminary relief, (3) that the balance of the equities tips in their favor, and (4) that an injunction is in the public interest. *Sherley v. Sebelius*, 644 F.3d 388, 392 (D.C. Cir. 2011) (quoting *Winter v. NRDC*, 555 U.S. 7, 20 (2008)). Both temporary restraining orders and preliminary injunctions are extraordinary remedies that "should be granted only when the party seeking relief, by a clear showing, carries the burden of persuasion." *Lofton v. District of Columbia*, 7 F. Supp. 3d 117, 120 (D.D.C. 2013). The D.C. Circuit has adopted a "sliding scale" approach when evaluating these injunction factors. *Sherley*, 644 F.3d at 392. Thus if the "movant makes an unusually strong showing on one of the factors, then it does not necessarily have to make a strong showing on another factor." *Davis v. Pension Benefit Guar. Corp.*, 571 F.3d 1288, 1291–92 (D.C. Cir. 2009). *But see League of Women Voters of U.S. v. Newby*, 838 F.3d 1, 7 (D.C. Cir. 2016) (noting that the court has "not yet decided" whether the sliding scale approach applies post-*Winter*).

ARGUMENT

This case presents the type of extraordinary circumstance that justifies a temporary restraining order. Absent a prohibition from this Court, the Commission will begin collecting and aggregating the sensitive, personal information of voters across the country in less than two weeks without any procedures in place to protect voter privacy or the security and integrity of the state voter data. There is already evidence in the record that the Commission has placed and will place voter data at risk.

First and foremost, this proposed collection violates a core provision of the E-Government Act of 2002, which requires that agencies establish sufficient protections *prior* to initiating any new collection of personal information using information technology. The Commission's actions also violate voters' Fifth Amendment right to informational privacy and, through their implementation, violate the Administrative Procedure Act (APA). Second, this collection and aggregation of sensitive personal information, as well as the exposure of this voter data through insecure systems with no protections in place, will cause irreparable harm to EPIC's members. Once data has been leaked, there is no way to control its spread. With a data breach, there is literally no way to repair the damage, once done. Third, the balance of the equities tips in EPIC's favor because the Commission will suffer no hardship if the collection is enjoined pending the completion of a privacy assessment as required under federal law. The Commission's mandate is to "study" election integrity. It has no authority to investigate or to gather state voter records. There is nothing that would justify the immediate collection of this voter data. Indeed, it is in the public interest to prevent any disruption or interference with states' voter registration systems. The integrity of state voting systems is of paramount importance and should not be put at risk at the whim of the Commission members.

A. EPIC is likely to succeed on the merits of its claims.

1. The collection of state voter data violates the E-Government Act and the APA

The Commission has made no attempt to comply with the Privacy Impact Assessment requirements of Section 208 of the E-Government Act of 2002, Pub. L. 107-347, 115 Stat. 2899, Title II § 208 (codified at 44 U.S.C. § 3501 note), which are clearly applicable to the collection of sensitive, personal information from state voter databases. The Commission's actions therefore violate the Administrative Procedures Act ("APA"), 5 U.S.C. § 706(2)(A). EPIC is likely to succeed on its statutory claims.

As the Department of Justice has explained, "Privacy Impact Assessments ("PIAs") are required by Section 208 of the E-Government Act for all Federal government agencies that develop or procure new information technology involving the collection, maintenance, or dissemination of information in identifiable form or that make substantial changes to existing information technology that manages information in identifiable form." Office of Privacy & Civil Liberties, U.S. Dep't of Justice, *E-Government Act of 2002* (June 18, 2014).[14] A Privacy Impact Assessment is "an analysis of how information is handled: (i) to ensure handling conforms to applicable legal, regulatory, and policy requirements regarding privacy, (ii) to determine the risks and effects of collecting, maintaining and disseminating information in identifiable form in an electronic information system, and (iii) to examine and evaluate protections and alternative processes for handling information to mitigate potential privacy risks." Joshua B. Bolten, Director, Office of Mgmt. & Budget, Executive Office of the President, M-03-22, Memorandum for Heads of Executive Departments and Agencies, Attachment A (Sept. 26, 2003) [hereinafter Bolten Memo], Ex. 5.

