Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable Matt Dunlap
Secretary of State
148 State House Station
Augusta, ME 04333

Dear Secretary Dunlap,

I serve as the Vice Chair for the Presidential Advisory Commission on Election Integrity ("Commission"), which was formed pursuant to Executive Order 13799 of May 11, 2017. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President of the United States that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine the American people's confidence in the integrity of federal elections processes.

As the Commission begins it work, I invite you to contribute your views and recommendations throughout this process. In particular:

1. What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections?
2. How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities?
3. What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer?
4. What evidence or information do you have regarding instances of voter fraud or registration fraud in your state?
5. What convictions for election-related crimes have occurred in your state since the November 2000 federal election?
6. What recommendations do you have for preventing voter intimidation or disenfranchisement?
7. What other issues do you believe the Commission should consider?

In addition, in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly-available voter roll data for Maine, including, if publicly available under the laws of your state, 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.

You may submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files. You can access the SAFE site at https://safe.amrdec.army.mil/safe/Welcome.aspx. We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public. If you have any questions, please contact Commission staff at the same email address.

On behalf of my fellow commissioners, I also want to acknowledge your important leadership role in administering the elections within your state and the importance of state-level authority in our federalist system. It is crucial for the Commission to consider your input as it collects data and identifies areas of opportunity to increase the integrity of our election systems.

I look forward to hearing from you and working with you in the months ahead.

Sincerely,

Kris Kobach

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009

Plaintiff,

v.

Civ. Action No. 17-1320 (CKK)

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as 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;
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

GENERAL SERVICES ADMINISTRATION
1800 F Street, N.W.
Washington, D.C. 20405

UNITED STATES DEPARTMENT OF DEFENSE
1000 Defense Pentagon
Washington, D.C. 20301-0001

Defendants.

AMENDED COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Administrative Procedure Act ("APA"), 5 U.S.C. §§ 551–706, the Federal Advisory Committee Act ("FACA"), 5 U.S.C. app. 2, and the United States Constitution for injunctive and other appropriate relief to halt the collection of state voter data by

the Presidential Advisory Commission on Election Integrity (the "PACEI" or the "Commission"), by officers of the Commission, and by the agencies which oversee and facilitate the activities of the Commission, including the Department of Defense.

2. The Electronic Privacy Information Center ("EPIC") challenges the Commission's intent to collect the personal data of millions of registered voters and to publish partial SSNs as an unconstitutional invasion of privacy and a violation of the agency's obligation to conduct a Privacy Impact Assessment ("PIA").

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, 5 U.S.C. § 702, and 5 U.S.C. § 704. This Court has personal jurisdiction over Defendants.

4. Venue is proper in this district under 5 U.S.C. § 703 and 28 U.S.C. § 1391.

Parties

5. Plaintiff EPIC is a nonprofit organization incorporated in Washington, D.C., and established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities. EPIC's Advisory Board members include distinguished experts in law, technology, public policy, and cybersecurity. EPIC has a long history of working to protect voter privacy and the security of election infrastructure. EPIC has specific expertise regarding the misuse of the Social Security Number ("SSN") and has sought stronger protections for the SSN for more than two decades.

6. EPIC's members include registered voters in California, the District of Columbia, Florida, Maryland, Massachusetts, Minnesota, New York, Pennsylvania, Texas, and Washington.

7. Defendant PACEI is an advisory committee of the U.S. government within the meaning of FACA, 5 U.S.C. app. 2 § 10. Defendant PACEI is also an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

8. Defendant Michael Pence is the Vice President of the United States and the Chair of the PACEI.

9. Defendant Kris Kobach is the Secretary of State of Kansas and the Vice Chair of the PACEI.

10. Defendant Executive Office of the President of the United States ("EOP") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

11. Defendant Office of the Vice President of the United States ("OVP") is a subcomponent of EOP and an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

12. Defendant General Services Administration ("GSA") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The GSA is charged with providing the PACEI "such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission . . . ." Ex. 1.[1]

13. Defendant United States Department of Defense ("DoD") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The DoD manages and controls the Safe Access File System ("SAFE").

Facts

The Commission's Unprecedented Collection of State Voter Data

14. The Commission was established by Executive Order on May 11, 2017 ("Commission Order"). Ex 1.[2]

[1] Exec. Order. No. 13,799, 82 Fed. Reg. 22,389, 22,390 (May 11, 2017).
[2] 82 Fed. Reg. at 22,389; *see also Voter Privacy and the PACEI*, EPIC.org (June 30, 2017), https://epic.org/privacy/voting/pacei/.

15. The Commission is charged with "study[ing] the registration and voting processes used in Federal elections." Ex. 1.[3] The Commission Order contains no authority to gather personal data or to undertake investigations.[4]

16. 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 had never been made by any federal official in the history of the country. 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.[5]

17. According to the U.S. Census, state voter rolls include the names, addresses, and other personally identifiable information of at least 157 million registered voters.[6]

18. One of the letters from the Commission, dated June 28, 2017, was sent to North Carolina Secretary of State Elaine Marshall. Ex. 3.[7]

19. In the letter ("Commission Letter"), the Vice Chair urged the Secretary of State 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,

---

[3] 82 Fed. Reg. at 22,389.
[4] *See generally id.*
[5] Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017).
[6] U.S. Census Bureau, *Voting and Registration in the Election of November 2016* at tbl. 4a (May 2017), https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html.
[7] Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017).

information regarding voter registration in another state, information regarding military status, and overseas citizen information." Ex. 3.[8]

20. The Commission Letter also asked "[w]hat evidence or information [the state had] regarding instances of voter fraud or registration fraud" and "[w]hat convictions for election-related crimes ha[d] occurred in [the] state since the November 2000 federal election." Ex. 3.[9]

21. The Commission Letter stated that "any documents that are submitted to the full Commission w[ould] also be made available to the public." Ex. 3.[10]

22. The Commission asked for a response by July 14, 2017. Ex. 3.[11] The "SAFE" URL, recommend by the Commission for the submission of voter data, leads election officials to a non-secure site. Regarding this website, Google Chrome states: "Your connection is not private. Attackers may be trying to steal your information from [the site proposed by the Commission] (for example, passwords, messages, or credit cards)." Ex. 4.[12]

23. As of July 7, 2017, the Department of Defense has received voter data from at least one state, Arkansas, in the SAFE system.

Many States Oppose the Commission's Demand for Personal Voter Data

24. In less than three days following the release of the Commission Letter, election officials in twenty-four states said that they would oppose, partiallly or fully, the demand for personal voter data.[13]

---

[8] *Id.* at 1–2.
[9] *Id.* at 1.
[10] *Id.* at 2.
[11] *Id.*
[12] Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Site (July 3, 2017 12:02 AM).
[13] 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),

25. California Secretary of State Alex Padilla stated 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."[14]

26. Kentucky Secretary of State Alison Lundergan Grimes stated 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."[15]

27. Virginia Governor Terry McAuliffe stated that he had "no intention of honoring [Kobach's] request."[16]

28. More than fifty experts in voting technology and twenty privacy organizations wrote to state election officials to warn that "[t]here is no indication how the information will be used, who will have access to it, or what safeguards will be established."[17]

The Commission's Failure to Conduct a Privacy Impact Assessment

29. Under the E-Government Act of 2002,[18] any agency "initiating a new collection of information that (I) will be collected, maintained, or disseminated using information technology;

---

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/.

[14] Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017), 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/.

[15] Bradford Queen, Secretary Grimes Statement on Presidential Election Commission's Request for Voters' Personal Information, Kentucky (last accessed July 3, 2017) http://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prId=129.

[16] Terry McAuliffe, *Governor McAuliffe Statement on Request from Trump Elections Commission* (June 29, 2017), https://governor.virginia.gov/newsroom/newsarticle?articleId=20595.

[17] Letter from EPIC et al. to Nat'l Ass'n of State Sec'ys (July 3, 2017), https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf.

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.[19]

30. The agency must "(i) conduct 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."[20]

31. The PACEI is an agency subject to the E-Government Act because it is an "establishment in the executive branch of the Government," a category which "includ[es] the Executive Office of the President."[21]

32. A Privacy Impact Assessment for a "new collection of information" must be "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information."[22] The PIA must specifically address "(I) what information is to be collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and] (VI) how the information will be secured . . . ."[23]

---

[18] Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note).
[19] 44 U.S.C. § 3501 note ("Privacy Impact Assessments").
[20] *Id.*
[21] 44 U.S.C. § 3502(1).
[22] § 3501 note ("Privacy Impact Assessments").
[23] *Id.*

33. Under the FACA, "records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [an] 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."[24]

34. The Commission has not conducted a Privacy Impact Assessment for its collection of state voter data.

35. The Commission has not ensured review of a PIA by any Chief Information Officer or equivalent official.

36. The Commission has not published a PIA or made such an assessment available for public inspection.

The DoD's Privacy Impact Assessment Does Not Permit
the Collection of Personal Information from The General Public

37. The DoD last approved a PIA for the Safe Access File Exchange system in 2015.[25]

38. The 2015 PIA indicates that the SAFE system may "collect, maintain, use and/or disseminate PII" about only "federal personnel and/or federal contractors."[26]

39. The 2015 PIA specifically indicates that the SAFE system may not be used to "collect, maintain, use and/or disseminate PII" from "members of the general public."[27]

40. According to the 2015 PIA, the SAFE system may not be used to collect the data set out in the June 28, 2017, from Vice Chair Kobach, directing state election officials to provide voter roll data.

---

[24] 5 U.S.C. app. 2 § 10(b).
[25] Army Chief Information Officer, U.S. Dep't of Def., *Privacy Impact Assessments* (April 27, 2016), http://ciog6.army.mil/PrivacyImpactAssessments/tabid/71/Default.aspx.
[26] EPIC Supp. Ex. 5, ECF No. 20-1, at 1.
[27] EPIC Supp. Ex. 5, ECF No. 20-1, at 1.

41. The DoD has not issued a PIA for the collection of personal data from the general public.

42. The DoD has not issued a PIA that would permit the receipt of data specified in the June 28, 2017, Kobach letter.

Count I

Violation of APA: Unlawful Agency Action

43. Plaintiff asserts and incorporates by reference paragraphs 1–42.

44. Defendants' collection of state voter data prior to creating, reviewing, and publishing a Privacy Impact Assessment, 44 U.S.C. § 3501 note, is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law under 5 U.S.C. § 706(2)(a) and short of statutory right under 5 U.S.C. § 706(2)(c).

45. Defendants' decision to initiate collection of voter data is a final agency action within the meaning of 5 U.S.C. § 704.

46. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

47. Plaintiff has exhausted all applicable administrative remedies.

Count II

Violation of APA: Agency Action Unlawfully Withheld

48. Plaintiff asserts and incorporates by reference paragraphs 1–42.

49. Defendants have failed to create, review, and/or publish a privacy impact assessment for Defendants' collection of voter data, as required by 44 U.S.C. § 3501 note and 5 U.S.C. app. 2 § 10(b).

50. Defendants' failure to take these steps constitutes agency action unlawfully withheld or unreasonably delayed in violation of 5 U.S.C. § 706(1).

51. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

52. Plaintiff has exhausted all applicable administrative remedies.

Count III

Violation of FACA: Failure to Make Documents Available for Public Inspection

53. Plaintiff asserts and incorporates by reference paragraphs 1–42.

54. Defendants have failed to make available for public inspection a privacy impact assessment for the collection of voter data.

55. Defendants' failure to make available for public inspection a PIA required by law is a violation of 5 U.S.C. app. 2 § 10(b).

56. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

57. Plaintiff has exhausted all applicable administrative remedies.

Count IV

Violation of Fifth Amendment: Substantive Due Process/Right to Informational Privacy

58. Plaintiff asserts and incorporates by reference paragraphs 1–42.

59. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have violated the informational privacy rights of millions of Americans, including members of the EPIC Advisory Board, guaranteed by the Due Process Clause of the Fifth Amendment. *See* U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

60. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

Count V

Violation of Fifth Amendment: Procedural Due Process

61. Plaintiff asserts and incorporates by reference paragraphs 1–42.

62. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have deprived EPIC's members of their liberty interest in avoiding the disclosure of personal matters. U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

63. Defendants have done so without providing notice to EPIC's members, without providing EPIC's members an opportunity to challenge the collection of their personal data, and without providing for a neutral decisionmaker to decide on any such challenges brought by EPIC's members.

64. Defendants have violated EPIC's members Fifth Amendment right to due process of law. U.S. Const. amend. V.

65. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

Requested Relief

WHEREFORE, Plaintiff requests that this Court:

A. Hold unlawful and set aside Defendants' authority to collect personal voter data from the states;

B. Order Defendants to halt collection of personal voter data;

C. Order Defendants to securely delete and properly disgorge any personal voter data collected or subsequently received;

D. Order Defendants to promptly conduct a privacy impact assessment prior to the collection of personal voter data;

E. Award EPIC costs and reasonable attorney's fees incurred in this action; and

F. Grant such other relief as the Court may deem just and proper.

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 7, 2017

AO 440 (Rev. 06/12) Summons in a Civil Action

UNITED STATES DISTRICT COURT

for the

District of Columbia

Electronic Privacy Information Center

Plaintiff(s)

v.

Presidential Advisory Commission on Election Integrity, et al.

Defendant(s)

Civil Action No. 1:17-cv-01320-CKK

SUMMONS IN A CIVIL ACTION

To: *(Defendant's name and address)*

UNITED STATES DEPARTMENT OF DEFENSE
1000 Defense Pentagon
Washington, D.C. 20301-0001

A lawsuit has been filed against you.

Within 21 days after service of this summons on you (not counting the day you received it) — or 60 days if you are the United States or a United States agency, or an officer or employee of the United States described in Fed. R. Civ. P. 12 (a)(2) or (3) — you must serve on the plaintiff an answer to the attached complaint or a motion under Rule 12 of the Federal Rules of Civil Procedure. The answer or motion must be served on the plaintiff or plaintiff's attorney, whose name and address are:

MARC ROTENBERG
ALAN BUTLER
ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009

If you fail to respond, judgment by default will be entered against you for the relief demanded in the complaint. You also must file your answer or motion with the court.

CLERK OF COURT

Date: _____

_____
Signature of Clerk or Deputy Clerk

Civil Action No.

PROOF OF SERVICE

(This section should not be filed with the court unless required by Fed. R. Civ. P. 4 (l))

This summons for *(name of individual and title, if any)* _____

was received by me on *(date)* _____ .

❒ I personally served the summons on the individual at *(place)* _____

_____ on *(date)* _____ ; or

❒ I left the summons at the individual's residence or usual place of abode with *(name)* _____

_____ , a person of suitable age and discretion who resides there,

on *(date)* _____ , and mailed a copy to the individual's last known address; or

❒ I served the summons on *(name of individual)* _____ , who is

designated by law to accept service of process on behalf of *(name of organization)* _____

_____ on *(date)* _____ ; or

❒ I returned the summons unexecuted because _____ ; or

❒ Other *(specify):*

My fees are $ _____ for travel and $ _____ for services, for a total of $ 0.00 .

I declare under penalty of perjury that this information is true.

Date: _____

_____

Server's signature

_____

Printed name and title

_____

Server's address

Additional information regarding attempted service, etc:

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 17-1320 (CKK)

ORDER
(July 10, 2017)

The Court has received Plaintiff's Amended Complaint, ECF No. 21, which has added the Department of Defense as a party to this litigation. The Amended Complaint was filed as of right pursuant to Federal Rule of Civil Procedure 15(a)(1)(A). The Court shall apply all of the arguments made in Defendants' briefing to the Department of Defense, and has received substantial testimony on the propriety of injunctive relief against the Department of Defense during the motions hearing held on July 7, 2017. The Court has reviewed the transcript of that hearing with respect to the Department of Defense. Accordingly, while it has not reached any decision regarding the merits of Plaintiff's request for injunctive relief, the Court does not see a need for supplemental briefing at this time. Nonetheless, in an abundance of caution, the Court shall permit Defendants to file supplemental briefing, solely with respect to issues particular to the Department of Defense, by **4:00 P.M.** on **July 10, 2017**.

SO ORDERED.

/s/
COLLEEN KOLLAR-KOTELLY
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER
1718 Connecticut Avenue, N.W.
Suite 200
Washington, D.C. 20009

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY; MICHAEL PENCE, in his official capacity as 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;
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

GENERAL SERVICES ADMINISTRATION
1800 F Street, N.W.
Washington, D.C. 20405

Defendants.

Case: 1:17-cv-01320
Assigned To : Kollar-Kotelly, Colleen
Assign. Date : 7/3/2017
Description: TRO/PI

COMPLAINT FOR INJUNCTIVE RELIEF

1. This is an action under the Administrative Procedure Act ("APA"), 5 U.S.C. §§ 551–706, the Federal Advisory Committee Act ("FACA"), 5 U.S.C. app. 2, and the United States Constitution for injunctive and other appropriate relief to halt the collection of state voter data by the Presidential Advisory Commission on Election Integrity (the "PACEI" or the

"Commission"), by officers of the Commission, and by the agencies which oversee and facilitate the activities of the Commission.

2. The Electronic Privacy Information Center ("EPIC") challenges the Commission's intent to collect the personal data of millions of registered voters and to publish partial SSNs as an unconstitutional invasion of privacy and a violation of the agency's obligation to conduct a Privacy Impact Assessment ("PIA").

Jurisdiction and Venue

3. This Court has subject matter jurisdiction over this action pursuant to 28 U.S.C. § 1331, 5 U.S.C. § 702, and 5 U.S.C. § 704. This Court has personal jurisdiction over Defendants.

4. Venue is proper in this district under 5 U.S.C. § 703 and 28 U.S.C. § 1391.

Parties

5. Plaintiff EPIC is a nonprofit organization incorporated in Washington, D.C., and established in 1994 to focus public attention on emerging privacy and civil liberties issues. Central to EPIC's mission is oversight and analysis of government activities. EPIC's Advisory Board members include distinguished experts in law, technology, public policy, and cybersecurity. EPIC has a long history of working to protect voter privacy and the security of election infrastructure. EPIC has specific expertise regarding the misuse of the Social Security Number ("SSN") and has sought stronger protections for the SSN for more than two decades.

6. EPIC's members include registered voters in California, the District of Columbia, Florida, Maryland, Massachusetts, Minnesota, New York, Pennsylvania, Texas, and Washington.

7. Defendant PACEI is an advisory committee of the U.S. government within the meaning of FACA, 5 U.S.C. app. 2 § 10. Defendant PACEI is also an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

8. Defendant Michael Pence is the Vice President of the United States and the Chair of the PACEI.

9. Defendant Kris Kobach is the Secretary of State of Kansas and the Vice Chair of the PACEI.

10. Defendant Executive Office of the President of the United States ("EOP") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

11. Defendant Office of the Vice President of the United States ("OVP") is a subcomponent of EOP and an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701.

12. Defendant General Services Administration ("GSA") is an agency within the meaning of 44 U.S.C. § 3502 and the APA, 5 U.S.C. § 701. The GSA is charged with providing the PACEI "such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission . . . ." Ex. 1.[1]

Facts

The Commission's Unprecedented Collection of State Voter Data

13. The Commission was established by Executive Order on May 11, 2017 ("Commission Order"). Ex 1.[2]

14. The Commission is charged with "study[ing] the registration and voting processes used in Federal elections." Ex. 1.[3] The Commission Order contains no authority to gather personal data or to undertake investigations.[4]

15. 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 had never been made

[1] Exec. Order. No. 13,799, 82 Fed. Reg. 22,389, 22,390 (May 11, 2017).
[2] 82 Fed. Reg. at 22,389; *see also Voter Privacy and the PACEI*, EPIC.org (June 30, 2017), https://epic.org/privacy/voting/pacei/.
[3] 82 Fed. Reg. at 22,389.
[4] *See generally id.*

by any federal official in the history of the country. 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.[5]

16. According to the U.S. Census, state voter rolls include the names, addresses, and other personally identifiable information of at least 157 million registered voters.[6]

17. One of the letters from the Commission, dated June 28, 2017, was sent to North Carolina Secretary of State Elaine Marshall. Ex. 3.[7]

18. In the letter ("Commission Letter"), the Vice Chair urged the Secretary of State 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." Ex. 3.[8]

19. The Commission Letter also asked "[w]hat evidence or information [the state had] regarding instances of voter fraud or registration fraud" and "[w]hat convictions for election-related crimes ha[d] occurred in [the] state since the November 2000 federal election." Ex. 3.[9]

---

[5] Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017).
[6] U.S. Census Bureau, *Voting and Registration in the Election of November 2016* at tbl. 4a (May 2017), https://www.census.gov/data/tables/time-series/demo/voting-and-registration/p20-580.html.
[7] Letter from Kris Kobach, Vice Chair, PACEI, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017).
[8] *Id.* at 1–2.
[9] *Id.* at 1.

20. The Commission Letter stated that "any documents that are submitted to the full Commission w[ould] also be made available to the public." Ex. 3.[10]

21. The Commission asked for a response by July 14, 2017. Ex. 3.[11] The "SAFE" URL, recommend by the Commission for the submission of voter data, leads election officials to a non-secure site. Regarding this website, Google Chrome states: "Your connection is not private. Attackers may be trying to steal your information from [the site proposed by the Commission] (for example, passwords, messages, or credit cards)." Ex. 4.[12]

Many States Oppose the Commission's Demand for Personal Voter Data

22. In less than three days following the release of the Commission Letter, election officials in twenty-four states said that they would oppose, partiallly or fully, the demand for personal voter data.[13]

23. California Secretary of State Alex Padilla stated 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."[14]

---

[10] *Id.* at 2.
[11] *Id.*
[12] Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Site (July 3, 2017 12:02 AM).
[13] 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), 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/.
[14] Press Release, Secretary of State Alex Padilla Responds to Presidential Election Commission Request for Personal Data of California Voters (June 29, 2017), 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/.

24. Kentucky Secretary of State Alison Lundergan Grimes stated 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."[15]

25. Virginia Governor Terry McAuliffe stated that he had "no intention of honoring [Kobach's] request."[16]

26. More than fifty experts in voting technology and twenty privacy organizations wrote to state election officials to warn that "[t]here is no indication how the information will be used, who will have access to it, or what safeguards will be established."[17]

The Commission's Failure to Conduct a Privacy Impact Assessment

27. Under the E-Government Act of 2002,[18] 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.[19]

28. The agency must "(i) conduct 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

---

[15] Bradford Queen, Secretary Grimes Statement on Presidential Election Commission's Request for Voters' Personal Information, Kentucky (last accessed July 3, 2017) http://kentucky.gov/Pages/Activity-stream.aspx?n=SOS&prId=129.
[16] Terry McAuliffe, *Governor McAuliffe Statement on Request from Trump Elections Commission* (June 29, 2017), https://governor.virginia.gov/newsroom/newsarticle?articleId=20595.
[17] Letter from EPIC et al. to Nat'l Ass'n of State Sec'ys (July 3, 2017), https://epic.org/privacy/voting/pacei/Voter-Privacy-letter-to-NASS-07032017.pdf.
[18] Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note).
[19] 44 U.S.C. § 3501 note ("Privacy Impact Assessments").

(ii), make the privacy impact assessment publicly available through the website of the agency, publication in the Federal Register, or other means."[20]

29. The PACEI is an agency subject to the E-Government Act because it is an "establishment in the executive branch of the Government," a category which "includ[es] the Executive Office of the President."[21]

30. A Privacy Impact Assessment for a "new collection of information" must be "commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information."[22] The PIA must specifically address "(I) what information is to be collected; (II) why the information is being collected; (III) the intended use of the agency of the information; (IV) with whom the information will be shared; (V) what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared; [and] (VI) how the information will be secured . . . ."[23]

31. Under the FACA, "records, reports, transcripts, minutes, appendixes, working papers, drafts, studies, agenda, or other documents which were made available to or prepared for or by [an] 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."[24]

32. The Commission has not conducted a Privacy Impact Assessment for its collection of state voter data.

---

[20] *Id.*
[21] 44 U.S.C. § 3502(1).
[22] § 3501 note ("Privacy Impact Assessments").
[23] *Id.*
[24] 5 U.S.C. app. 2 § 10(b).

33. The Commission has not ensured review of a PIA by any Chief Information Officer or equivalent official.

34. The Commission has not published a PIA or made such an assessment available for public inspection.

Count I

Violation of APA: Unlawful Agency Action

35. Plaintiff asserts and incorporates by reference paragraphs 1–35.

36. Defendants' collection of state voter data prior to creating, reviewing, and publishing a Privacy Impact Assessment, 44 U.S.C. § 3501 note, is arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law under 5 U.S.C. § 706(2)(a) and short of statutory right under 5 U.S.C. § 706(2)(c).

37. Defendants' decision to initiate collection of voter data is a final agency action within the meaning of 5 U.S.C. § 704.

38. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

39. Plaintiff has exhausted all applicable administrative remedies.

Count II

Violation of APA: Agency Action Unlawfully Withheld

40. Plaintiff asserts and incorporates by reference paragraphs 1–35.

41. Defendants have failed to create, review, and/or publish a privacy impact assessment for Defendants' collection of voter data, as required by 44 U.S.C. § 3501 note and 5 U.S.C. app. 2 § 10(b).

42. Defendants' failure to take these steps constitutes agency action unlawfully withheld or unreasonably delayed in violation of 5 U.S.C. § 706(1).

43. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

44. Plaintiff has exhausted all applicable administrative remedies.

Count III

Violation of FACA: Failure to Make Documents Available for Public Inspection

45. Plaintiff asserts and incorporates by reference paragraphs 1–35.

46. Defendant PACEI has failed to make available for public inspection a privacy impact assessment for the PACEI's collection of voter data.

47. Defendant PACEI's failure to do so is a violation of 5 U.S.C. app. 2 § 10(b).

48. Plaintiff, by itself and as a representative of its members, is adversely affected and aggrieved by Defendant PACEI's actions and inaction.

49. Plaintiff has exhausted all applicable administrative remedies.

Count IV

Violation of Fifth Amendment: Substantive Due Process/Right to Informational Privacy

50. Plaintiff asserts and incorporates by reference paragraphs 1–35.

51. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have violated the informational privacy rights of millions of Americans, including members of the EPIC Advisory Board, guaranteed by the Due Process Clause of the Fifth Amendment. *See* U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

52. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions.

Count V

Violation of Fifth Amendment: Procedural Due Process

53. Plaintiff asserts and incorporates by reference paragraphs 1–35.

54. Defendants, by seeking to assemble an unnecessary and excessive federal database of sensitive voter data from state records systems, have deprived EPIC's members of their liberty interest in avoiding the disclosure of personal matters. U.S. Const. amend. V; *NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Administrator of General Services*, 433 U.S. 425, 457 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600 (1977).

55. Defendants have done so without providing notice to EPIC's members, without providing EPIC's members an opportunity to challenge the collection of their personal data, and without providing for a neutral decisionmaker to decide on any such challenges brought by EPIC's members.

56. Defendants have violated EPIC's members Fifth Amendment right to due process of law. U.S. Const. amend. V.

57. Plaintiff, as a representative of its members, is adversely affected and aggrieved by Defendants' actions and inaction.

Requested Relief

WHEREFORE, Plaintiff requests that this Court:

A. Hold unlawful and set aside Defendants' authority to collect personal voter data from the states;

B. Order Defendants to halt collection of personal voter data;

C. Order Defendants to securely delete and properly disgorge any personal voter data collected or subsequently received;

D. Order Defendants to promptly conduct a privacy impact assessment prior to the collection of personal voter data;

E. Award EPIC costs and reasonable attorney's fees incurred in this action; and

F. Grant such other relief as the Court may deem just and proper.

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

LIST OF EXHIBITS

Exhibit 1	Exec. Order. No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017)
Exhibit 2	Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017)
Exhibit 3	Letter from Kris Kobach, Vice Chair, Presidential Advisory Commission on Election Integrity, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017)
Exhibit 4	Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Website (July 3, 2017 12:02 AM)

Exhibit 1

Federal Register
Vol. 82, No. 93
Tuesday, May 16, 2017

Presidential Documents

Title 3—

The President

Executive Order 13799 of May 11, 2017

Establishment of Presidential Advisory Commission on Election Integrity

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote fair and honest Federal elections, it is hereby ordered as follows:

Section 1. *Establishment.* The Presidential Advisory Commission on Election Integrity (Commission) is hereby established.

Sec. 2. *Membership.* The Vice President shall chair the Commission, which shall be composed of not more than 15 additional members. The President shall appoint the additional members, who shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience that the President determines to be of value to the Commission. The Vice President may select a Vice Chair of the Commission from among the members appointed by the President.

Sec. 3. *Mission.* The Commission shall, consistent with applicable law, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President that identifies the following:

(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 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.

Sec. 4. *Definitions.* For purposes of this order:

(a) The term "improper voter registration" means any situation where an individual who does not possess the legal right to vote in a jurisdiction is included as an eligible voter on that jurisdiction's voter list, regardless of the state of mind or intent of such individual.

(b) The term "improper voting" means the act of an individual casting a non-provisional ballot in a jurisdiction in which that individual is ineligible to vote, or the act of an individual casting a ballot in multiple jurisdictions, regardless of the state of mind or intent of that individual.

(c) The term "fraudulent voter registration" means any situation where an individual knowingly and intentionally takes steps to add ineligible individuals to voter lists.

(d) The term "fraudulent voting" means the act of casting a non-provisional ballot or multiple ballots with knowledge that casting the ballot or ballots is illegal.

Sec. 5. *Administration.* The Commission shall hold public meetings and engage with Federal, State, and local officials, and election law experts, as necessary, to carry out its mission. The Commission shall be informed by, and shall strive to avoid duplicating, the efforts of existing government entities. The Commission shall have staff to provide support for its functions.

Sec. 6. *Termination.* The Commission shall terminate 30 days after it submits its report to the President.

Sec. 7. *General Provisions.* (a) To the extent permitted by law, and subject to the availability of appropriations, the General Services Administration shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis.

(b) Relevant executive departments and agencies shall endeavor to cooperate with the Commission.

(c) Insofar as the Federal Advisory Committee Act, as amended (5 U.S.C. App.) (the "Act"), may apply to the Commission, any functions of the President under that Act, except for those in section 6 of the Act, shall be performed by the Administrator of General Services.

(d) Members of the Commission shall serve without any additional compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, to the extent permitted by law for persons serving intermittently in the Government service (5 U.S.C. 5701–5707).

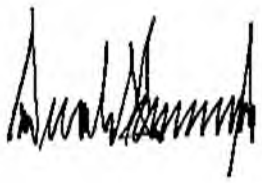
(e) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(g) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.



THE WHITE HOUSE,
May 11, 2017.

[FR Doc. 2017–10003
Filed 5–15–17; 8:45 am]
Billing code 3295–F7–P

Exhibit 2

the WHITE HOUSE

The White House
Office of the Vice President

For Immediate Release June 28, 2017

Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity

This morning, Vice President Mike Pence held an organizational call with members of the Presidential Advisory Commission on Election Integrity. The Vice President reiterated President Trump's charge to the commission with producing a set of recommendations to increase the American people's confidence in the integrity of our election systems.

"The integrity of the vote is a foundation of our democracy; this bipartisan commission will review ways to strengthen that integrity in order to protect and preserve the principle of one person, one vote," the Vice President told commission members today.

The commission set July 19 as its first meeting, which will take place in Washington, D.C.

Vice Chair of the Commission and Kansas Secretary of State Kris Kobach told members a letter will be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls and feedback on how to improve election integrity.

Exhibit 3

Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable Elaine Marshall
Secretary of State
PO Box 29622
Raleigh, NC 27626-0622

Dear Secretary Marshall,

I serve as the Vice Chair for the Presidential Advisory Commission on Election Integrity ("Commission"), which was formed pursuant to Executive Order 13799 of May 11, 2017. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President of the United States that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine the American people's confidence in the integrity of federal elections processes.

As the Commission begins it work, I invite you to contribute your views and recommendations throughout this process. In particular:

1. What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections?
2. How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities?
3. What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer?
4. What evidence or information do you have regarding instances of voter fraud or registration fraud in your state?
5. What convictions for election-related crimes have occurred in your state since the November 2000 federal election?
6. What recommendations do you have for preventing voter intimidation or disenfranchisement?
7. What other issues do you believe the Commission should consider?

In addition, in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly-available voter roll data for North Carolina, including, if publicly available under the laws of your state, 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.

You may submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files. You can access the SAFE site at https://safe.amrdec.army.mil/safe/Welcome.aspx. We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public. If you have any questions, please contact Commission staff at the same email address.

On behalf of my fellow commissioners, I also want to acknowledge your important leadership role in administering the elections within your state and the importance of state-level authority in our federalist system. It is crucial for the Commission to consider your input as it collects data and identifies areas of opportunity to increase the integrity of our election systems.

I look forward to hearing from you and working with you in the months ahead.

Sincerely,

Kris Kobach

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity

Exhibit 4

Privacy error ×

← C ⚠ Not Secure ~~https~~://safe.amrdec.army.mil/safe/Welcome.aspx ☆

Your connection is not private

Attackers might be trying to steal your information from **safe.amrdec.army.mil** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

Back to safety

● Washington DC, USA - current and ac...

Secure https://www.timeanddate.com/wor

Local time in Washington DC
Monday, July 3, 2017

12:02:40 am

EDT

CIVIL COVER SHEET

JS-44 (Rev. 6/17 DC)

I. (a) PLAINTIFFS
Electronic Privacy Information Center

(b) COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF _____
(EXCEPT IN U.S. PLAINTIFF CASES)

DEFENDANTS
Presidential Advisory Commission on Election Integrity; Michael Pence; Kris Kobach; Executive Office of the President of the United States; Office of the Vice President of the United States; General Services Administration

COUNTY OF RESIDENCE OF FIRST LISTED DEFENDANT 11001
(IN U.S. PLAINTIFF CASES ONLY)
NOTE: IN LAND CONDEMNATION CASES, USE THE LOCATION OF THE TRACT OF LAND INVOLVED

(c) ATTORNEYS (FIRM NAME, ADDRESS, AND TELEPHONE NUMBER)
Marc Rotenberg
1718 Connecticut Ave. NW
Washington, DC 20009
202-284-1140

Case: 1:17-cv-01320
Assigned To : Kollar-Kotelly, Colleen
Assign. Date : 7/3/2017
Description: TRO/PI

II. BASIS OF JURISDICTION
(PLACE AN x IN ONE BOX ONLY)

- ○ 1 U.S. Government Plaintiff
- ○ 3 Federal Question (U.S. Government Not a Party)
- ◉ 2 U.S. Government Defendant
- ○ 4 Diversity (Indicate Citizenship of Parties in item III)

III. CITIZENSHIP OF PRINCIPAL PARTIES (PLACE AN x IN ONE BOX FOR PLAINTIFF AND ONE BOX FOR DEFENDANT) **FOR DIVERSITY CASES ONLY!**

	PTF	DFT		PTF	DFT
Citizen of this State	○ 1	○ 1	Incorporated or Principal Place of Business in This State	○ 4	○ 4
Citizen of Another State	○ 2	○ 2	Incorporated and Principal Place of Business in Another State	○ 5	○ 5
Citizen or Subject of a Foreign Country	○ 3	○ 3	Foreign Nation	○ 6	○ 6

IV. CASE ASSIGNMENT AND NATURE OF SUIT
(Place an X in one category, A-N, that best represents your Cause of Action and one in a corresponding Nature of Suit)

○ **A. *Antitrust***
- ☐ 410 Antitrust

○ **B. *Personal Injury/ Malpractice***
- ☐ 310 Airplane
- ☐ 315 Airplane Product Liability
- ☐ 320 Assault, Libel & Slander
- ☐ 330 Federal Employers Liability
- ☐ 340 Marine
- ☐ 345 Marine Product Liability
- ☐ 350 Motor Vehicle
- ☐ 355 Motor Vehicle Product Liability
- ☐ 360 Other Personal Injury
- ☐ 362 Medical Malpractice
- ☐ 365 Product Liability
- ☐ 367 Health Care/Pharmaceutical Personal Injury Product Liability
- ☐ 368 Asbestos Product Liability

○ **C. *Administrative Agency Review***
- ☐ 151 Medicare Act

Social Security
- ☐ 861 HIA (1395ff)
- ☐ 862 Black Lung (923)
- ☐ 863 DIWC/DIWW (405(g))
- ☐ 864 SSID Title XVI
- ☐ 865 RSI (405(g))

Other Statutes
- ☐ 891 Agricultural Acts
- ☐ 893 Environmental Matters
- ☐ 890 Other Statutory Actions (If Administrative Agency is Involved)

◉ **D. *Temporary Restraining Order/Preliminary Injunction***

Any nature of suit from any category may be selected for this category of case assignment.

(If Antitrust, then A governs)

○ **E. *General Civil (Other)*** OR ○ **F. *Pro Se General Civil***

Real Property
- ☐ 210 Land Condemnation
- ☐ 220 Foreclosure
- ☐ 230 Rent, Lease & Ejectment
- ☐ 240 Torts to Land
- ☐ 245 Tort Product Liability
- ☐ 290 All Other Real Property

Personal Property
- ☐ 370 Other Fraud
- ☐ 371 Truth in Lending
- ☐ 380 Other Personal Property Damage
- ☐ 385 Property Damage Product Liability

Bankruptcy
- ☐ 422 Appeal 27 USC 158
- ☐ 423 Withdrawal 28 USC 157

Prisoner Petitions
- ☐ 535 Death Penalty
- ☐ 540 Mandamus & Other
- ☐ 550 Civil Rights
- ☐ 555 Prison Conditions
- ☐ 560 Civil Detainee – Conditions of Confinement

Property Rights
- ☐ 820 Copyrights
- ☐ 830 Patent
- ☐ 835 Patent – Abbreviated New Drug Application
- ☐ 840 Trademark

Federal Tax Suits
- ☐ 870 Taxes (US plaintiff or defendant)
- ☐ 871 IRS-Third Party 26 USC 7609

Forfeiture/Penalty
- ☐ 625 Drug Related Seizure of Property 21 USC 881
- ☐ 690 Other

Other Statutes
- ☐ 375 False Claims Act
- ☐ 376 Qui Tam (31 USC 3729(a))
- ☐ 400 State Reapportionment
- ☐ 430 Banks & Banking
- ☐ 450 Commerce/ICC Rates/etc.
- ☐ 460 Deportation
- ☐ 462 Naturalization Application
- ☐ 465 Other Immigration Actions
- ☐ 470 Racketeer Influenced & Corrupt Organization
- ☐ 480 Consumer Credit
- ☐ 490 Cable/Satellite TV
- ☐ 850 Securities/Commodities/ Exchange
- ☐ 896 Arbitration
- ☒ 899 Administrative Procedure Act/Review or Appeal of Agency Decision
- ☐ 950 Constitutionality of State Statutes
- ☐ 890 Other Statutory Actions (if not administrative agency review or Privacy Act)

(8)

18-F-1517//0053

○ G. *Habeas Corpus/ 2255* ☐ 530 Habeas Corpus – General ☐ 510 Motion/Vacate Sentence ☐ 463 Habeas Corpus – Alien Detainee	○ H. *Employment Discrimination* ☐ 442 Civil Rights – Employment (criteria: race, gender/sex, national origin, discrimination, disability, age, religion, retaliation) *(If pro se, select this deck)*	○ I. *FOIA/Privacy Act* ☐ 895 Freedom of Information Act ☐ 890 Other Statutory Actions (if Privacy Act) *(If pro se, select this deck)*	○ J. *Student Loan* ☐ 152 Recovery of Defaulted Student Loan (excluding veterans)
○ K. *Labor/ERISA (non-employment)* ☐ 710 Fair Labor Standards Act ☐ 720 Labor/Mgmt. Relations ☐ 740 Labor Railway Act ☐ 751 Family and Medical Leave Act ☐ 790 Other Labor Litigation ☐ 791 Empl. Ret. Inc. Security Act	○ L. *Other Civil Rights (non-employment)* ☐ 441 Voting (if not Voting Rights Act) ☐ 443 Housing/Accommodations ☐ 440 Other Civil Rights ☐ 445 Americans w/Disabilities – Employment ☐ 446 Americans w/Disabilities – Other ☐ 448 Education	○ M. *Contract* ☐ 110 Insurance ☐ 120 Marine ☐ 130 Miller Act ☐ 140 Negotiable Instrument ☐ 150 Recovery of Overpayment & Enforcement of Judgment ☐ 153 Recovery of Overpayment of Veteran's Benefits ☐ 160 Stockholder's Suits ☐ 190 Other Contracts ☐ 195 Contract Product Liability ☐ 196 Franchise	○ N. *Three-Judge Court* ☐ 441 Civil Rights – Voting (if Voting Rights Act)

V. ORIGIN

◉ 1 Original Proceeding ○ 2 Removed from State Court ○ 3 Remanded from Appellate Court ○ 4 Reinstated or Reopened ○ 5 Transferred from another district (specify) ○ 6 Multi-district Litigation ○ 7 Appeal to District Judge from Mag. Judge ○ 8 Multi-district Litigation – Direct File

VI. CAUSE OF ACTION (CITE THE U.S. CIVIL STATUTE UNDER WHICH YOU ARE FILING AND WRITE A BRIEF STATEMENT OF CAUSE.)
Suit for injunctive relief under Admin. Proc. Act, 5 U.S.C. § 702, and Fed. Advisory Committee Act, 5 U.S.C. app. 2 § 10(b)

VII. REQUESTED IN COMPLAINT CHECK IF THIS IS A CLASS ACTION UNDER F R.C.P 23 **DEMAND $** **JURY DEMAND:** Check YES only if demanded in complaint YES ☐ NO ☑

VIII. RELATED CASE(S) IF ANY (See instruction) YES ☐ NO ☑ If yes, please complete related case form

DATE: 7/3/2017 **SIGNATURE OF ATTORNEY OF RECORD** /s/ Marc Rotenberg

INSTRUCTIONS FOR COMPLETING CIVIL COVER SHEET JS-44
Authority for Civil Cover Sheet

The JS-44 civil cover sheet and the information contained herein neither replaces nor supplements the filings and services of pleadings or other papers as required by law, except as provided by local rules of court. This form, approved by the Judicial Conference of the United States in September 1974, is required for the use of the Clerk of Court for the purpose of initiating the civil docket sheet. Consequently, a civil cover sheet is submitted to the Clerk of Court for each civil complaint filed. Listed below are tips for completing the civil cover sheet. These tips coincide with the Roman Numerals on the cover sheet.