The E-Government Act requires that an agency "shall take actions described under subparagraph (B)" of Section 208 "before . . . initiating a new collection of information that—(I) will be collected, maintained, or disseminated using information technology; and (II) includes any information in an identifiable form permitting the physical or online contacting of a specific individual, if identical questions have been posed to, or identical reporting requirements imposed on, 10 or more persons, other than agencies, instrumentalities, or employees of the Federal Government." E-Government Act § 208(b)(1)(A)(ii). The actions described in subparagraph (B), which the Commission must take *before* collecting this information, include "(i) conduct[ing] a privacy assessment; (ii) ensur[ing] the review of the privacy impact assessment by the Chief

[14] https://www.justice.gov/opcl/e-government-act-2002.

Information Officer, or equivalent official, as determined by the head of the agency; and (iii) if practicable, after completion of the review under clause (ii), mak[ing] the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means." E-Government Act § 208(b)(1)(B).

The Commission has already "initiated a new collection" of personal information, but it has not complied with any of these requirements. The APA prohibits federal agencies from taking any action that is "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2). The Commission's actions are "not in accordance with law." The APA authorizes this Court to "compel agency action unlawfully withheld." 5 U.S.C. § 706(1). Such a claim may proceed "where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required to take.*" *Norton v. S. Utah Wildlife Alliance*, 542 U.S. 55, 64 (2004). An agency's failure to comply with the PIA requirements of the E-Government Act is reviewable under both provisions of APA § 706. *Fanin v. Dep't of Veteran Affairs*, 572 F.3d 868, 875 (11th Cir. 2009).

The E-Government Act defines "information technology" as "any equipment or interconnected system . . . used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly . . . ." 40 U.S.C. § 11101(6); *see* 44 U.S.C. § 3501 note, § 201 (applying definitions from 44 U.S.C. §§ 3502, 3601); 44 US.C. § 3502(9) (applying the definition of 40 U.S.C. § 11101(6)). Courts have found that a "minor change" to "a system or collection" that does not "create new privacy risks," such as the purchasing of a new external hard drive, would not require a PIA. *Perkins v. Dep't of Veteran Affairs*, No. 07-310, at *19

(N.D. Ala. Apr. 21, 2010) (quoting Bolten Memo § II.B.3.f). However, an agency is obligated to conduct a PIA before initiating a new collection of data that will be "collected, maintained, or disseminated using information technology" whenever that data "includes any information in identifiable form permitting the physical or online contacting of a specific individual" and so long as the questions have been posed to 10 or more persons. E-Government Act § 208(b)(1)(A)(ii). The term "identifiable form" means "any representation of information that permits the identity of an individual to whom the information applies to be reasonably inferred by either direct or indirect means." E-Government Act § 208(d).

There is no question that the PIA requirement applies in this case. The Commission's decision to initiate collection of comprehensive voter data by requesting personal information from Secretaries of State of all 50 states and the District of Columbia, including sensitive, personal information about hundreds of millions of voters, triggers the obligations of § 208(b)(1)(A)(ii) of the E-Government Act. The letter sent by Commission Vice Chair Kobach requests that the Secretary of State provide "voter roll data" including "the full first and last names of all registrants, middle names or initials if available, addresses, dates of birth, political party (if recorded in your state), last four digits of social security number if available, voter history (elections voted in) from 2006 onward, active/inactive status, cancelled status, information regarding any felony convictions, information regarding voter registration in another state, information regarding military status, and overseas information." Commission Letter 1–2. The states are instructed to submit their "responses *electronically* to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE")," a government website used to transfer files. *Id.* (emphasis added).[15] This sensitive voter roll data is

[15] The government file exchange website is not actually "safe." In fact, any user who follows the link provided in the Commission Letter will see a warning that the site is insecure. Ex 6.

precisely the type of "personal information" in "identifiable form" that the PIA provision was intended to protect, and the transfer of large data files via email or otherwise clearly involves the use of information technology.

As the court explained in *Perkins*, PIAs are necessary to address "(1) what information is collected and why, (2) the agency's intended use of the information, (3) with whom the information would be shared, (4) what opportunities the [individuals] would have to decline to provide information or to decline to share the information, (5) how the information would be secured, and (6) whether a system of records is being created." *Id. See* E-Government Act § 208(b)(2)(B); Bolten Memo § II.C.1.a. These types of inquiries are "certainly appropriate and required" when an agency "initially created" a new database system and "began collecting data." *Perkins*, No. 07-310, at *19–20.