I. COUNTY OF RESIDENCE OF FIRST LISTED PLAINTIFF/DEFENDANT (b) County of residence: Use 11001 to indicate plaintiff if resident of Washington, DC, 88888 if plaintiff is resident of United States but not Washington, DC, and 99999 if plaintiff is outside the United States.

III. CITIZENSHIP OF PRINCIPAL PARTIES: This section is completed only if diversity of citizenship was selected as the Basis of Jurisdiction under Section II.

IV. CASE ASSIGNMENT AND NATURE OF SUIT: The assignment of a judge to your case will depend on the category you select that best represents the primary cause of action found in your complaint. You may select only one category. You must also select one corresponding nature of suit found under the category of the case.

VI. CAUSE OF ACTION: Cite the U.S. Civil Statute under which you are filing and write a brief statement of the primary cause.

VIII. RELATED CASE(S), IF ANY: If you indicated that there is a related case, you must complete a related case form, which may be obtained from the Clerk's Office.

Because of the need for accurate and complete information, you should ensure the accuracy of the information provided prior to signing the form.

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 17-1320 (CKK)

ORDER
(July 5, 2017)

The Court is in receipt of Defendants' [8] Memorandum in Opposition to Plaintiff's Emergency Motion for a Temporary Restraining Order, and hereby instructs Defendants to respond to the following questions by **12:00 P.M.** on **Thursday, July 6, 2017**.

1) Who are the current members of the Presidential Advisory Commission on Election Integrity, and what are their affiliations?

2) If there are no current members who are officials of a federal agency, what is the likelihood that an official of a federal agency will become a member of the Presidential Advisory Commission on Election Integrity in the near future? Identify any likely members who are currently officials of a federal agency.

3) To what extent has or will the General Services Administration be involved in the collection and storage of data for the Presidential Advisory Commission on Election Integrity?

4) Who is the current operator of the website https://safe.amrdec.army.mil/safe/Welcome.aspx?

5) Who is responsible for collecting and storing data received via the website https://safe.amrdec.army.mil/safe/Welcome.aspx? Who will transfer that data to the Presidential Advisory Commission on Election Integrity?

So that Plaintiff may have an opportunity to review Defendants' responses, Plaintiff's reply shall be due by **2:00 P.M.** on **Thursday, July 6, 2017**.

SO ORDERED.

/s/
COLLEEN KOLLAR-KOTELLY
United States District Judge

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 1:17-cv-1320 (CKK)

MEMORANDUM IN OPPOSITION TO PLAINTIFF'S EMERGENCY MOTION FOR A TEMPORARY RESTRAINING ORDER

INTRODUCTION

The Court should deny plaintiff Electronic Privacy Information Center's ("EPIC") extraordinary request for an emergency injunction prohibiting the Presidential Advisory Commission on Election Integrity ("the Commission") from collecting, on a voluntary basis, publicly available voter data from state election officials.

As a threshold matter, the Court lacks jurisdiction to issue a temporary restraining order because EPIC failed to establish its standing. EPIC alleged no facts that the organization itself has suffered any injury, nor did it identify a single member who is suffering injury. In any event, EPIC's members could not possibly be injured by the transfer of *public* information from one sovereign to another. Its concerns about a possible data breach at some point in the future by unknown third parties fall well short of an imminent and concrete injury that is traceable to the Commission and redressable by this Court.

Even assuming the Court has jurisdiction, EPIC has not established its entitlement to emergency injunctive relief. EPIC has not shown that it will suffer any harm – much less *irreparable* harm – in the absence of a temporary restraining order. The voter data that EPIC seeks to enjoin the Commission from collecting is already made publicly available by the states. The Commission has established reasonable measures to protect the security of the voter data by using a secure method to transfer the data and storing any data in the White House's information systems.

Nor has EPIC established a substantial likelihood of success on the merits because it has no viable claims. Both the Administrative Procedure Act ("APA") and the E-Government Act of 2002 apply only to "agencies," but the Commission is not an "agency" within the meaning of

these statutes because its sole purpose is to provide advice to the President. EPIC's claim that the voluntary collection of publicly available voter information violates a constitutional right to informational privacy is meritless. Neither the Supreme Court nor the D.C. Circuit has held that such a right even exists. Even if such a right did exist, it would not apply to information that is already publicly available.

Finally, the public interest weighs against emergency injunctive relief. The President established the Commission "in order to promote fair and honest Federal elections." Executive Order No. 13,799, 82 Fed. Reg. 22,389, 22,389 (May 11, 2017). By collecting voter data from the states, the Commission seeks to "enhance the American people's confidence in the integrity of the voting processes used in Federal elections." *Id.* EPIC seeks to halt this important work with meritless claims and a baseless fear about the states voluntarily submitting publicly available voter data to the federal government. Accordingly, EPIC's motion for a temporary restraining order should be denied.

BACKGROUND

The President established the Presidential Advisory Commission on Election Integrity in Executive Order No. 13,799. 82 Fed. Reg. 22,389 (May 11, 2017) [hereinafter Exec. Order No. 13,799]; *see also* Declaration of Kris W. Kobach ("Kobach Decl.") ¶ 3 & Exh. 1. The Commission is charged with "study[ing] the registration and voting processes used in Federal elections," "consistent with applicable law." Exec. Order No. 13,799, § 3. Vice President Pence is the Chairman of the Commission. *Id.* § 2. Kansas Secretary of State Kris Kobach is the Vice Chair of the Commission. Kobach Decl. ¶¶ 2, 3. The members of the Commission come from federal, state, and local jurisdictions across the political spectrum. *Id.* ¶ 3.

In furtherance of the Commission's mandate, the Vice Chair has sent letters to the states and the District of Columbia requesting publicly available data from state voter rolls and feedback on how to improve election integrity. Kobach Decl. ¶ 4. Among other things, the letters sent by the Vice Chair requested:

> the *publicly-available* voter roll data for [the State], including, *if publicly available under the laws of your state*, 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.

See, e.g., *id.*, Exh. 3 (letter to Alabama) (emphasis supplied).

The Vice Chair requested responses by July 14, 2017. Kobach Decl. ¶ 5 & Exh. 3. He provided two methods for the states to respond. *Id.* Narrative responses, not containing data, can be sent via email to the address provided in the letter. *Id.* This email is a White House email address (in the Office of the Vice President) subject to the security protecting all White House communications and networks. *Id.*

For data files, which would be too large to send via electronic mail, states can use the Safe Access File Exchange ("SAFE"), which is a secure method of transferring large files up to two gigabytes in size. Kobach Decl. ¶ 5 & Exh. 3. Once received, the Commission intends to maintain the transferred data on the computer systems of the White House. *Id.* ¶ 5. SAFE is a tested and reliable method of secure file transfer used routinely by the military for large, unclassified data sets. *Id.* It also supports encryption by individual users. *Id.; see generally* Safe Access File Exchange, https://safe.amrdec.army.mil/safe/Welcome.aspx (last visited July 5,

2017). Individuals who access the site receive a security warning that the user is accessing a U.S. government network. *See id.* Undersigned counsel were not able to reproduce any error message indicating that the site was insecure. *See* Pl.'s TRO Mem. (ECF No. 3), at 7.

The Commission has not yet received any substantive responses or data from the states. Kobach Decl. ¶ 6.

ARGUMENT

EPIC IS NOT ENTITLED TO A TEMPORARY RESTRAINING ORDER

"The standard for issuance of the extraordinary and drastic remedy of a temporary restraining order or a preliminary injunction is very high." *Jack's Canoes & Kayaks, LLC v. Nat'l Park Serv.*, 933 F. Supp. 2d 58, 76 (D.D.C. 2013) (citation omitted). An interim injunction is "never awarded as of right," *Winter v. Nat. Res. Def. Council, Inc.*, 555 U.S. 7, 24 (2008), and "should be granted only when the party seeking the relief, by a clear showing, carries the burden of persuasion," *Cobell v. Norton*, 391 F.3d 251, 258 (D.C. Cir. 2004). A party moving for a temporary restraining order or a preliminary injunction "must demonstrate '(1) a substantial likelihood of success on the merits, (2) that it would suffer irreparable injury if the injunction is not granted, (3) that an injunction would not substantially injure other interested parties, and (4) that the public interest would be furthered by the injunction.'" *Jack's Canoes,* 933 F. Supp. 2d at 75-76 (quoting *CityFed Fin. Corp. v. Office of Thrift Supervision*, 58 F.3d 738, 746 (D.C. Cir. 1995)).

I. EPIC HAS NOT ESTABLISHED THAT IT HAS STANDING

EPIC's request for a temporary restraining order must be denied because it has failed to establish standing to seek such relief. *See Aamer v. Obama*, 742 F.3d 1023, 1028 (D.C. Cir. 2014) ("We begin, as we must, with the question of subject-matter jurisdiction." (citing *Steel Co. v. Citizens for a Better Env't*, 523 U.S. 83, 101-02 (1998))). The doctrine of standing, an essential aspect of the Article III case-or-controversy requirement, demands that a plaintiff have "a personal stake in the outcome of the controversy [so] as to warrant his invocation of federal-court jurisdiction." *Warth v. Seldin*, 422 U.S. 490, 498 (1975). At its "irreducible constitutional minimum," the doctrine requires a plaintiff to establish three elements: (1) a concrete and particularized injury-in-fact, either actual or imminent, (2) a causal connection between the injury and defendants' challenged conduct, and (3) a likelihood that the injury suffered will be redressed by a favorable decision. *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 560 (1992).

To establish injury-in-fact, a plaintiff must show that the defendant's action affects him or her in a "personal and individual way," *see id.* at 560 n.1, rather than in some generalized way common to the general public, *see United States v. Richardson*, 418 U.S. 166, 176 (1974). Moreover, a plaintiff must show more than a "possible future injury"; he or she must show that harm has actually occurred or is "certainly impending." *Whitmore v. Arkansas*, 495 U.S. 149, 158 (1990) (citations omitted). The Supreme Court has emphasized that "threatened injury must be certainly impending to constitute injury in fact, and that allegations of possible future injury are not sufficient." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 133 S. Ct. 1138, 1147 (2013) (citations omitted).

EPIC claims standing in its own right and as a representative of its members. Compl. (ECF No. 1) ¶¶ 5, 6; Pl.'s TRO Mem. 2. To bring suit on its own behalf, an organization must itself meet the requirements for standing. *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 378 (1982). To establish representational standing, an organization must demonstrate that "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Ass'n of Flight Attendants–CWA v. Dep't of Transp.*, 564 F.3d 462, 464 (D.C. Cir. 2009) (citations omitted).

EPIC cannot demonstrate standing either for itself or as a representative of its members. It has not established that the organization has been or will be injured because none of the voting data at issue pertains to EPIC itself. EPIC has also failed to identify a single member who has suffered or will suffer an injury. *Chamber of Commerce of U.S. v. EPA*, 642 F.3d 192, 199 (D.C. Cir. 2011) ("When a petitioner claims associational standing, it is not enough to aver that unidentified members have been injured." (citing *Summers v. Earth Island Inst.*, 555 U.S. 488, 498 (2009))); *Am. Chemistry Council v. Dep't of Transp.*, 468 F.3d 810, 820 (D.C. Cir. 2006) ("[A]n organization bringing a claim based on associational standing must show that at least one specifically-identified member has suffered an injury-in-fact. . . . At the very least, the identity of the party suffering an injury in fact must be firmly established.").

Even if a member were identified, any claim of injury would be entirely speculative. EPIC claims that its members may be harmed in the future if the publicly available data is not securely transferred to the Commission and if that data is then breached by an unknown third party. Pl.'s TRO Mem. 17-18. To guard against such breaches, the data is intended to be

transmitted via a secure method and then maintained on secure White House servers. *See* Kobach Decl. ¶ 5 & Exh. 3. Particularly in view of these safeguards, plaintiff's "highly attenuated chain of possibilities" is insufficient to establish standing. *Clapper*, 133 S. Ct. at 1148.

EPIC further claims that the Commission will publicly disclose its members' voting information and that the unnamed members could be harmed when this data is then used for "deviant purposes." Pl.'s TRO Mem. 17. EPIC overlooks that the Commission only requested information that is already publicly available from the states. The Commission will not publicly disclose the data in personally identifiable form. *See* Kobach Decl. ¶ 5. In any event, EPIC's amorphous fear of a future data breach by unknown bad actors does not establish imminent and concrete injury. *See In re Sci. Applications Int'l Corp. (SAIC) Backup Tape Data Theft Lit.*, 45 F. Supp. 3d 14, 26 (D.D.C. 2014) (increased risk of identity theft alone does not confer standing in data-breach cases); *see also Welborn v. IRS*, 218 F. Supp. 3d 64, 77 (D.D.C. 2016) (even an "objectively reasonable likelihood" of future breach cannot support standing) (quoting *Clapper*, 133 S. Ct. at 1157-48), *appeal dismissed by* 2017 WL 2373044 (D.C. Cir. Apr. 18, 2017) Nor is any risk of a data-breach injury fairly traceable to the Commission. This data is equally vulnerable (if at all) in the hands of the states. Securely transferring data to a secure White House server does not increase the risk of improper disclosure.

In sum, because EPIC lacks standing, the Court lacks jurisdiction to issue a temporary restraining order.

II. EPIC HAS FAILED TO ESTABLISH THAT IT OR ITS MEMBERS WILL SUFFER IRREPARABLE HARM

The motion should also be denied because EPIC has not established that it will suffer irreparable injury absent a temporary restraining order. The D.C. Circuit "has set a high standard for irreparable injury." *In re Navy Chaplaincy*, 534 F.3d 756, 766 (D.C. Cir. 2008) (citation omitted). It is a "well known and indisputable principle[]" that a "unsubstantiated and speculative" harm cannot constitute "irreparable harm" sufficient to justify injunctive relief. *Wisc. Gas Co. v. FERC*, 758 F.2d 669, 674 (D.C. Cir. 1985) (per curiam).

EPIC cannot demonstrate irreparable injury for the same reason it lacks standing. It cannot establish that the organization or one of its members has suffered or will suffer a concrete or "certainly impending" injury. EPIC is concerned that the Commission will publicly disclose the information it obtains, but the Commission has only requested data that is *already* publicly available, much, if not all, of it pursuant to the National Voter Registration Act, 52 U.S.C. § 20507(i)(1), or through public access laws of individual states. *See* National Conference of State Legislatures, States and Election Reform (Feb. 2015) (discussing availability of voter information under state laws), http://www.ncsl.org/Documents/Elections/The_Canvass_February_2016_66.pdf; *see also Project Vote v. Long*, 682 F.3d 331, 336 (4th Cir. 2012) (holding that 52 U.S.C. § 20507(i)(1) "unmistakably encompasses completed voter registration applications"). The Commission has no intention of publicly disclosing data that are personally identifiable. Kobach Decl. ¶ 5. EPIC's speculative fear of a future breach of White House information systems by unknown third parties causing the release of information already available to the public cannot establish irreparable injury. Even without the Commission's collection of the information, the possibility of a breach will always exist (unfortunately) at the

state level; moreover, as the Commission has only requested information that is otherwise publicly available, there is nothing to prevent members of the public from accessing that information through a lawful request. Accordingly, the Commission's request for information has done nothing to increase any risk to EPIC's members and certainly does not create "irreparable injury" caused by the Commission and justifying emergency injunctive relief.

EPIC's claim of irreparable injury based on a violation of a supposed constitutional right to informational privacy also fails. As discussed below, there is no constitutional right to informational privacy for information that is already public. Because EPIC fails to establish irreparable harm, there is no basis for the Court to invoke its emergency powers at this early stage in the litigation.

III. PLAINTIFF HAS NOT ESTABLISHED SUBSTANTIAL LIKELIHOOD OF SUCCESS ON THE MERITS

EPIC has also failed to demonstrate substantial likelihood of success on the merits because it has no viable claim. First, EPIC has failed to state a claim under the APA or the E-Government Act of 2002 because the Commission is not an "agency" within the meaning of those statutes. Second, neither the Supreme Court nor the D.C. Circuit has recognized a constitutional right to informational privacy, but even if such a right exists, it would not apply to information that is already publicly available.

A. The Commission Is Not an "Agency" for Purposes of the Administrative Procedure Act or the E-Government Act of 2002

As an initial matter, EPIC does not have a valid claim under the E-Government Act. "[T]he E-Government Act of 2002 does not provide a private right of action." *Greenspan v. Admin. Office of the U.S. Courts*, No. 14-cv-2396, 2014 WL 6847460, at *8 (N.D. Cal. Dec. 4,

2014). EPIC must therefore use the Administrative Procedure Act's ("APA") cause of action. 5 U.S.C. § 702. The APA, however, only applies to *agency* action, and the Commission is not an agency for the purposes of the APA.[1] Accordingly, EPIC has no valid claim under the APA.

The APA defines an "agency" as "each authority of the Government of the United States," subject to several limitations not applicable here. 5 U.S.C. § 551(1). It is well established that the President and his close advisors do not fall within the APA's ambit. *See Franklin v. Massachusetts*, 505 U.S. 788, 800-01 (1992) (holding that "[o]ut of respect for the separation of powers and the unique constitutional position of the President," he is not subject to the APA). In *Meyer v. Bush*, 981 F.2d 1288 (D.C. Cir. 1993), the D.C. Circuit laid out a three-factor test to determine whether a group within the Executive Office of the President constituted an "agency": "(1) how close operationally the group is to the President, (2) whether it has a self-contained structure, and (3) the nature of its delegated authority." *Armstrong v. Exec. Office of the Pres.*, 90 F.3d 553, 558 (D.C. Cir. 1996) (quoting *Meyer*, 981 F.3d at 1293); *see also id.* ("The closer an entity is to the President, the more it is like the White House staff, which solely advises and assists the President, and the less it is like an agency to which substantial independent authority has been delegated.").[2]

---

[1] Although the General Services Administration ("GSA") is named as a defendant to this action, the present motion seeks to enjoin the collection of data, in which only the Commission is involved. *See* Pl.'s TRO Mot.; Kobach Decl. ¶ 4.

[2] This guidance comes mainly in the context of case law interpreting the definition of "agency" for purposes of the Freedom of Information Act ("FOIA"), which is broader than the definition of "agency" for purposes of the APA. The APA defines an "agency" as "each authority of the Government of the United States." 5 U.S.C. § 551(1). The FOIA, in turn, incorporates the definition set out in section 551(1) of the APA, and then expands the definition, stating that it "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

In applying this test, courts look at whether the entity has "substantial independent authority," including regulatory or funding powers. *Citizens for Resp. & Ethics in Wash.* ("*CREW*") *v. Office of Admin.*, 566 F.3d 219, 222-23 (D.C. Cir. 2009). For example, this Circuit has held that the Council of Economic Advisors is not an "agency" because it lacks regulatory power or independent authority, *id.* at 223, the National Security Council is not an "agency" because it plays only a "coordinating role on behalf of the President," *id.* (quoting *Armstrong*, 90 F.3d at 565), and the Office of Administration within the Executive Office of the President is not an "agency" because it provides "operational and administrative" tasks in "direct support of the President," *id.* at 224-25. *See also Armstrong*, 90 F.3d at 558-59 (collecting cases). Plaintiff does not even acknowledge, let alone attempt to distinguish, this line of cases.

Like these other White House entities, the Commission is an entity that "serve[s] solely to advise and assist the President," *Armstrong*, 90 F.3d at 558, and is not, therefore, an agency subject to the APA. The Commission reports directly to the President and is "solely advisory," Exec. Order No. 13,799; *see also* Charter, Presidential Advisory Commission on Election Integrity ¶ 4 ("The Commission will function solely as an advisory body.") (Kobach Decl., Exh. 2). It is chaired by the Vice President, a constitutional officer (and not, of course, an agency head). Exec. Order No. 13,799, at § 2. Its purpose is to "submit a report to the President" that identifies rules and activities that enhance and undermine the "American people's confidence in the integrity of the voting processes used in Federal elections" and to identify vulnerabilities in voting systems that could lead to improprieties. *Id.* § 3(a)-(c). The Commission has no

---

agency." 5 U.S.C. § 552(f)(1). *See also* Aaron J. Saiger, *Obama's 'Czars' for Domestic Policy and the Law of the White House Staff*, 79 Ford. L. Rev. 2577, 2599 (2011) ("FOIA uses a definition of 'agency' more expansive than used under the rest of the APA . . . .").

regulatory or funding powers, nor does it have any independent administrative responsibilities. Instead, it exists solely to provide research and advice to the President. *CREW*, 566 F.3d at 222-23. It is not, therefore, an "agency" subject to the APA, and the plaintiff's APA claim fails for that threshold reason alone.

Nor has EPIC stated a valid claim that the Commission was required to conduct a Privacy Impact Assessment under Section 208 of the E-Government Act, even if EPIC were able to assert a claim directly under the statute (which it cannot). E-Government Act of 2002, Pub. L. No. 107-347, § 208, 116 Stat. 2899. The E-Government Act applies to "agencies," as defined in 44 U.S.C. § 3502(1), which uses the same definition of "agency" as the FOIA (and is therefore subject to the same limitations as the D.C. Circuit has above defined). *See* E-Government Act § 201, 116 Stat. 2899. Because the Commission, which provides only advice and assistance to the President, is not an agency, it was not required to perform a Privacy Impact Assessment.[3]

Although not a basis for the present motion, EPIC's assertion that the Commission violated section 10(b) of the Federal Advisory Committee Act ("FACA"), 5 U.S.C. App. 2 § 10(b), by failing to publish a Privacy Impact Assessment or make one available for public inspection fares no better. *See* Compl. ¶ 41, 45-49. Defendants do not concede that FACA applies to the Commission or that EPIC has a cause of action under FACA here. *See In re Cheney*, 406 F.3d 723, 728 (D.C. Cir. 2005) (construing FACA statute strictly); *Ass'n of Am.*

---

[3] Even apart from the functional test establishing that the Commission exists to advise and assist the President, and is therefore not an "agency" under the APA, it is clear that an entity cannot be at once both an advisory committee and an agency. *See Heartwood, Inc. v. U.S. Forest Serv.*, 431 F. Supp. 2d 28, 36 (D.D.C. 2006) (noting that an "'advisory committee cannot have a double identity as an agency'" (quoting *Wolfe v. Weinberger*, 403 F. Supp. 238, 242 (D.D.C. 1975))).

Physicians & Surgeons, Inc. v. Clinton, 997 F.3d 898, 909-10 (D.C. Cir. 1993) (application of FACA to presidential advisory groups can raise constitutional concerns). Regardless, EPIC's FACA claim is meritless because the Commission – which is not an agency – is not required to conduct a Privacy Impact Assessment, nor has it done so, and therefore there is no report to publish. Accordingly, EPIC has failed to establish any violation of FACA.

B. Neither the Supreme Court Nor the D.C. Circuit Has Recognized a Constitutional Right to Informational Privacy, But Even If There Were, It Would Not Prohibit the Federal Government From Requesting Publicly Available Information From States

EPIC's claim of a constitutional right to informational privacy fails because neither the Supreme Court nor the D.C. Circuit has held that a federal constitutional right to informational privacy exists. Although the Supreme Court has assumed, without deciding, that the Constitution protects the individual "interest in avoiding disclosure of personal matters," *Nat'l Aeronautics & Space Admin. v. Nelson*, 562 U.S. 134, 138 (2011), the Court has not specifically held that a supposed constitutional right to informational privacy actually exists.[4] For its part, the D.C. Circuit has expressed "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information." *Am. Fed'n of Gov't Emps., AFL-CIO v. Dep't of House. & Urban Dev.,* 118 F.3d 786, 791 (D.C. Cir. 1997).

---

[4] Several justices have criticized that approach and expressly questioned the existence of a constitutional right to informational privacy. *See Nelson*, 562 U.S. at 159-60 (Scalia, J., concurring in the judgment) ("'[I]nformational privacy' seems like a good idea . . . [b]ut it is up to the People to enact those laws, to shape them, and, when they think it appropriate, to repeal them. A federal constitutional right to 'informational privacy' does not exist."); *id.* at 169 (Thomas, J., concurring in the judgment) ("I agree with Justice Scalia that the Constitution does not protect a right to informational privacy. No provision in the Constitution mentions such a right." (internal citations omitted))).

Even assuming such a right exists, EPIC's claim would still fail because the Commission has only requested information that is "publicly available." Kobach Decl., Exh. 3, at 1-2. Whatever the bounds of a supposed constitutional right to informational privacy, it does not extend to matters already in the public record. Indeed, courts have repeatedly held that "there is no question that an individual cannot expect to have a constitutionally protected privacy interest in matters of public record." *Doe v. City of N.Y.*, 15 F.3d 264, 268 (2d Cir. 1994) (citing *Cox Broadcasting Corp. v. Cohn*, 420 U.S. 469, 493-96 (1975)); *see also Doe v. Lockwood*, No. 95-3499, 1996 WL 367046, at *4 (6th Cir. June 27, 1996) (table) ("In order to sustain their claim that John Doe has a federal constitutional right to informational privacy, the Does must allege facts to show that the information regarding John Doe's HIV status was not already in the public realm."); *Lewis v. Delarosa*, No. C-15-2689, 2015 WL 5935311, at *3 (N.D. Cal. Oct. 13, 2015) ("Plaintiff's allegations that his right to informational privacy was violated when his non-private identification information was published on the internet is not included in even the outer confines of a federal right to informational privacy."); *Jones v. Lacey*, 108 F. Supp. 3d 573, 584-85 (E.D. Mich. 2015) (no right to informational privacy with respect to information that had been publicly released); *Pelosi v. Spota*, 607 F. Supp. 2d 366, 373 (E.D.N.Y. 2009) (same).

EPIC has not pled – much less established – that the Commission's explicit request only for "publicly available voter roll data," Kobach Decl. ¶ 4, encompasses *private* sensitive personal information not already available to the general public as a matter of public record.[5] Nor has

[5] The last four digits of a social security number are not generally considered private information. For example, Federal Rule of Civil Procedure 5.2(a)(1) provides that filings on an public docket may include "the last four digits of a social-security number." Fed. R. Civ. P. 5.2(a)(1). Furthermore, 52 U.S.C. § 21083(c), which governs computerized statewide voter registration list requirements as part of the Help America Vote Act, states that the last four digits

EPIC challenged the states' collection of that voter data or their designation of that information as publicly available. Because the Commission has only requested public information from the states, EPIC could never show that a constitutional right to informational privacy – even if it were to exist – has been violated.[6]

---

of a social security number may be used as part of the voter registration process for an election for federal office without running afoul of the Privacy Act.

[6] The Supreme Court's decision in *U.S. Department of Justice v. Reporters Committee for Freedom of the Press*, 489 U.S. 749 (1989), is not to the contrary. There, the Court held that for purposes of the Freedom of Information's Act's statutory limitation on the release of information that "could reasonably be expected to constitute an unwarranted invasion of personal privacy," 5 U.S.C. § 552(b)(7)(C), federal "rap sheets" need not be disclosed. The Court concluded that "[a]lthough much rap-sheet information is a matter of public record, the availability and dissemination of the actual rap sheet to the public is limited." *Reporters Comm.*, 489 U.S. at 743. Additionally, the fact that there was a "web of federal statutory and regulatory provisions that limits the disclosure of rap-sheet information," *id.* at 764-65, combined with "the fact that most States deny the general public access to their criminal-history summaries," *id.* at 767, permitted an agency to withhold the requested information under FOIA.

The *Reporters Committee* Court was explicit, however, that "[t]he question of the statutory meaning of privacy under the FOIA is, of course, not the same as . . . the question of whether an individual's interest in privacy is protected by the Constitution." *Id.* at 762 n.13 (citing *Paul v. Davis*, 424 U.S. 693, 712-14 (1976) (no constitutional privacy right affected by publication of name of arrested but untried shoplifter)). Following this direction, courts have "repeatedly stressed that *Reporters Committee* is inapposite on the issue of those privacy interests entitled to protection under the United States Constitution." *A.A. v. New Jersey*, 176 F. Supp. 2d 274, 305 (D.N.J. 2002) (citing *E.B. v. Verniero*, 119 F.3d 1077, 1100 n.21 (3d Cir. 1997)), *aff'd in part, remanded in part sub nom. A.A. ex rel. M.M. v. New Jersey*, 341 F.3d 206 (3d Cir. 2003); *see also Cutshall v. Sundquist*, 193 F.3d 466, 481 (6th Cir. 1999) (holding that *Reporters Committee* did not establish a constitutional right to prevent disclosure).

In any event, the instant case may be distinguished on its facts. Here, the Commission requested only publicly available information from the states, and plaintiff has not pled, much less proved, that such information is restricted or available to the public only for limited access.

IV. A TEMPORARY RESTRAINING ORDER WOULD HARM THE PUBLIC INTEREST

A party seeking a temporary restraining order or preliminary injunction must also demonstrate "that the balance of equities tips in [its] favor, and that an injunction is in the public interest." *Winter*, 555 U.S. at 20. "These factors merge when the Government is the opposing party." *Nken v. Holder*, 556 U.S. 418, 435 (2009).

Here, the public interest cuts against an injunction. The President charged the Commission with the important task of "study[ing] the registration and voting processes used in Federal elections." Exec. Order No. 13,799, § 3. The Commission must prepare a report that identifies laws that either enhance or undermine the American people's confidence in the integrity of the voting processes used in Federal elections. The Commission must also investigate "those vulnerabilities in voting systems and practices used for Federal elections that could lead to improper voter registrations and improper voting." *Id.*

As a necessary first step toward achieving these objectives, the Commission has begun to request information from the states, to be provided on a voluntary basis. EPIC seeks to enjoin these first steps, which will prevent the Commission from even beginning its work. The public interest lies in favor of allowing the Commission to begin collecting data so it can accomplish its important mission.

CONCLUSION

For the foregoing reasons, the Court should deny EPIC's emergency motion for a temporary restraining order.

Dated: July 5, 2017

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General
Civil Division

BRETT A. SHUMATE
Deputy Assistant Attorney General

ELIZABETH J. SHAPIRO
Deputy Director

/s/ Carol Federighi
CAROL FEDERIGHI
Senior Trial Counsel
JOSEPH E. BORSON
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
Phone: (202) 514-1903
Email: carol.federighi@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*, Defendants.	Civil Action No. 1:17-cv-1320 (CKK)

DECLARATION OF KRIS W. KOBACH

I, Kris W. Kobach, declare as follows:

1. I am the Secretary of State of Kansas, having served in that position since 2011. I am also the Vice-Chair of the Presidential Advisory Commission on Election Integrity (the "Commission"), which the President established on May 11, 2017, pursuant to Executive Order 13799. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine Americans' confidence in the integrity of the federal election process.

2. The information provided in this declaration is based on my personal knowledge and upon information provided to me in my official capacity as Vice-Chair of the Commission.

3. The Commission was established within the Executive Office of the President and is chaired by the Vice President. The membership, not more than fifteen, is appointed by the President. The members of the Commission come from federal, state, and local jurisdictions

across the political spectrum. The Commission, which is solely advisory, is charged with submitting a report to the President containing its findings and recommendations. The duties of the Commission are set forth in Executive Order 13799 (attached as Exhibit 1) and the Commission's Charter (attached as Exhibit 2). Pursuant to the Charter, the records of the Commission and any subcommittees shall be maintained pursuant to the Presidential Records Act of 1978.

4. In furtherance of the Commission's mandate, I directed that identical letters (with different addressees) be sent to the secretaries of state or chief election officers of each of the fifty states and the District of Columbia. The letters solicit the views and recommendations of the secretaries of state and request their assistance in providing to the Commission publicly-available voter roll data to enable the Commission to fully analyze vulnerabilities and issues related to voter registration and voting. Specifically, I asked for the following data, "if publicly available under the laws of your state": full first and last names of registrants; middle names or initials if available; addresses; dates of birth; political party (if recorded); last four digits of social security numbers; voter history (elections voted in) from 2006; active/inactive status; cancelled status; information regarding prior felony convictions; information regarding voter registration in another state; military status; and overseas citizen information. The information requested is similar to the information that states are required to maintain and to make available for public inspection under the National Voter Registration Act (NVRA) and the Help America Vote Act (HAVA). *See, e.g.*, 52 U.S.C. §§ 20507(i), 21083. The letter I sent to the Secretary of State of Alabama, which is representative of all the letters, is attached as Exhibit 3.

5. In these letters, I requested that the states respond by July 14, 2017, and described two methods for responding. I intended that narrative responses, not containing voter roll data,

be sent via email to the address provided in the letter. This email is a White House email address (in the Office of the Vice President) and subject to the security protecting all White House communications and networks. For voter roll data, I intended that the states use the Safe Access File Exchange ("SAFE"), which is a secure method of transferring large files up to two gigabytes (GB) in size. SAFE is a tested and reliable method of secure file transfer used routinely by the military for large, unclassified data sets. It also supports encryption by individual users. My letters state that "documents" submitted to the Commission will be made available to the public. That refers only to the narrative responses. With respect to voter roll data, the Commission intends to de-identify any such data prior to any public release of documents. In other words, the voter rolls themselves will not be released to the public by the Commission. The Commission intends to maintain the data on the White House computer system.

6. To my knowledge, as of July 5, 2017, no Secretary of State had yet provided to the Commission any of the information requested in my letter. I have read media reports that numerous states have indicated that they will decline to provide all or some portion of the information, in some cases because individual state law prohibits such transfer of information. However, it is my belief that there are inaccuracies in those media reports with respect to various states.

7. I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

***

Executed this 5th day of July 2017.

Kris W. Kobach

EXHIBIT 1

Federal Register
Vol. 82, No. 93
Tuesday, May 16, 2017

Presidential Documents

Title 3—

The President

Executive Order 13799 of May 11, 2017

Establishment of Presidential Advisory Commission on Election Integrity

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote fair and honest Federal elections, it is hereby ordered as follows:

Section 1. *Establishment.* The Presidential Advisory Commission on Election Integrity (Commission) is hereby established.

Sec. 2. *Membership.* The Vice President shall chair the Commission, which shall be composed of not more than 15 additional members. The President shall appoint the additional members, who shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience that the President determines to be of value to the Commission. The Vice President may select a Vice Chair of the Commission from among the members appointed by the President.

Sec. 3. *Mission.* The Commission shall, consistent with applicable law, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President that identifies the following:

(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 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.

Sec. 4. *Definitions.* For purposes of this order:

(a) The term "improper voter registration" means any situation where an individual who does not possess the legal right to vote in a jurisdiction is included as an eligible voter on that jurisdiction's voter list, regardless of the state of mind or intent of such individual.

(b) The term "improper voting" means the act of an individual casting a non-provisional ballot in a jurisdiction in which that individual is ineligible to vote, or the act of an individual casting a ballot in multiple jurisdictions, regardless of the state of mind or intent of that individual.

(c) The term "fraudulent voter registration" means any situation where an individual knowingly and intentionally takes steps to add ineligible individuals to voter lists.

(d) The term "fraudulent voting" means the act of casting a non-provisional ballot or multiple ballots with knowledge that casting the ballot or ballots is illegal.

Sec. 5. *Administration.* The Commission shall hold public meetings and engage with Federal, State, and local officials, and election law experts, as necessary, to carry out its mission. The Commission shall be informed by, and shall strive to avoid duplicating, the efforts of existing government entities. The Commission shall have staff to provide support for its functions.

Sec. 6. *Termination*. The Commission shall terminate 30 days after it submits its report to the President.

Sec. 7. *General Provisions*. (a) To the extent permitted by law, and subject to the availability of appropriations, the General Services Administration shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis.

(b) Relevant executive departments and agencies shall endeavor to cooperate with the Commission.

(c) Insofar as the Federal Advisory Committee Act, as amended (5 U.S.C. App.) (the "Act"), may apply to the Commission, any functions of the President under that Act, except for those in section 6 of the Act, shall be performed by the Administrator of General Services.

(d) Members of the Commission shall serve without any additional compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, to the extent permitted by law for persons serving intermittently in the Government service (5 U.S.C. 5701–5707).

(e) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(g) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,

May 11, 2017.

[FR Doc. 2017–10003

Filed 5–15–17; 8:45 am]

Billing code 3295–F7–P

EXHIBIT 2

CHARTER

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY

1. **Committee's Official Designation**. Presidential Advisory Commission on Election Integrity ("Commission").

2. **Authority**. The Commission is established in accordance with Executive Order 13799 of May 11, 2017, "Establishment of a Presidential Advisory Commission on Election Integrity," ("Order") and the provisions of the Federal Advisory Committee Act ("FACA"), as amended (5 U.S.C. App.).

3. **Objectives and Scope of Activities**. The Commission will, consistent with applicable law and the Order, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President of the United States ("President") that identifies the following:

    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 voting processes used in Federal elections; and
    c. those vulnerabilities in 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.

4. **Description of Duties**. The Commission will function solely as an advisory body.

5. **Agency or Official to Whom the Committee Reports**. The Commission shall provide its advice and recommendations to the President.

6. **Agency Responsible for Providing Support**. The General Services Administration ("GSA") shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission, to the extent permitted by law and on a reimbursable basis. However, the President's designee will be responsible for fulfilling the requirements of subsection 6(b) of the FACA.

7. **Estimated Annual Operating Costs and Staff Years**. The estimated annual costs to operate the Commission are approximately $250,000 in FY2017 and approximately $250,000 in FY2018, as needed, including approximately three full-time equivalent employees (FTEs) over the duration of the Commission.

8. **Designated Federal Officer**. Pursuant to 41 CFR § 102-3.105 and in consultation with the chair of the Commission, the GSA Administrator shall appoint a full-time or part-time federal employee as the Commission's Designated Federal Officer ("DFO"). The DFO will approve or

call all Commission meetings, prepare or approve all meeting agendas, attend all Commission meetings and any subcommittee meetings, and adjourn any meeting when the DFO determines adjournment to be in the public interest. In the DFO's discretion, the DFO may utilize other Federal employees as support staff to assist the DFO in fulfilling these responsibilities.

9. **Estimated Number and Frequency of Meetings**. Meetings shall occur as frequently as needed, called, and approved by the DFO. It is estimated the Commission will meet five times at a frequency of approximately 30-60 days between meetings, subject to members' schedules and other considerations.

10. **Duration and Termination**. The Commission shall terminate no more than two (2) years from the date of the Executive Order establishing the Commission, unless extended by the President, or thirty (30) days after it presents its final report to the President, whichever occurs first.

11. **Membership and Designation**.

    (a) The Vice President shall chair the Commission, which shall be composed of not more than fifteen (15) additional members.

    (b) Members shall be appointed by the President of the United States and shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience determined by the President to be of value to the Commission. Members of the Commission may include both regular Government Employees and Special Government Employees.

    (c) The Vice President may select a Vice Chair from among those members appointed by the President, who may perform the duties of the chair if so directed by the Vice President. The Vice President may also select an executive director and any additional staff he determines necessary to support the Commission.

    (d) Members of the Commission will serve without additional compensation. Travel expenses will be allowed, including per diem in lieu of subsistence, as authorized by law for persons serving intermittently in the Government service (5 U.S.C. 5701-5707), consistent with the availability of funds.

12. **Subcommittees**. The Chair of the Commission, in consultation with the DFO, is authorized to create subcommittees as necessary to support the Commission's work. Subcommittees may not incur costs or expenses without prior written approval of the Chair or the Chair's designee and the DFO. Subcommittees must report directly to the Commission, and must not provide advice or work products directly to the President, or any other official or agency.

13. **Recordkeeping**. The records of the Commission and any subcommittees shall be maintained pursuant to the Presidential Records Act of 1978 and FACA.

14. **Filing Date**. The filing date of this charter is June 23, 2017.

EXHIBIT 3

Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable John Merrill
Secretary of State
PO Box 5616
Montgomery, AL 36103-5616

Dear Secretary Merrill,

I serve as the Vice Chair for the Presidential Advisory Commission on Election Integrity ("Commission"), which was formed pursuant to Executive Order 13799 of May 11, 2017. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President of the United States that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine the American people's confidence in the integrity of federal elections processes.

As the Commission begins it work, I invite you to contribute your views and recommendations throughout this process. In particular:

1. What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections?
2. How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities?
3. What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer?
4. What evidence or information do you have regarding instances of voter fraud or registration fraud in your state?
5. What convictions for election-related crimes have occurred in your state since the November 2000 federal election?
6. What recommendations do you have for preventing voter intimidation or disenfranchisement?
7. What other issues do you believe the Commission should consider?

In addition, in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly-available voter roll data for Alabama, including, if publicly available under the laws of your state, 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.

You may submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files. You can access the SAFE site at https://safe.amrdec.army.mil/safe/Welcome.aspx. We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public. If you have any questions, please contact Commission staff at the same email address.

On behalf of my fellow commissioners, I also want to acknowledge your important leadership role in administering the elections within your state and the importance of state-level authority in our federalist system. It is crucial for the Commission to consider your input as it collects data and identifies areas of opportunity to increase the integrity of our election systems.

I look forward to hearing from you and working with you in the months ahead.

Sincerely,

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al*,

Defendants.

Civil Action No. 1:17-cv-1320 (CKK)

[PROPOSED] ORDER

It is hereby ORDERED that Plaintiff's Motion for a Temporary Restraining Order, ECF No. 3, is DENIED.