The APA defines "agency" as "each authority of the Government of the United States, whether or not it is within or subject to review by another agency," but excludes from the definition 8 specific types of entities not relevant to this case. 5 U.S.C. § 701(b). The E-Government definition provided in 44 U.S.C. § 3502, E-Government Act § 201, is even broader than the APA definition and includes "any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency, but does not include (A) the Government Accountability Office; (B) Federal Election Commission; (C) the governments of the District of Columbia and of the territories and possessions of the United States, and their various subdivisions; or (D) Government-owned contractor-operated facilities, including laboratories engaged in national defense research and production activities." Under both definitions, the Commission is an

"agency" and was therefore required to conduct a PIA prior to initiating the collection of voter data.

2. The publication of voters' personal information violates the constitutional right to informational privacy

The Supreme Court has long recognized that individuals have a constitutionally protected interest in "avoiding disclosure of personal matters." *Whalen v. Roe*, 429 U.S. 589, 599 (1977); *accord Nixon v. Administrator of Gen. Servs.*, 433 U.S. 425, 457 (1977). The constitutionality of a "government action that encroaches upon the privacy rights of an individual is determined by balancing the nature and extent of the intrusion against the government's interest in obtaining the information it seeks." *United States v. District of Columbia*, 44 F. Supp. 2d 53, 60–61 (D.D.C. 1999). The "individual interest in protecting the privacy of information sought by the government" is more important when that information is to be "disseminated publicly." *Am. Fed'n of Gov't Emps., AFL-CIO v. HUD*, 118 F.3d 786, 793 (D.C. Cir. 1997) [hereinafter *AFGE v. HUD*] (assuming without concluding that the right exists).

The Government has previously survived right to informational privacy challenges where it implemented measures to protect the confidentiality and security of the personal information that it was collecting or there was a federal law that provided substantial protection. *See id.* (upholding collection of personal information by HUD on the SF 85P form); *NASA v. Nelson*, 562 U.S. 134, 156 (2011). But when no such safeguards exist, when the Government has not "evidence a proper concern" for individual privacy, the individual's interest in prohibiting the collection of their information by an agency is strongest. *NASA*, 562 U.S. at 156. That is especially true when the data includes identifying and sensitive information such as addresses, date of birth, SSNs, and political affiliations.

The Commission has taken no steps to protect this sensitive personal information that they are seeking to collect. Instead, they have disclaimed all responsibility for maintaining the security and confidentiality of these records. In the letter to Secretaries of State, Vice Chair Kobach tells the states to "be aware that any documents that are submitted to the full Commission will also be made available to the public." Commission Letter 2. The Commission has provided no justification for such broad collection and disclosure of voters' personal information. In the letter, the Vice Chair claims, without any supporting evidence, that the data will be used to "analyze vulnerabilities and issues related to voter registration and voting." Commission Letter 1. But the Office of the Vice President and the Commission have no authority to oversee state voter registration, and the Executive Order makes clear that the purpose of the Commission is to "study" election integrity.

Informational privacy claims merit heightened scrutiny. *See, e.g.*, *Eisenbud v. Suffolk County*, 841 F.2d 42, 45 (2d Cir. 1988); *Fraternal Order of Police, Lodge 5, v. City of Philadelphia*, 812 F.2d 105, 110 (3d Cir. 1987). This requires a "delicate task of weighing competing interests," *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 578 (3d Cir. 1980). *See Doe v. Attorney General*, 941 F.2d 780 (9th Cir. 1991). In order to overcome the constitutional obligation to protect personal information from disclosure, the government must demonstrate "sufficiently weighty interests in obtaining the information sought" and "justify the intrusions into the individuals' privacy." *AFGE v. HUD*, 118 F.3d at 793. The Commission has not identified any legitimate interests that would justify such a sweeping and unprecedented public disclosure of voter records.

B. EPIC's members will suffer irreparable harm if relief is not granted.

If the Court does not enjoin the Commission's unlawful collection, aggregation, and public disclosure of voter data, EPIC's members will be irreparably harmed. Individual voter

data is not broadly available to the public; otherwise there would be no need for the Commission to request it from the states. These records are collected by the states for a specific purpose—voter registration—and voters have not authorized its dissemination to or by the Commission for an entirely different, and undisclosed, purpose. The unauthorized disclosure of this sensitive personal information would cause immeasurable harm that would be impossible to repair because once this data is publicly available there is no way to control its spread or use.