DATE:_____

_____

HON. COLLEEN KOLLAR-KOTELLY
UNITED STATES DISTRICT JUDGE

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 1:17-cv-1320 (CKK)

DEFENDANTS' RESPONSE TO THE COURT'S JULY 5, 2017, ORDER

In response to the Court's July 5, 2017, Order, ECF No. 9, Defendants attach the Second Declaration of Kris W. Kobach, which addresses each of the five enumerated questions identified in the Court's Order.

Dated: July 6, 2017

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General
Civil Division

BRETT A. SHUMATE
Deputy Assistant Attorney General

ELIZABETH J. SHAPIRO
Deputy Director

/s/ Joseph E. Borson
CAROL FEDERIGHI
Senior Trial Counsel
JOSEPH E. BORSON
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
Phone: (202) 514-1944
Email: joseph.borson@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER, Plaintiff, v. PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*, Defendants.	Civil Action No. 1:17-cv-1320 (CKK)

SECOND DECLARATION OF KRIS W. KOBACH

I, Kris W. Kobach, declare as follows:

As described in my declaration of July 5, 2017, I am the Vice Chair of the Presidential Advisory Commission on Election Integrity. I submit this second declaration in response to the Court's order of July 5, 2017, requesting answers to five enumerated questions. I have addressed each question below. The answers are based on my personal knowledge and upon information provided to me in my official capacity as Vice Chair of the Commission.

1. **Who are the current members of the Presidential Advisory Commission on Election Integrity, and what are their affiliations?**

   - Vice President Mike Pence, Vice President of the United States, *Chair* (R)
   - Secretary Kris Kobach, Secretary of State for Kansas, *Vice Chair* (R)
   - Secretary Connie Lawson, Secretary of State of Indiana (R)
   - Secretary Bill Gardner, Secretary of State of New Hampshire (D)
   - Secretary Matt Dunlap, Secretary of State of Maine (D)
   - Ken Blackwell, former Secretary of State of Ohio (R)
   - Commissioner Christy McCormick, Election Assistance Commission (R)
   - David Dunn, former Arkansas State Representative (D)
   - Mark Rhodes, Wood County, West Virginia Clerk (D)
   - Hans von Spakovsky, Senior Legal Fellow, Heritage Foundation (R)

2. **If there are no current members who are officials of a federal agency, what is the likelihood that an official of a federal agency will become a member of the Presidential Advisory Commission on Election Integrity in the near future? Identify any likely members who are currently officials of a federal agency.**

Christy McCormick is a member of the Election Assistance Commission (EAC). However, Ms. McCormick is not serving in her official capacity as a member of the EAC; she was selected based upon her experience in election law and administration, including as an employee of the U.S. Department of Justice. The Commission has no legal relationship with the EAC. The President has discretion to appoint additional members to the Commission. To my knowledge, however, no other federal agency officials are currently under consideration for appointment to the Commission.

3. **To what extent has or will the General Services Administration be involved in the collection and storage of data for the Presidential Advisory Commission on Election Integrity?**

At this time, there are no plans for the General Services Administration to collect or store any voter registration or other elections-related data for the Commission.

4. **Who is the current operator of the website https://safe.amrdec.army.mil/safe/Welcome.aspx?**

The U.S. Army Aviation and Missile Research Development and Engineering Center operates that website, which the White House uses for data transfers. *See* https://safe.amrdec.army.mil/safe/About.aspx.

5. **Who is responsible for collecting and storing data received via the website https://safe.amrdec.army.mil/safe/Welcome.aspx? Who will transfer that data to the Presidential Advisory Commission on Election Integrity?**

The Safe Access File Exchange (SAFE) is an application for securely exchanging files.

States will upload data to the SAFE website, and Commission staff will download the files from SAFE onto White House computers. As this is a Presidential advisory commission, the White House is responsible for collecting and storing data for the Commission. The Commission's Designated Federal Officer (an employee within the Office of the Vice President) will work with White House Information Technology staff to facilitate collection and storage.

I declare under penalty of perjury that the foregoing is true and correct to the best of my knowledge.

***

Executed this 6th day of July 2017.

Kris Kobach

Kris W. Kobach

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 1:17-cv-1320 (CKK)

DEFENDANTS' SUPPLEMENTAL BRIEF ON INFORMATIONAL STANDING

EPIC lacks informational standing, just as it lacks any other form of Article III standing. *See* ECF No. 8, at 5-7. Informational standing only applies when a statute *requires* the government to make specific, *preexisting* information public. EPIC seeks a Privacy Impact Assessment ("PIA") that the Commission did not (and was not required to) create. But informational standing does not apply when a plaintiff seeks to compel an agency to create something that does not already exist. EPIC "assert[s] a right to the informational product of [defendants'] programmatic activities, information which has not been withheld or misrepresented, but simply has not yet been generated." *Am. Farm Bureau v. E.P.A.*, 121 F. Supp. 2d 84, 97 (D.D.C. 2000). This amounts to a "generalized grievance" and "generalized interest in the enforcement of law," not a specific injury that supports standing. *Id.* (quoting *Judicial Watch, Inc. v. FEC*, 180 F.3d 277, 278 (D. C. Cir.1999)).

Informational standing is a "narrowly defined" theory of standing. *Common Cause v. FEC*, 108 F.3d 413, 420 (D.C. Cir. 1997). It exists when a plaintiff has been denied existing information to which it is statutorily entitled. *See Friends of Animals v. Jewell*, 828 F.3d 989, 992-93 (D.C. Cir. 2016). Informational standing is not a doctrine that allows a plaintiff to compel an agency to *create* a document to which, once it exists, the plaintiff will have a statutory entitlement. *See id.* And yet that is precisely the situation that EPIC finds itself in – it seeks to force the Commission to create a PIA which, it claims, it will then be entitled to view. That is not enough for standing

The D.C. Circuit has recently made clear that informational standing cannot be used to force an agency to make a written finding simply because, once made, that finding will be publically available to the plaintiff. In *Friends of Animals v. Jewell*, the court explained this principle in the context of the Endangered Species Act ("ESA"). *Id.* at 990-91. The ESA requires an agency to make a decision within 12 months as to whether a species should be listed on the Endangered Species List, and once it makes that decision, the agency must publish it in the Federal Register. *Id.* at 991. The plaintiff in *Friends of Animals* sued, claiming that the agency had not timely responded, and therefore it had not received the published finding to which it said it was entitled, causing it informational injury. Both the district and circuit courts rejected this argument because the information the plaintiff sought did not yet exist. "In truth, then, [plaintiff] is not seeking pre-existing 'information,' but is instead seeking to compel the Department to comply with the ESA by making a decision along the statute's timeline that will *generate* information. . . . [the plaintiff] has not alleged that the Department withheld any specific, concrete information *in its possession* concerning [the animals in question]; its

allegations, instead, focus on the Department's repeated failures to meet the various deadlines in the ESA's species-listing process." *Friends of Animals v. Jewell*, 115 F. Supp. 3d 107, 114 (D.D.C. 2015) (second emphasis added). The D.C. Circuit affirmed. It recognized that the agency "must publish [information] *after* making a given finding," but concluded that those publication requirements did not take effect *until* the agency actually made that finding in the first place. 828 F.3d at 933; *see also id.* ("By adopting this sequential procedural structure, Congress placed the Secretary under no obligation to publish any information in the Federal Register until after making a . . . finding."). Accordingly, there was no informational injury, and thus no standing.

The same principle applies here. The E-Government Act only requires disclosure of a PIA after it has already been created. *See* E-Government Act, 116 Stat. 2899, § 208(b)(1)(B)(iii) (stating that a PIA shall be made publically available, "if practicable," only "after completion of the review"). Just like the *Friends of Animals* plaintiff could not use the fact that an ESA finding must be published to force the agency to issue such a finding, EPIC cannot use the fact that a PIA should generally be made available as a "hook" to require the Commission to create a document it has not created (and, of course, it is not obligated to create).[1] It therefore lacks informational standing.

---

[1] Nor, unlike *Friends of Animals*, is it clear that the E-Government Act has a mandatory disclosure requirement. Section 208 of the E-Government Act states that an agency – which the Commission is not – shall "conduct a privacy impact assessment." 116 Stat 2899, § 208(b)(1)(B)(i). But it need only disclose the PIA "*if practicable* . . . ." *Id.* § 208(b)(1)(B)(iii) (emphasis added). The qualifier "if practicable" does not create an unqualified right to receive a PIA. *See e.g.*, *Friends of Animals*, 828 F.3d at 994 (informational standing only exists if statute "*guaranteed* a right to receive information in a particular form") (emphasis added).

Dated: July 7, 2017

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General
Civil Division

BRETT A. SHUMATE
Deputy Assistant Attorney General

ELIZABETH J. SHAPIRO
Deputy Director

/s/ Joseph E. Borson
CAROL FEDERIGHI
Senior Trial Counsel
JOSEPH E. BORSON
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
Phone: (202) 514-1944
Email: joseph.borson@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 1:17-cv-1320 (CKK)

DEFENDANTS' UNOPPOSED MOTION TO FILE SURREPLY

Defendants hereby move the Court for leave to file a short surreply in opposition to plaintiff's emergency motion for a temporary restraining order. In its reply brief filed yesterday, plaintiff for the first time identified the basis for its assertion of injury, and hence standing, and attached nine declarations by individual members attesting to their alleged injuries. Defendants have not had a chance to address these new allegations. Accordingly, good cause exists to grant the government's request to file a surreply to address the issue of standing. *See Hoskins v. Napolitano*, 842 F. Supp. 2d 8, 12 n.1 (D.D.C. 2012) (surreplies are allowed "when a reply is filed leaving 'a party . . . "unable to contest matters presented to the court for the first time"'" (quoting *Ben-Kotel v. Howard Univ.*, 319 F.3d 532, 536 (D.C. Cir. 2003))).

Undersigned counsel contacted counsel for plaintiff, Marc Rotenberg, who stated that plaintiff does not oppose this motion, on the condition that defendants not oppose plaintiff's request to file a sur-surreply.

The proposed surreply is attached as Exhibit 1 hereto.

For the foregoing reasons, the Court should grant defendants leave to file the attached surreply.

Dated: July 7, 2017

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General
Civil Division

BRETT A. SHUMATE
Deputy Assistant Attorney General

ELIZABETH J. SHAPIRO
Deputy Director

/s/ Carol Federighi
CAROL FEDERIGHI
Senior Trial Counsel
JOSEPH E. BORSON
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
Phone: (202) 514-1903
Email: carol.federighi@usdoj.gov

Counsel for Defendants

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 1:17-cv-1320 (CKK)

DEFENDANTS' SURREPLY IN OPPOSITION TO PLAINTIFF'S EMERGENCY MOTION FOR A TEMPORARY RESTRAINING ORDER

As stated in defendants' memorandum in opposition to plaintiff's emergency motion for a temporary restraining order ("TRO") (Doc. 8, at 6), it is well settled that, in order to establish the injury-in-fact needed to establish Article III standing as a representative of its members, a plaintiff-organization such as the Electronic Privacy Information Center ("EPIC") must "make specific allegations establishing that at least one identified member had suffered or would suffer harm" by "naming the affected member[]" and showing that he or she has "suffered the requisite harm." *Summers v. Earth Island Inst.*, 555 U.S. 488, 498-99 (2009). The same holds true at the subsequent TRO stage of a case, at which an associational plaintiff seeking injunctive relief must (among other things) demonstrate with evidence an imminent injury warranting extraordinary judicial relief. For the same reasons that the association must show an injury-in-fact through a

specifically named member to establish representational standing, the association must show an imminent injury through such a member to warrant TRO relief.

As defendants previously pointed out, EPIC's complaint failed to make any "specific allegations" naming any one of its members who would be harmed. *See Earth Island*, 555 U.S. at 498. Yesterday, for the first time in its reply brief, EPIC has filed declarations from nine members of its Advisory Board who claim an injury from the release of their voter-registration information. *See* Doc. 13, Ex. 1-9. Those Board members assert that they are registered to vote in six jurisdictions: California (Ex. 1, 3, 6), the District of Columbia (Ex. 5), Maine (Ex. 9), Maryland (Ex. 2), Massachusetts (Ex. 4, 8), and Minnesota (Ex. 7). However, as set forth below, EPIC's belated evidentiary showing is insufficient to establish, on a representational basis, either its Article III standing or an imminent injury warranting a TRO. These reasons further support and bolster the reasons set forth in defendants' opposition memorandum for the Court's lack of jurisdiction in this matter.

EPIC does not cite any case supporting the proposition that an association has standing to sue on behalf of *Advisory Board* members. In fact, a closer examination sparked by the declarations submitted by the Advisory Board members indicates that EPIC may not have "members" at all in the traditional sense, on whose behalf it could establish standing. *See* About EPIC, http://epic.org/epic/about.html (last visited July 6, 2017) (EPIC "ha[s] no clients, no customers, and no shareholders"). Nor has EPIC shown that it is the "functional equivalent of a traditional membership organization" that might be entitled to representational standing, because it has not shown, or even alleged, that it is "a representative of a special group," that its affiliates (such as the Advisory Board members) possess the "indicia of membership," such as electing the

officers and financing its activities, and that its "fortunes [are] tied closely to those of any members." *See Washington Legal Found. v. Leavitt*, 477 F. Supp. 2d 202, 209-12 (D.D.C. 2007); *see also Electr. Privacy Info. Ctr. v. U.S. Dep't of Educ.*, 48 F. Supp. 3d 1, 22 (D.D.C. 2014) (noting that "defendant raises serious questions about whether EPIC is an association made up of members that may avail itself of the associational standing doctrine" but declining to reach the issue). In any event, Advisory Board "members" would not be the type of members on whose behalf an organization could sue, as such individuals' role is to *advise* the organization -- the organization does not "represent" them. *See* About EPIC, http://epic.org/epic/about.html (last visited July 6, 2017) ("EPIC works closely with a distinguished advisory board"). Accordingly, EPIC cannot establish standing on a representational basis.

Even assuming EPIC could sue on behalf of its Advisory Board members, those members' allegations of imminent injury caused by a feared "disclosure" of their personal information that will allegedly be transferred to the Commission (*see* Decls. ¶ 7) are controverted by the current facts. At present, the declarants' information is not at risk of imminent transfer to the Commission by the states in which they are registered to vote. EPIC's own website shows that five of the six relevant jurisdictions have rejected the Commission's request for voter information. *See* https://epic.org/privacy/voting/pacei/ (attached as Ex. 1). And the sixth jurisdiction – Maine – has recently rejected the Commission's information request. *See* http://www.maine.gov/sos/news/2017/denyvoterreginfo.html (attached as Ex. 2); *see also* Ex. 3 (copy of letter from Maine Secretary of State denying request). Nor have plaintiff's declarants established that the feared "disclosure" of information transferred to the Commission is anything

more than speculative. The Commission has explained that the "voter rolls themselves will not be released to the public." Kobach Decl. (Doc. 8-1) ¶ 5.

In addition, even if EPIC could proceed in this case as a representative of its Advisory Board members, it could obtain relief only for those members for whom it has demonstrated a relevant injury. Under Article III, "[t]he remedy" sought must "be limited to the inadequacy that produced the injury in fact that the plaintiff has established." *Lewis* v. *Casey*, 518 U.S. 343, 357 (1996). "The actual-injury requirement would hardly serve [its] purpose . . . of preventing courts from undertaking tasks assigned to the political branches[,] if once a plaintiff demonstrated harm from one particular inadequacy in government administration, the court were authorized to remedy *all* inadequacies in that administration." *Id.*; *see City of Los Angeles* v. *Lyons*, 461 U.S. 95, 101-02 (1983). Equitable principles independently require that injunctions be no broader than "necessary to provide complete relief to the plaintiffs." *Madsen* v. *Women's Health Ctr., Inc.*, 512 U.S. 753, 765 (1994) (citation omitted). Thus, even if a TRO might otherwise be appropriate, the TRO could properly extend no further than a decree preventing the transfer of information concerning those Advisory Board members who would suffer an imminent injury from such a transfer.

In sum, EPIC lacks standing for the following reasons – first, EPIC does not have standing in its own right (Defs.' Opp. 6) because its advocacy and educational efforts in furtherance of its mission (Pl.'s Reply 20-21) are not Article III injuries and defendants' actions have not "perceptibly impaired" EPIC's activities. *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 920 (D.C. Cir. 2015); *Electr. Privacy Info. Ctr.*, 48 F. Supp. 3d at 22-24 (no standing where defendant's action "has not impeded EPIC's programmatic concerns and activities, but

fueled them"). Second, EPIC is not a membership organization entitled to avail itself of representational standing, *Washington Legal Found.*, 477 F. Supp. 2d at 209-12. Third, even if it was, its Advisory Board "members" are not members on whose behalf EPIC can sue. *Id.* (discussing "indicia of membership"). Fourth, even if EPIC could sue on behalf of Advisory Board members with cognizable Article III injuries, the declarations submitted do not establish such an injury here. The declarants' voter information is not at risk of being transferred to the Commission because their states are declining to do so and, even if it was, it is purely speculative at this point that the transfer will result in any "disclosure" that would infringe the declarants' privacy interests. Exs. 1-3; Kobach Decl. (Doc. 8-1) ¶ 5. Finally, to the extent that the Court finds that any declarant or declarants has or have established the necessary injury (which it shouldn't), any TRO should be limited to the state or states in which those declarants are registered to vote and should be no broader than that. *Madsen*, 512 U.S. at 765.

EPIC therefore has failed to establish its Article III standing or that it is entitled to entry of a TRO. Indeed, EPIC's failure to name any injured member at the pleading stage should alone warrant dismissal of its complaint for want of Article III jurisdiction.

CONCLUSION

For the foregoing reasons and the reasons stated in defendants' opposition memorandum, the Court should deny plaintiff's emergency motion for a temporary restraining order.

Dated: July 7, 2017

Respectfully submitted,

CHAD A. READLER
Acting Assistant Attorney General
Civil Division

BRETT A. SHUMATE
Deputy Assistant Attorney General

ELIZABETH J. SHAPIRO
Deputy Director

/s/ Carol Federighi
CAROL FEDERIGHI
Senior Trial Counsel
JOSEPH E. BORSON
Trial Attorney
United States Department of Justice
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
Phone: (202) 514-1903
Email: carol.federighi@usdoj.gov

Counsel for Defendants

EXHIBIT 1

Voter Privacy and the PACEI

Overview

The Presidential Advisory Commission on Election Integrity ("PACEI") was established on May 11, 2017, and is chaired by the Vice President. The President appoints the members of the committee, up to a maximum of 15 members, and those members serve without additional compensation (other than travel expenses). The stated purpose of the Commission is to "study the registration and voting processes used in Federal Elections" and to issue a report to the President addressing three specific issues. The Commission shall terminate 30 days after it submits its report to the President.

The Commission was the subject of controversy even before it was created. The President first announced the idea of the Commission in connection with his claim that 3-5 million illegal votes were cast in the 2016 election. The Commission also drew criticism when, as its first official action, it asked all 50 states and the District of Columbia to provide data from state voter rolls. More than forty states

have announced that they will partially or fully refuse the Commission's request.

Membership

The Executive Order establishing the Commission states that President "shall appoint additional members, who shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience that the President determines to be of value to the Commission. The Vice President may select a Vice Chair of the Commission from among the members appointed by the President." Vice President Pence has appointed Kansas Secretary of State Kris Kobach as the Vice Chair of the Committee. Reports indicate that the final commission will include six Democrats and Six Republicans. So far, four Democrats have been named: Mark Rhodes (a county clerk in West Virginia), David Dunn (a former Arkansas state representative), Matt Dunlap (the Secretary of State of Main), and Bill Gardner (the Secretary of State of New Hampshire). Other Republican members include Connie Lawson (the Secretary of State of Indiana), Luis Borunda (the Deputy Secretary of State of Maryland), and Hans Von Spakovsky (Heritage Foundation).

Mission and Report

The primary state purpose of the Commission is to issue a report to the President identifying the following:

- 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;
- 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

18-F-1517//0107

- those vulnerabilities in 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.

Request for State Voter Records

On June 28, 2017, the Commission's Vice Chair Kris Kobach sent a letter to election officials for all 50 states and the District of Columbia. In the letter, the Vice Chair requested "views and recommendations" on 7 specific questions. In addition, the Commission requested that the states "provide to the Commission the publicly-available voter roll data" including "if publicly available under the laws of your state":

- 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

The Commission requested that the states "submit [their] responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files." The Commission requested a response by July 14, 2017,

and notified the states that "any documents that are submitted to the full Commission will also be made available to the public." The other questions outlined in the letter are as follows: (1) What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections? (2) How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities? (3) What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer? (4) What evidence or information do you have regarding instances of voter fraud or registration fraud in your state? (5) What convictions for election-related crimes have occurred in your state since the November 2000 federal election? (6) What recommendations do you have for preventing voter intimidation or disenfranchisement? (7) What other issues do you believe the Commission should consider?