A violation of the constitutional right to informational privacy, alone, is sufficient to satisfy the irreparable harm test. *Fort Wayne Women's Health v. Bd. of Comm'rs, Allen County, Ind.*, 735 F. Supp. 2d 1045, 1061 (N.D. Ind. 2010). *See Am. Fed'n of Gov't Emps., AFL-CIO v. Sullivan*, 744 F. Supp. 294, 298 (D.D.C. 1990). But the disclosure of personal identifying information itself also gives rise to an irreparable injury. *Does v. Univ. of Wash.*, No. 16-1212, 2016 WL 4147307, *slip op.* at *2 (W.D. Wash. Aug. 3, 2016). "In the age of the internet, when information is made public quickly and without borders, it is nearly impossible to contain an impermissible disclosure after the fact, as information can live on in perpetuity in the ether to be shared for any number of deviant purposes." *Wilcox v. Bastiste*, No. 17-122, 2017 WL 2525309, *slip op.* at *3 (E.D. Wash. June 9, 2017); *see also Pacific Radiation Oncology, LLC v. Queen's Medical Center*, 47 F. Supp. 3d 1069, 1076 (D. Haw. 2014) (noting that it is "beyond dispute that the public disclosure of that information" in medical files would subject patients "to potential irreparable harm").

Even the mere collection and aggregation of the state voter data would cause an irreparable harm to EPIC's members because the Commission has refused to adopt measures to ensure the privacy and security of that data as required by law. Instead, the Commission has encouraged the states to use insecure tools to transfer voters' sensitive personal information. The

Commission has also failed to assess or disclose how the data will be handled and secured once it is collected. Given the recent history of data breaches in federal government systems that house sensitive information, the lack of planning and foresight on the part of the Commission poses an immediate and inexcusable risk to the privacy of all voters.

C. The balance of the equities and public interest favor relief.

The balance of the equities and public interest factors favor entry of the temporary restraining order that EPIC seeks. This purpose of temporary relief is to preserve, not "upend the status quo." *Sherley v. Sebelius*, 644 F.3d 388, 398 (D.C. Cir. 2011); *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 43 (2008). Preserving the status quo is the purpose of EPIC's motion. Currently there is no single federal database that houses state voter roll data. The Commission now seeks in an unprecedented shift to change that fact without prior review of the privacy implications as required by law. The public interest and balance of the equities favor EPIC's request to preserve the status quo pending review by this Court.

There are no countervailing interests that weigh against the relief EPIC seeks. The Commission would not be harmed by a temporary halt to its plans, as it has no valid interest in violating the PIA requirements in the E-Government Act. "There is generally no public interest in the perpetuation of unlawful agency action." *League of Women Voters*, 838 F.3d at 12 (citing *Pursuing America's Greatness v. FEC*, 831 F.3d 500, 511-12 (D.C. Cir. 2016); *Gordon v. Holder*, 721 F.3d 638, 653 (D.C. Cir. 2013)). In fact, "there is a substantial public interest in having governmental agencies abide by the federal laws that govern their existence and operations." *Id.* at 12.

The Commission's actions cut directly against the stated mission to "identif[y] areas of opportunity to increase the integrity of our election systems." Commission Letter 2. By collecting and aggregating detailed, sensitive personal voter information without first conducting

a PIA, the Commission is threatening the security and integrity of the entire voting system. This action will not only put voter data at risk; it will risk disincentivizing voters in a way similar to the restrictive documentation requirements in *League of Women Voters*. The court the found that the requirement to reveal "sensitive citizenship documents" in order to register to vote caused the voter registration numbers to "plummet[]" and found that there was a strong public interest in favor of enjoining the change. *League of Women Voters*, 838 F.3d at 4, 9, 13. The right to vote is "preservative of all rights" and of "most fundamental significance under our constitutional structure." *Id.* at 12. The Commission has not provided any evidence that the collection and aggregation of sensitive voter data would "increase the integrity of our election systems." More likely, it will have the opposite effect.

CONCLUSION

The Emergency Motion for a Temporary Restraining Order should be granted, and Defendants should be restrained from collecting state voter data prior to the completion of a Privacy Impact Assessment.

Respectfully Submitted,

/s/ Marc Rotenberg
Marc Rotenberg, D.C. Bar # 422825
EPIC President and Executive Director

Alan Butler, D.C. Bar # 1012128
EPIC Senior Counsel

ELECTRONIC PRIVACY
INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009
(202) 483-1140 (telephone)
(202) 483-1248 (facsimile)

Dated: July 3, 2017