On the same day that the Commission requested voter roll data from all 50 states, the Department of Justice Civil Rights Division sent a parallel request for the "procedures for compliance with the statewide voter registration list maintenance provisions" required under the National Voter Registration Act ("NVRA"), 52 U.S.C. § 20501 et seq. and the Help America Vote Act ("HAVA"), 52 U.S.C. § 20901 et seq. These requirements apply to "covered states" and relate to the "maintenance of accurate statewide voter lists" as well as the use of "uniform statewide database requirements." The DOJ stated that their review would include "an analysis of voter registration data reported by each state to the U.S. Election Assistance Commission ("EAC") as part of its biennial Election Administration and Voting Survey ("EAVS"). The DOJ also requested "All statutes, regulations, written guidance, internal policies, or database user manuals that set out the procedures" related to four specified under the HAVA and NVRA. The DOJ also requested "an explanation of which election

officials are responsible for implementing" the voter registration list maintenance program.

State Responses

States Opposed to the Commission's Demand for Personal Voter Data

- California
- Delaware
- District of Columbia
- Kentucky
- Louisiana
- Maryland
- Massachusetts (according to news reports)
- Minnesota
- Mississippi
- New Mexico
- New York
- Oregon
- Pennsylvania
- South Dakota (according to news reports)
- Tennessee
- Virginia
- Wyoming (according to news reports)

States Transferring Some or All Personal Voter Data to the Commission

- Arizona
- Alaska
- Colorado
- Connecticut
- Georgia (according to news reports)

- Idaho (according to news reports)
- Indiana
- Iowa
- Kansas (according to news reports)
- Michigan
- Missouri
- Nevada
- New Hampshire (according to news reports)
- North Carolina
- North Dakota (according to news reports)
- Ohio
- Oklahoma (according to news reports)
- Texas
- Utah
- Vermont
- Wisconsin

States Reviewing or Still Awaiting the Commission's Demand for Personal Voter Data

- Alabama
- Florida
- Hawaii
- Illinois (according to news reports)
- Maine
- Montana (according to news reports)
- Nebraska (according to news reports)
- Rhode Island
- South Carolina (according to news reports)
- Washington

- West Virginia (according to news reports)

Legal Documents

EPIC v. Commission, No. 1:17-cv-01320-CKK (D.D.C. filed July 3, 2017)

- Complaint (July 3, 2017)
    - Exhibits
- EPIC Emergency Motion for Temporary Restraining Order (July 3, 2017)
    - Exhibits
    - Proposed Order
- Scheduling Order (July 3, 2017)

Other Documents

- Presidential Executive Order on the Establishment of Presidential Advisory Commission on Election Integrity (May 11, 2017), Exec. Order No. 13,799, 82 Fed. Reg. 22,389
- Letter from Kris W. Kobach, Vice Chair, PACEI, to Hon. Elaine Marshall, Secretary of State, North Carolina (June 28, 2017)
- Letter from T. Christian Herren, Jr., Chief, Voting Section, Civil Rights Division, U.S. Dep't of Justice, to Hon. Kim Westbrook Strach, Exec. Dir., State Bd. of Elections, North Carolina (June 28, 2017)

News

- Christopher Ingraham, Trump's voter-fraud commission wants to know voting history, party ID and address of every voter in the U.S., Washington Post (June 29, 2017)
- John Myers, California Secretary of State Refuses to Provide Voter Records for Trump's Election Fraud Probe, L.A. Times (June 29, 2017)

- Pam Fessler, White House Panel Asks States for their Voter Rolls, NPR (June 29, 2017)

EPIC Resources

- Voting Privacy
- Veasey v. Abbott
- Crawford v. Marion County Election Board

epic.org

Electronic Privacy Information Center
1718 Connecticut Ave, N.W.
Suite 200
Washington, DC 20009
202.483.1140
info[at]epic[dot]org

About EPIC
About EPIC
EPIC Advisory Board
EPIC Board and Staff
Contact EPIC
Fellowships and Clerkships
EPIC Bookstore
Privacy Policy
EPIC 2013 Annual Report
EPIC 2015 Brochure
EPIC Image Archive

Press Center
EPIC in the News
Press Kit
EPIC Alert
EPIC Commentaries
Videos
Events
Privacy Infographics

EPIC's Work
Litigation Docket
Amicus Briefs
APA Comments
EPIC Consumer Privacy Project
EPIC Domestic Surveillance Project
FOIA Cases
EPIC International Privacy Project
EPIC Open Government Project
EPIC Policy Project
EPIC Student Privacy Project
EPIC Congressional Testimony
EPIC Publications
Privacy Campaigns
Spotlight on Surveillance
EPIC Amicus Tracker

EPIC Affiliated Sites
Thepublicvoice.org
foia.rocks
privacycoalition.org
csisac.org

Hot Policy Issues
Algorithmic Transparency
Big Data
Cloud Computing
Consumer Privacy Bill of Rights
Cybersecurity
Donor Privacy
Drones and UAVs
EU Data Protection Directive
Facebook
Government Surveillance
Internet of Things
Location Privacy
Right to be Forgotten
Privacy Shield
Search Engine Privacy
Schrems Case (Safe Harbor)
Social Media Monitoring
Student Privacy
Uber Privacy Policy
Voter ID Laws

Electronic Privacy Information Center
1718 Connecticut Ave. NW Washington, DC 20009
More info

EXHIBIT 2

Department of the Secretary of State

Home → News → Elections Commission request Denied

FOR IMMEDIATE RELEASE
Monday, July 3, 2017
Contact: Kristen Muszynski/ 207-441-7638

Secretary Dunlap will deny Elections Commission request based on provisions of Maine law

AUGUSTA – Secretary of State Matthew Dunlap, in consultation with Attorney General Janet Mills, has determined that the State of Maine cannot fulfill the request for voter registration information from President Donald Trump's Advisory Commission on Election Integrity.

On Wednesday, June 28, 2017, Secretary Dunlap received a letter from Kansas Secretary of State Kris Kobach, on behalf of the commission. Secretary Kobach serves as vice chairman on the commission, of which Secretary Dunlap is also a member.

In his letter, Secretary Kobach states: "... in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly available voter roll data for Maine, including, if publicly available under the laws of your state, 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. ... We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public."

Due to the stipulation in Secretary Kobach's letter that "any documents submitted to the full Commission will also be made available to the public," Maine's Central Voter Registration (CVR) information cannot be released because the request is in direct conflict with Title 21-A MRSA section 196-A subsection 1, which states "information

contained electronically in the central voter registration system and any information or reports generated by the system are confidential and may be accessed only by municipal and state election officials for the purposes of election and voter registration administration."

In addition to the stipulation that the voter information cannot be made public, much of the requested information -- such as full date of birth, political party, Social Security number and voter history – are not available for release to the commission due to other restrictions in Maine's CVR statute.

"Maine citizens can be confident that our office will not release any data that is protected under Maine law, to the commission or any other requesting entity," said Secretary Dunlap.

Credits

EXHIBIT 3

STATE OF MAINE
OFFICE
OF THE
SECRETARY OF STATE

3 July 2017

The Honorable Kris Kobach
Vice Chair, Presidential Advisory Commission
On Election Integrity

Dear Secretary Kobach,

I am in receipt of yours of the 28th ultimo regarding the Commission's request for voter registration data from the State of Maine. As we do with any such request, we review the request to determine whether the requestor is a qualified entity that meets the parameters of law as described in Title 21-A MRSA § 196-A. We have consulted with our own senior election staff and the Office of the Attorney General to make a determination on the request.

Upon review, the request is denied.

Your correspondence informs us of the following: "Please be aware that any documents that are submitted to the full Commission will also be made available to the public." As a matter of law, that conflicts with State statute, which states in 21-A MRSA § 196-A §§ 1 that "Information contained electronically in the central voter registration system and any information or reports generated by the system are **confidential** and may be accessed only by municipal and state election officials for the purposes of election and voter registration administration…" (emphasis mine)

Because the statute on confidentiality is directory and the statute on access to the voter file is discretionary, it is not possible for my office to comply with the request and also comply with the law.

Please let me know if you have any questions about this determination, and I am and shall remain very humbly and sincerely yours,

Matthew Dunlap
Maine Secretary of State

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

ELECTRONIC PRIVACY INFORMATION CENTER,

Plaintiff,

v.

PRESIDENTIAL ADVISORY COMMISSION ON ELECTION INTEGRITY, *et al.*,

Defendants.

Civil Action No. 1:17-cv-1320 (CKK)

[PROPOSED] ORDER GRANTING DEFENDANTS' UNOPPOSED MOTION TO FILE SURREPLY

It is hereby ORDERED that Defendants' Unopposed Motion to File Surreply is GRANTED. The Clerk is directed to file Defendants' Surreply in Opposition to Plaintiff's Emergency Motion for a Temporary Restraining Order, with its three exhibits, in the docket of this case.

DATE: _____

_____
HON. COLLEEN KOLLAR-KOTELLY
UNITED STATES DISTRICT JUDGE

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.

Case: 1:17-cv-01320
Assigned To : Kollar-Kotelly, Colleen
Assign. Date : 7/3/2017
Description: TRO/PI

PLAINTIFF'S EMEREGNCY 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. _____

AFFIRMATION OF MARC ROTENBERG IN SUPPORT OF THE PLAINTIFF'S EMERGENCY MOTION FOR A TEMPORARY RESTRAINING ORDER

MARC ROTENBERG, an attorney admitted to practice before this Court, affirms the following to be true under the penalties of perjury:

1. I am the President and Executive Director of the Electronic Privacy Information Center ("EPIC") and counsel for EPIC in the above-captioned member. I submit this affirmation in support of the plaintiff's motion for a temporary restraining order in the above-captioned matter.

2. Annexed hereto as Exhibit 1 is a true and correct copy of Executive Order No. 13,799, 82 Fed. Reg. 22,389, issued by President Donald Trump on May 11, 2017.

3. Annexed hereto as Exhibit 2 is a true and correct copy of "Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity," a press release issued by the Office of the Vice President on June 28, 2017.

4. Annexed hereto as Exhibit 3 is a true and correct copy of a letter sent by Kris Kobach, Vice Chair of the Presidential Advisory Commission on Election Integrity, to Elaine Marshall, North Carolina Secretary of State, on June 28, 2017.

5. Annexed hereto as Exhibit 4 is a true and correct copy of a memorandum opinion issued by the U.S. District Court for the Northern District of Alabama in *Perkins v. Dep't of Veteran Affairs*, No. 07-310, on April 21, 2010.

6. Annexed hereto as Exhibit 5 is a true and correct copy of M-03-22, a memorandum issued by Josh Bolten, Director of the Office of Management and Budget, to the heads of executive departments and agencies on September 23, 2003.

7. Annexed hereto as Exhibit 6 is a true and correct copy of a screenshot of a Google Chrome security warning for the Secure Access File Exchange ("SAFE") website, captured on July 3, 2017 at 12:02 AM.

Respectfully Submitted,

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

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

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. _____

AFFIRMATION OF MARC ROTENBERG IN SUPPORT OF THE PLAINTIFF'S EMERGENCY MOTION FOR A TEMPORARY RESTRAINING ORDER

MARC ROTENBERG, an attorney admitted to practice before this Court, affirms the following to be true under the penalties of perjury:

1. I am the President and Executive Director of the Electronic Privacy Information Center ("EPIC") and counsel for EPIC in the above-captioned member. I submit this affirmation in support of the plaintiff's motion for a temporary restraining order in the above-captioned matter.

2. Annexed hereto as Exhibit 1 is a true and correct copy of Executive Order No. 13,799, 82 Fed. Reg. 22,389, issued by President Donald Trump on May 11, 2017.

3. Annexed hereto as Exhibit 2 is a true and correct copy of "Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity," a press release issued by the Office of the Vice President on June 28, 2017.

4. Annexed hereto as Exhibit 3 is a true and correct copy of a letter sent by Kris Kobach, Vice Chair of the Presidential Advisory Commission on Election Integrity, to Elaine Marshall, North Carolina Secretary of State, on June 28, 2017.

5. Annexed hereto as Exhibit 4 is a true and correct copy of a memorandum opinion issued by the U.S. District Court for the Northern District of Alabama in *Perkins v. Dep't of Veteran Affairs*, No. 07-310, on April 21, 2010.

6. Annexed hereto as Exhibit 5 is a true and correct copy of M-03-22, a memorandum issued by Josh Bolten, Director of the Office of Management and Budget, to the heads of executive departments and agencies on September 23, 2003.

7. Annexed hereto as Exhibit 6 is a true and correct copy of a screenshot of a Google Chrome security warning for the Secure Access File Exchange ("SAFE") website, captured on July 3, 2017 at 12:02 AM.

Respectfully Submitted,

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

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

LIST OF EXHIBITS

Exhibit 1	Exec. Order. No. 13,799, 82 Fed. Reg. 22,389 (May 11, 2017)
Exhibit 2	Press Release, Office of the Vice President, Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity (June 28, 2017)
Exhibit 3	Letter from Kris Kobach, Vice Chair, Presidential Advisory Commission on Election Integrity, to Elaine Marshall, Secretary of State, North Carolina (June 28, 2017)
Exhibit 4	*Perkins v. Dep't of Veteran Affairs*, No. 07-310 (N.D. Ala. Apr. 21, 2010)
Exhibit 5	Memorandum M-03-22 from Josh Bolten, Dir. of Office of Mgmt. & Budget, to Heads of Exec. Dep'ts & Agencies (Sep. 23, 2003)
Exhibit 6	Screenshot: Google Chrome Security Warning for Safe Access File Exchange ("SAFE") Website (July 3, 2017 12:02 AM)

Exhibit 1

Federal Register
Vol. 82, No. 93
Tuesday, May 16, 2017

Presidential Documents

Title 3—

The President

Executive Order 13799 of May 11, 2017

Establishment of Presidential Advisory Commission on Election Integrity

By the authority vested in me as President by the Constitution and the laws of the United States of America, and in order to promote fair and honest Federal elections, it is hereby ordered as follows:

Section 1. *Establishment.* The Presidential Advisory Commission on Election Integrity (Commission) is hereby established.

Sec. 2. *Membership.* The Vice President shall chair the Commission, which shall be composed of not more than 15 additional members. The President shall appoint the additional members, who shall include individuals with knowledge and experience in elections, election management, election fraud detection, and voter integrity efforts, and any other individuals with knowledge or experience that the President determines to be of value to the Commission. The Vice President may select a Vice Chair of the Commission from among the members appointed by the President.

Sec. 3. *Mission.* The Commission shall, consistent with applicable law, study the registration and voting processes used in Federal elections. The Commission shall be solely advisory and shall submit a report to the President that identifies the following:

(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 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.

Sec. 4. *Definitions.* For purposes of this order:

(a) The term "improper voter registration" means any situation where an individual who does not possess the legal right to vote in a jurisdiction is included as an eligible voter on that jurisdiction's voter list, regardless of the state of mind or intent of such individual.

(b) The term "improper voting" means the act of an individual casting a non-provisional ballot in a jurisdiction in which that individual is ineligible to vote, or the act of an individual casting a ballot in multiple jurisdictions, regardless of the state of mind or intent of that individual.

(c) The term "fraudulent voter registration" means any situation where an individual knowingly and intentionally takes steps to add ineligible individuals to voter lists.

(d) The term "fraudulent voting" means the act of casting a non-provisional ballot or multiple ballots with knowledge that casting the ballot or ballots is illegal.

Sec. 5. *Administration.* The Commission shall hold public meetings and engage with Federal, State, and local officials, and election law experts, as necessary, to carry out its mission. The Commission shall be informed by, and shall strive to avoid duplicating, the efforts of existing government entities. The Commission shall have staff to provide support for its functions.

Sec. 6. *Termination.* The Commission shall terminate 30 days after it submits its report to the President.

Sec. 7. *General Provisions.* (a) To the extent permitted by law, and subject to the availability of appropriations, the General Services Administration shall provide the Commission with such administrative services, funds, facilities, staff, equipment, and other support services as may be necessary to carry out its mission on a reimbursable basis.

(b) Relevant executive departments and agencies shall endeavor to cooperate with the Commission.

(c) Insofar as the Federal Advisory Committee Act, as amended (5 U.S.C. App.) (the "Act"), may apply to the Commission, any functions of the President under that Act, except for those in section 6 of the Act, shall be performed by the Administrator of General Services.

(d) Members of the Commission shall serve without any additional compensation for their work on the Commission, but shall be allowed travel expenses, including per diem in lieu of subsistence, to the extent permitted by law for persons serving intermittently in the Government service (5 U.S.C. 5701–5707).

(e) Nothing in this order shall be construed to impair or otherwise affect:

(i) the authority granted by law to an executive department or agency, or the head thereof; or

(ii) the functions of the Director of the Office of Management and Budget relating to budgetary, administrative, or legislative proposals.

(f) This order shall be implemented consistent with applicable law and subject to the availability of appropriations.

(g) This order is not intended to, and does not, create any right or benefit, substantive or procedural, enforceable at law or in equity by any party against the United States, its departments, agencies, or entities, its officers, employees, or agents, or any other person.

THE WHITE HOUSE,
May 11, 2017.

[FR Doc. 2017–10003
Filed 5–15–17; 8:45 am]
Billing code 3295–F7–P

Exhibit 2

the WHITE HOUSE

The White House
Office of the Vice President

For Immediate Release June 28, 2017

Readout of the Vice President's Call with the Presidential Advisory Commission on Election Integrity

This morning, Vice President Mike Pence held an organizational call with members of the Presidential Advisory Commission on Election Integrity. The Vice President reiterated President Trump's charge to the commission with producing a set of recommendations to increase the American people's confidence in the integrity of our election systems.

"The integrity of the vote is a foundation of our democracy; this bipartisan commission will review ways to strengthen that integrity in order to protect and preserve the principle of one person, one vote," the Vice President told commission members today.

The commission set July 19 as its first meeting, which will take place in Washington, D.C.

Vice Chair of the Commission and Kansas Secretary of State Kris Kobach told members a letter will be sent today to the 50 states and District of Columbia on behalf of the Commission requesting publicly-available data from state voter rolls and feedback on how to improve election integrity.

Exhibit 3

Presidential Advisory Commission on Election Integrity

June 28, 2017

The Honorable Elaine Marshall
Secretary of State
PO Box 29622
Raleigh, NC 27626-0622

Dear Secretary Marshall,

I serve as the Vice Chair for the Presidential Advisory Commission on Election Integrity ("Commission"), which was formed pursuant to Executive Order 13799 of May 11, 2017. The Commission is charged with studying the registration and voting processes used in federal elections and submitting a report to the President of the United States that identifies laws, rules, policies, activities, strategies, and practices that enhance or undermine the American people's confidence in the integrity of federal elections processes.

As the Commission begins it work, I invite you to contribute your views and recommendations throughout this process. In particular:

1. What changes, if any, to federal election laws would you recommend to enhance the integrity of federal elections?
2. How can the Commission support state and local election administrators with regard to information technology security and vulnerabilities?
3. What laws, policies, or other issues hinder your ability to ensure the integrity of elections you administer?
4. What evidence or information do you have regarding instances of voter fraud or registration fraud in your state?
5. What convictions for election-related crimes have occurred in your state since the November 2000 federal election?
6. What recommendations do you have for preventing voter intimidation or disenfranchisement?
7. What other issues do you believe the Commission should consider?

In addition, in order for the Commission to fully analyze vulnerabilities and issues related to voter registration and voting, I am requesting that you provide to the Commission the publicly-available voter roll data for North Carolina, including, if publicly available under the laws of your state, 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.

You may submit your responses electronically to ElectionIntegrityStaff@ovp.eop.gov or by utilizing the Safe Access File Exchange ("SAFE"), which is a secure FTP site the federal government uses for transferring large data files. You can access the SAFE site at https://safe.amrdec.army.mil/safe/Welcome.aspx. We would appreciate a response by July 14, 2017. Please be aware that any documents that are submitted to the full Commission will also be made available to the public. If you have any questions, please contact Commission staff at the same email address.

On behalf of my fellow commissioners, I also want to acknowledge your important leadership role in administering the elections within your state and the importance of state-level authority in our federalist system. It is crucial for the Commission to consider your input as it collects data and identifies areas of opportunity to increase the integrity of our election systems.

I look forward to hearing from you and working with you in the months ahead.

Sincerely,

Kris Kobach

Kris W. Kobach
Vice Chair
Presidential Advisory Commission on Election Integrity

Exhibit 4

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

JIM HENRY PERKINS and JESSIE FRANK QUALLS, on their own behalf and on the behalf of all others similarly situated,

Plaintiffs,

v. **CV No. 2:07-310-IPJ**

UNITED STATES DEPARTMENT OF VETERANS AFFAIRS; et al.

Defendants.

MEMORANDUM OPINION

This case is before the court upon remand from the Eleventh Circuit to conduct a "claim-by-claim" analysis to determine the validity of plaintiffs' remaining challenges brought under the Administrative Procedures Act ("APA"), 5 U.S.C. § 551 *et seq.*, and seeking to enforce provisions of the Privacy Act, 5 U.S.C. § 552a; the E-Government Act of 2002, 44 U.S.C. § 3501 note; and the Veterans Benefits, Health Care, and Information Technology Act of 2006, 38 U.S.C. § 5724. Only counts two, five, six, and eight remain, and the court examines each claim in turn.

Factual Background

On January 22, 2007, an employee of the U.S. Department of Veterans

Affairs ("VA") reported an external hard drive containing personally identifiable information and individually identifiable health information of over 250,000 veterans was missing from the Birmingham, Alabama Medical Center's Research Enhancement Award Program ("REAP"). VA Office of Inspector General ("OIG") Report, at 7. The IT Specialist responsible for the external hard drive, "John Doe," used the hard drive to back up data on his computer and other data from a shared network drive.[1] The hard drive is thought to contain the names, addresses, social security numbers ("SSN"), dates of birth, phone numbers, and medical files of hundreds of thousands of veterans and also information on more than 1.3 million medical providers. VA OIG Report at 7, 9 (doc. 33-2). To date, it has not been recovered.

John Doe was an IT Specialist working for the Birmingham REAP, a program that focused on "changing the practices of health care providers to ensure that they provide the latest evidence-based treatment, and on using VA databases

---

[1]The REAP Director approved the purchase of external hard drives as a means to provide more space to the Medical Center's near-full server. VA OIG Report, at 15. No policy required the protection of sensitive data on removable computer storage devices unless such devices were to be carried outside a VA facility. *Id.* at 16. The REAP Director claimed the Information Security Officer ("ISO") conferred with him in making the decision to purchase the external hard drives, but the ISO claimed he was not involved and did not know of the need for additional server space. The VA OIG concluded no one made a timely request to the ISO for additional space. VA OIG Report, at 15.

to link the care of VA patients to more general information on the population as a whole." *Id.* at 3. To reach these goals, the Birmingham REAP collects data on patients and medical providers from multiple sources for dozens of separate research projects." *Id.* The Data Unit of the Birmingham REAP was comprised of the Data Unit Manager, three IT Specialists, and two student program support Assistants. *Id.* at 4. John Doe worked "with national VA databases and design[ed] statistical programs to support Birmingham REAP research projects." *Id.*

The VA OIG identified three projects for which John Doe was conducting research. The first "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure"; the second "involved examining the quality of care to patients following myocardial infarction . . ., and attempted to determine whether certain demographic characteristics of the medical providers, such as their age, impacted the care rendered to these patients"; and the third "involved using a patient survey to identify use of over-the-counter medications in patients taking prescription medications and link the information obtained to various VA databases to determine whether patients suffered any adverse effects from the combination of medications." *Id.* at 22, 25, 30. In gathering the information needed to complete these projects, John Doe improperly received

access to various databases and stores of information, and various components of the VA improperly released information to John Doe or gave John Doe such access. *Id.* at 22-33. He was therefore able "to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of the projects he was working on. [The OIG] believe[s] much of this information was stored on the missing external hard drive." *Id.* at 22. Accurate reporting of what information was on the external hard drive has been difficult because the hard drive is still missing; John Doe encrypted or deleted multiple files from his computer after reporting the data missing; and John Doe was not initially forthright with criminal investigators. *Id.* at ii.

After John Doe reported the missing hard drive on January 22, 2007, the VA Security Operations Center ("SOC") was immediately notified. *Id.* at 7. The SOC wrote a report and provided it to the VA OIG on January 23, 2007; on that same day, an OIG criminal investigator came to the Birmingham VAMC and conducted an interview. The Federal Bureau of Investigation became involved in the investigation on January 24, 2007. A forensic analysis of John Doe's computer began on January 29, 2007, and on February 1, 2007, the OIG began to analyze what data could have been on the missing hard drive. *Id.* at 8, 9. Press releases dated on February 2 and 10, 2007, discussed the loss of the hard drive and the information it contained.

> Subsequent to the reported loss of the Birmingham REAP data but prior to receiving the results of the OIG analysis of this data on February 7, 2007, VA senior management concluded that anyone whose SSN was thought to be contained in any of the missing files, irrespective of the ability of anyone possessing this data to match an SSN with a name or any other personal identifier, should be notified and offered credit protection. The basis for this decision was a memorandum issued on November 7, 2006. . . . The memorandum states that "in the event of a data loss involving individual and personal information. . . VA officials have a responsibility to notify the individual(s) of the loss in a timely manner and to offer these protection services."

Id. at 11. The VA sent letters to those individuals whose information was thought to be compromised by the data breach, which gave them the option of one year of free credit monitoring services. *Id.* at 12.

The VA had also requested the Department of Health and Human Services to perform a risk analysis focusing on the Centers for Medicaid and Medicare Services ("CMS") data involved in the breach. *Id.* The missing external hard drive contained approximately 1.3 million health care providers' information,

including the SSNs of 664,165 health care providers. *Id.* On March 28, 2007, the CMS Chief Information Officer and Director sent a letter to the VA Assistant Secretary for Office of Information and Technology that stated, based on the CMS's completed independent risk analysis:

> [T]here is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned. The letter requested that "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file."

Id. From April 17 to May 22, 2007, the VA sent notification letters to the 1.3 million health care providers. *Id.* By May 31, 2007, it sent additional letters offering one year of credit monitoring to the 664,165 health care providers whose SSNs appeared to be on the hard drive. VA OIG Report, at 12.

Analysis

A valid claim under the APA must attack agency action, which is defined as "includ[ing] the whole or a part of an agency rule, order, license, sanction, relief or the equivalent or denial thereof, or failure to act." *Fanin v. U.S. Dep't of*

Veterans Aff., 572 F.3d 868, 877 (11th Cir. 2009) (citing 5 U.S.C. § 551(13)).

> If the claim attacks an agency's action, instead of failure to act, and the statute allegedly violated does not provide a private right of action, then the "agency action" must also be a "final agency action." [5 U.S.C. § 704; *see also Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 61-62, 124 S.Ct. 2373, 2379 (2004)]. "To be considered 'final,' an agency's action: (1) must mark the consummation of the agency's decisionmaking process–it must not be of a merely tentative or interlocutory nature; and (2) must be one by which rights or obligations have been determined, or from which legal consequences will flow. *U.S. Steel Corp. v. Astrue*, 495 F.3d 1272, 1280 (11th Cir. 2007)(quoting *Bennett v. Spear*, 520 U.S. 154, 177-78, 117 S.Ct. 1154, 1168 (1997)).

Id. However, if the claim challenges a failure to act, the court may compel "agency action unlawfully withheld or unreasonably delayed. . . only where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required* to take." *Id.* at 877-878 (citing *Norton*, 542 U.S. at 64) (emphasis in original).

Further, the court notes the remaining claims seek only injunctive and

declaratory relief. Such relief may be granted only if the plaintiffs demonstrate that they are "likely to suffer future injury." *City of Los Angeles v. Lyons*, 461 U.S. 95, 105, 103 S.Ct. 1660, 1667 (1983); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564, 112 S.Ct. 2130, 2138 (1992) (citing *Lyons*, 461 U.S. at 102) ("'Past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief.'"); *Seigel v. LePore*, 234 F.3d 1163, 1176-77 (11th Cir. 2000) (*en banc*) ("As we have emphasized on many occasions, the asserted irreparable injury "must be neither remote nor speculative, but actual and imminent.") (citations omitted). *Emory v. Peeler*, 756 F.2d 1547, 1552 (11th Cir. 1985) (To grant declaratory relief, "there must be a substantial continuing controversy between parties having adverse legal interests. The plaintiff must allege facts from which the continuation of the dispute may be reasonably inferred. Additionally, the continuing controversy . . . must be real and immediate, and create a definite, rather than speculative threat of future injury.").

Count Two

The plaintiffs claim that the VA failed "to create and maintain an accounting of the date, nature, and purpose of its disclosures" pursuant to the Privacy Act, 5 U.S.C. § 552a(c)(1), when John Doe accessed VA files to complete

VA projects. Joint Status Report ("JSR"), at 8 (doc. 56). The Privacy Act requires

> [e]ach agency, with respect to each system of records under its control, shall–
>
> (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of–
>
> (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and
>
> (B) the name and address of the person or agency to whom the disclosure is made. . .

5 U.S.C. § 552a(c)(1). Under the exception provided in subsection (b)(1), agencies need not provide an accounting for disclosures made to "officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). Accordingly, to the extent John Doe needed the information that he accessed to perform his duties, the VA had no obligation to account.

To the extent John Doe had no need for the information contained on the external hard drive in the performance of his duties, the plaintiffs must show the disclosure was pursuant to one of the provisions in 5 U.S.C. § 552a(b)(3)-(12).

See 5 U.S.C. § 552a(c)(1)(A). After failing to argue in the JSR that any of those subsections apply, plaintiffs now claim that the VA's disclosure to John Doe falls under 5 U.S.C. § 552a(b)(5), which requires accounting when the disclosure is "to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable."

However, the accounting requirement in 5 U.S.C. § 552a(b)(5) is not triggered by the activity at issue in this case. An accounting is required only upon a disclosure to a recipient described in that subsection. Although "recipient" is not defined in the Privacy Act, it does not stand to reason that an agency that maintains records needed by one of its own researchers to fulfill his duties would be required to provide *itself* with "advance adequate written assurance that the record will be used solely as a statistical research or reporting record." Indeed, pertinent legislative history and Office of Management and Budget ("OMB") regulations suggest that an accounting was only intended when the disclosures were to individuals or agencies outside the agency maintaining the record. *See* S. REP. NO. 93-1183 (1974) *reprinted in* U.S. CODE CONGRESSIONAL AND ADMINISTRATIVE NEWS, 6916, 6967 (stating that subsection 201(b)(4) "[r]equires any federal agency that maintains a personal information system or file to maintain an accurate accounting of the date, nature, and purpose of nonregular access

granted to the system, and each disclosure of personal information made to any person *outside the agency, or to another agency. . . .*") (emphasis added); H.R. No. 93-1416, 2 (describing the summary and purpose of the Act as "requir[ing] agencies to keep an accounting of transfers of personal records *to other agencies and outsiders*"); 40 Fed. Reg. 28955 (July 9, 1975) (differentiating between "agencies disclosing records" and "recipient agencies" in the context of 5 U.S.C. § 552a(b)(5)).

Even if subsection (b)(5) is applicable in this case, the plaintiffs argue only that John Doe gave an advance adequate written assurance before accessing information from only one database, the Veterans Integrated Service Network ("VISN") 7 Data Warehouse. Plaintiff's Response (doc. 64) at 4. Accordingly, subsection (b)(5) applies only for John Doe's access to the VISN 7 Data Warehouse to perform research for "Project 1," which involved diabetes management research. *See* VA OIG Report, at 22. Moreover, the plaintiffs cannot show that any failure to account for John Doe's access to the VISN 7 Data Warehouse to research diabetes management is causing them harm. Although the plaintiffs are upset about the loss of their personal information and the prospect of potential credit fraud in the future, any accompanying harm is attributable to the

loss of the information in the first place, *not* the purported failure to account.[2] Thus, even assuming *arguendo* that 5 U.S.C. § 552a(b)(5) applies, the plaintiffs cannot show that the alleged harm is fairly traceable to the VA's conduct, a deficiency fatal to their claim. *See Allen v. Wright*, 468 U.S. 737, 753 & n.19, 104 S.Ct. 3315, 3325 & n.19 (1984) (plaintiffs do not have standing where they failed to allege injuries that are caused by the defendants).

Because of these sufficient and independent reasons, the plaintiffs have not shown that the VA failed to take discrete agency action that it was required to take. Accordingly, the court finds that the plaintiffs have failed to state a claim upon which relief can be granted, and Count Two is due to be **DISMISSED**.

---

[2]The plaintiffs urge, "The Veterans have a right to know what information [was on the hard drive]. They deserve to know the 'purpose' for which John Doe was using the information," Plaintiff's Response, at 8 (doc. 64). However, the VA OIG report details, to the extent determinable, the information on the hard drive and the purpose for which John Doe was accessing the information. The VA OIG Report states that the hard drive is believed to contain "personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the [CMS], on over 1.3 million medical providers." VA OIG Report, at i. Moreover, it was difficult for the VA to make such a determination, as John Doe was not candid when he was interviewed; he deleted or encrypted files from his computer after the hard drive went missing; and he tried to hide the extent, magnitude, and impact of the missing data. *Id.* at ii. Lastly, the plaintiffs know that the purpose John Doe was accessing the VISN 7 Data Warehouse was related to his research for "Project 1," *id.* at 22-23, which "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure," VA OIG Report, at 22.

Count Five

Count Five involves the VA's alleged failure to establish appropriate safeguards in violation of the Privacy Act, 5 U.S.C. § 552a(e)(10). The plaintiffs have failed to argue that the alleged conduct of the VA constituted a failure of discrete agency action that the VA was required to take, but request that Count Five "move forward as detailed in the Plaintiffs' Statement in the Joint Report." Plaintiff's Brief, at 13 (doc. 64). In the Joint Status Report, the plaintiffs devote just over one page to briefing this issue and cite 5 U.S.C. § 552a(e)(10),[3] arguing that the VA failed to enforce this subsection in the numerous ways listed in their complaint.[4] Joint Status Report ("JSR"), at 10-11 (doc. 56). The plaintiffs then

---

[3]5 U.S.C. § 552a(e)(10) requires the VA to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

[4]Plaintiffs cite specifically to paragraph 80 of the Second Amended Complaint (doc. 21), which states:

> Among other things, Defendants' failures include operating a computer system or database from which an employee, including John Doe, can download or copy information, like the Personal Information and the Medical Information, onto the VA External Hard Drive without proper encryption and when not necessary to perform his or her duties; failing to conduct a data access inventory for John Doe and other VA employees and contractors with access to the VA's office at the Pickwick Conference Center; failing to provide software that would require or enable encryption of data downloaded or copied

ask the court for an injunction forcing full implementation and compliance "with Handbook 6500 and other procedures and policies put in place in Birmingham by the VA in response to this incident, to conduct an independent audit of its compliance, and to file that audit with the court." Plaintiff's Response, at 14 (doc. 64) (footnotes added). Such an injunction is untenable.

Handbook 6500 is a seventy-one page (seven appendices excluded) document that details the responsibilities of almost two dozen information security personnel and dozens of policies and procedures. As pointed out by the defense, policies explained in the Handbook include maintaining the temperature in the building and proper use of the facsimile machines. In addition, the "other procedures and policies" put in place at the Birmingham facility are also

---

> to mobile hard drives and devices, like the VA External Hard Drive from VA computers and databases at the VA offices and facilities in the Birmingham, Alabama area; failing to secure the VA External Hard Drive under lock and key when not in the immediate vicinity of John Doe; failing to house and protect the VA External Hard Drive to reduce the opportunities for unauthorized access, use, or removal; failing to provide intrusion detection systems at the VA office at the Pickwick Conference Center; failing to store the VA External Hard Drive in a secure area that requires proper escorting for access; failing to require and conduct appropriate background checks on all VA employees and contractors with access to the VA Office in the Pickwick Conference Center; and failing to protect against the alienation and relinquishment of control over the VA External Hard Drive, causing the Personal Information and Medical Information to be exposed to unidentified third parties.

Second Amended Complaint (doc. 21), ¶ 80.

numerous. *See e.g.*, VA Directive 6504 (doc. 61-3) (governing the transmission, transportation and use of, and access to, VA data outside VA facilities); VA Handbook 6500, at 7 (doc. 61-4) (a seventy-one page document "establish[ing] the foundation for VA's comprehensive information security program and its practices that will protect the confidentiality, integrity, and availability of information"); Medical Center Memo 00-ISO-02 (doc. 61-5) ("assign[ing] responsibility and establish[ing] procedures for managing computer files at the Birmingham VA Medical Center"); Medical Center Memo 00-ISO-05 (doc. 61-6) (requiring VA employees at the Medical Center to get permission before use of removable storage media, especially Universal Serial Bus ("USB") devices, and requiring written permission for the removal of sensitive information from VA facilities); Information Security Program VISN 7 AIS Operational Security Policy (doc. 61-9) (establishing procedures to implement a "structured program to safeguard all IT assets"); Memorandum 10N7-077 of VISN 7 VA Southeast Network (doc. 61-10) (stating "It is the policy of VISN 7 that no sensitive information ([personal health information or personal identifiable information]) will be stored on the storage media of any device without encryption or where the device is not *physically secured* to prevent accidental loss of sensitive information in the event of theft") (emphasis in original).

Cases that suggest a broad injunction enforcing all of these policies is

appropriate are "relic[s] of a time when the federal judiciary thought that structural injunctions taking control of executive functions were sensible. That time has past." *Rahman v. Chertoff*, 530 F.3d 622, 626 (7th Cir. 2008). "The limitation to discrete agency action precludes the kind of broad programmatic attack [the Supreme Court] rejected in *Lujan v. National Wildlife Federation*, 497 U.S. 871, 110 S.Ct 3177, 111 L.Ed.2d 695 (1990)." *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64, 124 S.Ct. 2373, 2379-2380 (2004); *see Lujan*, 497 U.S. at 891 When presented with similar circumstances in *Lujan*, the Supreme Court responded:

> Respondent alleges that violation of the law is rampant within this program-failure to revise land plans in proper fashion, failure to submit certain recommendations to Congress, failure to consider multiple use, inordinate focus upon mineral exploitation, failure to provide required public notice, failure to provide adequate environmental impact statements. Perhaps so. But respondent cannot seek *wholesale* improvement of this program by court decree, rather than in the office of the Department or the halls of Congress, where programmatic improvements are normally made.

Lujan, 497 U.S. at 891. Courts are not empowered to compel "compliance with

broad statutory mandates," *Norton*, 542 U.S. at 66-67, nor can they engage in general review of an agency's day-to-day operations to ensure such compliance. *Id.*; *Lujan*, 497 U.S. at 899.

Even if this court could pass on such a generalized challenge, the court is convinced that Count Five is moot.

> "'[A] case is moot when the issues presented are no longer "live" or the parties lack a legally cognizable interest in the outcome.' " *County of Los Angeles v. Davis,* 440 U.S. 625, 631, 99 S.Ct. 1379, 59 L.Ed.2d 642 (1979) (quoting *Powell v. McCormack,* 395 U.S. 486, 496, 89 S.Ct. 1944, 23 L.Ed.2d 491 (1969)). The underlying concern is that, when the challenged conduct ceases such that " 'there is no reasonable expectation that the wrong will be repeated,' " *United States v. W.T. Grant Co.,* 345 U.S. 629, 633, 73 S.Ct. 894, 97 L.Ed. 1303 (1953), then it becomes impossible for the court to grant " 'any effectual relief whatever' to [the] prevailing party," *Church of Scientology of Cal. v. United States,* 506 U.S. 9, 12, 113 S.Ct. 447, 121 L.Ed.2d 313 (1992) (quoting *Mills v. Green,* 159 U.S. 651, 653, 16 S.Ct. 132, 40 L.Ed. 293 (1895)).

City of Erie v. Pap's A.M., 529 U.S. 277, 287, 120 S.Ct. 1382, 1390 (2000).

Because the evidence submitted to the court shows that new security procedures and policies have been implemented and the deficiencies revealed in the VA OIG Report have been remedied, there is no "live" issue for which this court can grant effectual relief.

Count Six

In Count Six, the plaintiffs claim that the VA failed to perform a privacy impact assessment ("PIA") pursuant to the E-Government Act of 2002 when it procured the external hard drives. Pursuant to the E-Government Act, agencies must perform a PIA before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form." 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(1)(A)). The definition of "information technology" includes "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)). The disputed issue is whether the purchase of the external hard drives triggered the duty to perform a PIA.

The plaintiffs claim that the inclusion of "any equipment" in the definition of information technology brings the hard drives within the meaning of the term, thereby requiring the PIA. However, such an interpretation is implausible, as it would require government agencies that maintain personal information on individuals to conduct or update a PIA each time it purchases any computer, monitor, router, telephone, calculator, or other piece of equipment involved in a system that stores, analyzes, or manages the data. Rather, the purchase of several external hard drives, seems to be a "minor change[] to a system or collection that do[es] not create new privacy risks," and therefore does not require a PIA. *See* M-03-22, Attachment A 2.B.3.g., Office and Management and Budget ("OMB") Guidance Implementing the Privacy Provisions of the E-Government Act of 2002, at Section II.B.3.f (doc. 61-15) (hereinafter "M-03-22").

Lending support to this interpretation is the fact that PIAs are required 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 veterans 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. *See* 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(2)(B)); M-03-22, at Section II.C.1.a. These types of inquiries are certainly appropriate and required when the VA initially

created the Birmingham VAMC system and began collecting data, but not where already collected and stored data is simply being transferred from a server to an external hard drive. The factors above are not relevant for such a transfer and a new PIA would not be informative of what information is being collected, the intended use of the information, or with whom the information would be shared. Under such circumstances, Congress surely did not intend a PIA to be performed.

To the extent the plaintiffs argue that security procedures were not followed or hardware security protocols were breached at the VA facility in Birmingham when the external hard drive went missing, such claims are not actionable under the E-Government Act of 2002. Rather, those arguments should have been pursued pursuant to the Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541 *et seq.*, a claim that the plaintiffs waived after not pursuing it on appeal. *Fanin v. U.S. Dep't of Veterans Affairs*, 572 F.3d 868, 876 n.1.

Count 8

The final count before the court involves the VA's alleged failure to perform an independent risk analysis ("IRA") to determine the risk presented by the loss of the hard drive pursuant to the Veterans Benefits, Health Care, and Information Technology Act of 2006 (VBHCITA), 38 U.S.C. § 5724(a)(1). The plaintiffs also claim that the VA acted unreasonably by providing only one year of credit monitoring services.

The VBHCITA[5] provides:

> In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity or the Office of Inspector General of the Department conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

38 U.S.C. § 5724(a)(1).

After John Doe reported the missing hard drive on January 22, 2007, the VA launched an immediate investigation that culminated in the decision to offer one year of free credit monitoring services for 198,760 living individuals whose information was contained on the hard drive. VA OIG Report, at 12. The VA made this decision *before* the completion of the IRA conducted by the Centers for Medicaid & Medicare Services ("CMS"). On February 7, 2007, VA senior

---

[5]The VBHCITA became effective December 22, 2006. The data breach incident at issue occurred on January 22, 2007. The VA passed regulations that became effective June 22, 2007, six months after the passage of the VBHCITA and five months after the loss of the external hard drive.

management decided that anyone whose SSN was on the hard drive should be notified and offered credit protection. *Id.* at 11. Approximately one and one-half months later, on March 28, 2007, the CMS Chief Information Officer and Director stated that based on the IRA, "There is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned." *Id.* at 12. He recommended that the "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file." *Id.* Notification letters were sent out to the health care providers by May 31, 2007. *Id.*

Thus, the VA proactively assumed that the veterans were at risk and provided the remedy provided in the statute[6] *before* it had confirmation from the IRA that such a remedy was appropriate under the circumstances. By presuming a reasonable risk of harm from the disclosure of personally identifiable information and providing credit protection services required when an IRA reveals a "reasonable risk" of harm, *see* 38 U.S.C. § 5724(a)(2), the VA has provided the

---

[6]In addition, VA regulations limit credit monitoring awarded to those who are subject to a reasonable risk for misuse of sensitive personal information to one year. 38 C.F.R. § 75.118(a).

plaintiffs with any relief they are due.[7] Indeed, the IRA conducted by CMS affirmed the propriety of the relief offered by the VA.

Despite having been given such relief, the plaintiffs insist the IRA was insufficient and urge an additional IRA focusing on the veterans must be completed. However, the statute does not require an *individual* risk analysis as the plaintiffs state in their JSR, *See* JSR, at 12-13, 15, only an *independent* risk analysis.[8] The VA OIG Report contains multiple groups of individuals whose private information was compromised: veterans, VA OIG Report, at 7; physicians, *id.* at 10; deceased physicians, *id.*; other health care providers, *id.*; non-veteran, non-VA employees, *id.* at 24; and VA employees, *id.* Furthermore, some veterans were only identified by their SSNs; others were identified by SSNs and dates of birth; others by their name, SSN, and medical information; and others identified

---

[7] The plaintiffs offer a General Accountability Office report that states that a May 5, 2006, incident involving a missing tape with sensitive information of thousands of individuals on it warranted "credit protection and data breach analysis for 2 years." JSR, at 14. As the plaintiffs explain, however, only one year of credit protection was offered, while two years of breach analysis was given. Declaration of Michael Hogan ("Hogan Decl."), ¶¶ 2 (doc. 61-19) and Attachment A (doc. 61-20).

[8]The plaintiffs' argument that the CMS was an inappropriate entity to perform the IRA has no merit, as the statute requires either the VA OIG or a non-Department [of Veterans Affairs] entity to conduct the IRA. 38 U.S.C. § 5724(a)(1). The CMS is under the purview of the Department of Health and Human Services.

by various combinations of seven fields of identifying information. *Id.* at 9. The health care providers are identified on the hard drive by different combinations of forty-eight different fields of data. *Id.* at 10. All of this information was on a single external hard drive lost during a single data breach. The statute only requires an "independent risk analysis of the data breach," not multiple IRAs for each group of individuals whose information was compromised. *See* 38 U.S.C. § 5724(a)(1).

Because the plaintiffs were awarded appropriate relief and because the VA conducted an adequate IRA of the data breach, the court finds that the VA did not fail to take agency action it was required to take with respect to count eight.

Conclusion

Having considered the foregoing and being of the opinion that the plaintiffs have failed to properly state any claims challenging final agency action under the Administrative Procedures Act, 5 U.S.C. § 551 *et seq.*, the court finds that Counts Two, Five, Six, and Eight shall be **DISMISSED**. The court shall so rule by separate order.

DONE and **ORDERED**, this the 21st day of April 2010.

INGE PRYTZ JOHNSON
U.S. DISTRICT JUDGE

Exhibit 5

OFFICE OF
MANAGEMENT AND BUDGET

September 26, 2003

M-03-22

MEMORANDUM FOR HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

FROM: Joshua B. Bolten
DirectoR

SUBJECT: OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002

The attached guidance provides information to agencies on implementing the privacy provisions of the E-Government Act of 2002, which was signed by the President on December 17, 2002 and became effective on April 17, 2003.

The Administration is committed to protecting the privacy of the American people. This guidance document addresses privacy protections when Americans interact with their government. The guidance directs agencies to conduct reviews of how information about individuals is handled within their agency when they use information technology (IT) to collect new information, or when agencies develop or buy new IT systems to handle collections of personally identifiable information. Agencies are also directed to describe how the government handles information that individuals provide electronically, so that the American public has assurances that personal information is protected.

The privacy objective of the E-Government Act complements the National Strategy to Secure Cyberspace. As the National Strategy indicates, cyberspace security programs that strengthen protections for privacy and other civil liberties, together with strong privacy policies and practices in the federal agencies, will ensure that information is handled in a manner that maximizes both privacy and security.

Background

Section 208 of the E-Government Act of 2002 (Public Law 107-347, 44 U.S.C. Ch 36) requires that OMB issue guidance to agencies on implementing the privacy provisions of the E-Government Act (see Attachment A). The text of section 208 is provided as Attachment B to this Memorandum. Attachment C provides a general outline of regulatory requirements pursuant to the Children's Online Privacy Protection Act ("COPPA"). Attachment D summarizes the modifications to existing guidance resulting from this Memorandum. A complete list of OMB privacy guidance currently in effect is available at OMB's website.

As OMB has previously communicated to agencies, for purposes of their FY2005 IT budget requests, agencies should submit all required Privacy Impact Assessments no later than October 3, 2003.

For any questions about this guidance, contact Eva Kleederman, Policy Analyst, Information Policy and Technology Branch, Office of Management and Budget, phone (202) 395-3647, fax (202) 395-5167, e-mail Eva_Kleederman@omb.eop.gov.

Attachments

Attachment A
Attachment B
Attachment C
Attachment D

Attachment A

E-Government Act Section 208 Implementation Guidance

I. General

A. ***Requirements.*** Agencies are required to:

1. conduct privacy impact assessments for electronic information systems and collections and, in general, make them publicly available (see Section II of this Guidance),
2. post privacy policies on agency websites used by the public (see Section III),
3. translate privacy policies into a standardized machine-readable format (see Section IV), and
4. report annually to OMB on compliance with section 208 of the E-Government Act of 2002 (see Section VII).

B. ***Application.*** This guidance applies to:

1. all executive branch departments and agencies ("agencies") and their contractors that use information technology or that operate websites for purposes of interacting with the public;
2. relevant cross-agency initiatives, including those that further electronic government.

C.

Modifications to Current Guidance. Where indicated, this Memorandum modifies the following three memoranda, which are replaced by this guidance (see summary of modifications at Attachment D):

1. Memorandum 99-05 (January 7, 1999), directing agencies to examine their procedures for ensuring the privacy of personal information in federal records and to designate a senior official to assume primary responsibility for privacy policy;
2. Memorandum 99-18 (June 2, 1999), concerning posting privacy policies on major entry points to government web sites as well as on any web page collecting substantial personal information from the public; and
3. Memorandum 00-13 (June 22, 2000), concerning (i) the use of tracking technologies such as persistent cookies and (ii) parental consent consistent with the Children's Online Privacy Protection Act ("COPPA").

II. Privacy Impact Assessment

A. ***Definitions.***

1. *Individual* - means a citizen of the United States or an alien lawfully admitted for permanent residence.[1]
2. *Information in identifiable form*- is information in an IT system or online collection: (i) that directly identifies an individual (e.g., name, address, social security number or other identifying number or code, telephone number, email address, etc.) or (ii) by which an agency intends to identify specific individuals in conjunction with other data elements, i.e., indirect identification. (These data elements may include a combination of gender, race, birth date, geographic indicator, and other descriptors).[2]
3. *Information technology (IT)* - means, as defined in the Clinger-Cohen Act[3], any equipment, software or interconnected system or subsystem that is used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information.
4. *Major information system* - embraces "large" and "sensitive" information systems and means, as defined in OMB Circular A-130 (Section 6.u.) and annually in OMB Circular A-11 (section 300-4 (2003)), a system or project that requires special management attention because of its: (i) importance to the agency mission, (ii) high development, operating and maintenance costs, (iii) high risk, (iv) high return, (v) significant role in the administration of an agency's programs, finances, property or other resources.
5. *National Security Systems* - means, as defined in the Clinger-Cohen Act[4], an information system operated by the federal government, the function, operation or use of which involves: (a) intelligence activities, (b) cryptologic activities related to national security, (c) command and control of military forces, (d) equipment that is an integral part of a weapon or weapons systems, or (e) systems critical to the direct fulfillment of military or intelligence missions, but does not include systems used for routine administrative and business applications, such as payroll, finance, logistics and personnel management.
6. *Privacy Impact Assessment (PIA)*- 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.
7. *Privacy policy in standardized machine-readable format*- means a statement about site privacy

practices written in a standard computer language (not English text) that can be read automatically by a web browser.

B. ***When to conduct a PIA:***[5]
   1. *The E-Government Act requires agencies to conduct a PIA before:*
      a. developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public, or
      b. initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government).
   2. *In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risks. For example:*
      a. Conversions - when converting paper-based records to electronic systems;
      b. Anonymous to Non-Anonymous - when functions applied to an existing information collection change anonymous information into information in identifiable form;
      c. Significant System Management Changes - when new uses of an existing IT system, including application of new technologies, significantly change how information in identifiable form is managed in the system:
         - For example, when an agency employs new relational database technologies or web-based processing to access multiple data stores; such additions could create a more open environment and avenues for exposure of data that previously did not exist.
      d. Significant Merging - when agencies adopt or alter business processes so that government databases holding information in identifiable form are merged, centralized, matched with other databases or otherwise significantly manipulated:
         - For example, when databases are merged to create one central source of information; such a link may aggregate data in ways that create privacy concerns not previously at issue.
      e. New Public Access - when user-authenticating technology (e.g., password, digital certificate, biometric) is newly applied to an electronic information system accessed by members of the public;
      f. Commercial Sources - when agencies systematically incorporate into existing information systems databases of information in identifiable form purchased or obtained from commercial or public sources. (Merely querying such a source on an ad hoc basis using existing technology does not trigger the PIA requirement);
      g. New Interagency Uses - when agencies work together on shared functions involving significant new uses or exchanges of information in identifiable form, such as the cross-cutting E-Government initiatives; in such cases, the lead agency should prepare the PIA;
         - For example the Department of Health and Human Services, the lead agency for the Administration's Public Health Line of Business (LOB) Initiative, is spearheading work with several agencies to define requirements for integration of processes and accompanying information exchanges. HHS would thus prepare the PIA to ensure that all privacy issues are effectively managed throughout the development of this cross agency IT investment.
      h. Internal Flow or Collection - when alteration of a business process results in significant new uses or disclosures of information or incorporation into the system of additional items of information in identifiable form:
         - For example, agencies that participate in E-Gov initiatives could see major changes in how they conduct business internally or collect information, as a result of new business processes or E-Gov requirements. In most cases the focus will be on integration of common processes and supporting data. Any business change that results in substantial new requirements for information in identifiable form could warrant examination of privacy issues.
      i. Alteration in Character of Data - when new information in identifiable form added to a collection raises the risks to personal privacy (for example, the addition of health or financial information)
   3. *No PIA is required where information relates to internal government operations, has been previously assessed under an evaluation similar to a PIA, or where privacy issues are unchanged, as in the following circumstances:*
      a. for government-run websites, IT systems or collections of information to the extent that they do not collect or maintain information in identifiable form about members of the general public (this includes government personnel and government contractors and consultants);[6]
      b. for government-run public websites where the user is given the option of contacting the site operator for the limited purposes of providing feedback (e.g., questions or comments) or

obtaining additional information;

c. for national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-Government Act);
d. when all elements of a PIA are addressed in a matching agreement governed by the computer matching provisions of the Privacy Act (see 5 U.S.C. §§ 552a(8-10), (e)(12), (o), (p), (q), (r), (u)), which specifically provide privacy protection for matched information;
e. when all elements of a PIA are addressed in an interagency agreement permitting the merging of data for strictly statistical purposes and where the resulting data are protected from improper disclosure and use under Title V of the E-Government Act of 2002;
f. if agencies are developing IT systems or collecting non-identifiable information for a discrete purpose, not involving matching with or retrieval from other databases that generates information in identifiable form;
g. for minor changes to a system or collection that do not create new privacy risks.

4. *Update of PIAs:* Agencies must update their PIAs to reflect changed information collection authorities, business processes or other factors affecting the collection and handling of information in identifiable form.

C. ***Conducting a PIA.***

1. *Content.*
   a. PIAs must analyze and describe:
      i. what information is to be collected (e.g., nature and source);
      ii. why the information is being collected (e.g., to determine eligibility);
      iii. intended use of the information (e.g., to verify existing data);
      iv. with whom the information will be shared (e.g., another agency for a specified programmatic purpose);
      v. what opportunities individuals have to decline to provide information (i.e., where providing information is voluntary) or to consent to particular uses of the information (other than required or authorized uses), and how individuals can grant consent;
      vi. how the information will be secured (e.g., administrative and technological controls[7]); and
      vii. whether a system of records is being created under the Privacy Act, 5 U.S.C. 552a.
   b. Analysis: PIAs must identify what choices the agency made regarding an IT system or collection of information as a result of performing the PIA.
2. Agencies should commence a PIA when they begin to develop a new or significantly modified IT system or information collection:
   a. *Specificity.* The depth and content of the PIA should be appropriate for the nature of the information to be collected and the size and complexity of the IT system.
      i. *IT development stage.* PIAs conducted at this stage:
         1. should address privacy in the documentation related to systems development, including, as warranted and appropriate, statement of need, functional requirements analysis, alternatives analysis, feasibility analysis, benefits/cost analysis, and, especially, initial risk assessment;
         2. should address the impact the system will have on an individual's privacy, specifically identifying and evaluating potential threats relating to each of the elements identified in section II.C.1.a.(i)-(vii) above, to the extent these elements are known at the initial stages of development;
         3. may need to be updated before deploying the system to consider elements not identified at the concept stage (e.g., retention or disposal of information), to reflect a new information collection, or to address choices made in designing the system or information collection as a result of the analysis.
      ii. *Major information systems.* PIAs conducted for these systems should reflect more extensive analyses of:
         1. the consequences of collection and flow of information,
         2. the alternatives to collection and handling as designed,
         3. the appropriate measures to mitigate risks identified for each alternative and,
         4. the rationale for the final design choice or business process.
      iii. *Routine database systems.* Agencies may use a standardized approach (e.g., checklist or template) for PIAs involving simple systems containing routine information and involving limited use and access.
   b. *Information life cycle analysis/collaboration.* Agencies must consider the information "life cycle" (i.e., collection, use, retention, processing, disclosure and destruction) in evaluating how information handling practices at each stage may affect individuals' privacy. To be

comprehensive and meaningful, privacy impact assessments require collaboration by program experts as well as experts in the areas of information technology, IT security, records management and privacy.

3. *Review and publication.*
   a. a. Agencies must ensure that:
      i. the PIA document and, if prepared, summary are approved by a "reviewing official" (the agency CIO or other agency head designee, who is other than the official procuring the system or the official who conducts the PIA);
      ii. for each covered IT system for which 2005 funding is requested, and consistent with previous guidance from OMB, the PIA is submitted to the Director of OMB no later than October 3, 2003 (submitted electronically to PIA@omb.eop.gov along with the IT investment's unique identifier as described in OMB Circular A-11, instructions for the Exhibit 300[8]); and
      iii. the PIA document and, if prepared, summary, are made publicly available (consistent with executive branch policy on the release of information about systems for which funding is proposed).
         1. Agencies may determine to not make the PIA document or summary publicly available to the extent that publication would raise security concerns, reveal classified (i.e., national security) information or sensitive information (e.g., potentially damaging to a national interest, law enforcement effort or competitive business interest) contained in an assessment[9]. Such information shall be protected and handled consistent with the Freedom of Information Act (FOIA).
         2. Agencies should not include information in identifiable form in their privacy impact assessments, as there is no need for the PIA to include such information. Thus, agencies may not seek to avoid making the PIA publicly available on these grounds.

D. *Relationship to requirements under the Paperwork Reduction Act (PRA)*[10].
   1. Joint Information Collection Request (ICR) and PIA. Agencies undertaking new electronic information collections may conduct and submit the PIA to OMB, and make it publicly available, as part of the SF83 Supporting Statement (the request to OMB to approve a new agency information collection).
   2. If Agencies submit a Joint ICR and PIA:
      a. All elements of the PIA must be addressed and identifiable within the structure of the Supporting Statement to the ICR, including:
         i. a description of the information to be collected in the response to Item 1 of the Supporting Statement[11];
         ii. a description of how the information will be shared and for what purpose in Item 2 of the Supporting Statement[12];
         iii. a statement detailing the impact the proposed collection will have on privacy in Item 2 of the Supporting Statement[13];
         iv. a discussion in item 10 of the Supporting Statement of:
            1. whether individuals are informed that providing the information is mandatory or voluntary
            2. opportunities to consent, if any, to sharing and submission of information;
            3. how the information will be secured; and
            4. whether a system of records is being created under the Privacy Act)[14].
      b. For additional information on the requirements of an ICR, please consult your agency's organization responsible for PRA compliance.
   3. Agencies need not conduct a new PIA for simple renewal requests for information collections under the PRA. As determined by reference to section II.B.2. above, agencies must separately consider the need for a PIA when amending an ICR to collect information that is significantly different in character from the original collection.

E. *Relationship to requirements under the Privacy Act of 1974, 5 U.S. C. 552a.*

   1. Agencies may choose to conduct a PIA when developing the System of Records (SOR) notice required by subsection (e)(4) of the Privacy Act, in that the PIA and SOR overlap in content (e.g., the categories of records in the system, the uses of the records, the policies and practices for handling, etc.).
   2. Agencies, in addition, may make the PIA publicly available in the Federal Register along with the Privacy Act SOR notice.

3. Agencies must separately consider the need for a PIA when issuing a change to a SOR notice (e.g., a change in the type or category of record added to the system may warrant a PIA).

III. Privacy Policies on Agency Websites

A. *Privacy Policy Clarification.* To promote clarity to the public, agencies are required to refer to their general web site notices explaining agency information handling practices as the "Privacy Policy."

B. *Effective Date.* Agencies are expected to implement the following changes to their websites by December 15, 2003.

C. *Exclusions:* For purposes of web privacy policies, this guidance does not apply to:
   1. information other than "government information" as defined in OMB Circular A-130;
   2. agency intranet web sites that are accessible only by authorized government users (employees, contractors, consultants, fellows, grantees);
   3. national security systems defined at 40 U.S.C. 11103 as exempt from the definition of information technology (see section 202(i) of the E-government Act).

D. *Content of Privacy Policies.*
   1. Agency Privacy Policies must comply with guidance issued in OMB Memorandum 99-18 and must now also include the following two new content areas:
      a. *Consent to collection and sharing*[15]. Agencies must now ensure that privacy policies:
         i. inform visitors whenever providing requested information is voluntary;
         ii. inform visitors how to grant consent for use of voluntarily-provided information; and
         iii. inform visitors how to grant consent to use mandatorily-provided information for other than statutorily-mandated uses or authorized routine uses under the Privacy Act.
      b. *Rights under the Privacy Act or other privacy laws*[16]. Agencies must now also notify web-site visitors of their rights under the Privacy Act or other privacy-protecting laws that may primarily apply to specific agencies (such as the Health Insurance Portability and Accountability Act of 1996, the IRS Restructuring and Reform Act of 1998, or the Family Education Rights and Privacy Act):
         i. in the body of the web privacy policy;
         ii. via link to the applicable agency regulation (e.g., Privacy Act regulation and pertinent system notice); or
         iii. via link to other official summary of statutory rights (such as the summary of Privacy Act rights in the FOIA/Privacy Act Reference Materials posted by the Federal Consumer Information Center at www.Firstgov.gov).
   2. Agency Privacy Policies must continue to address the following, modified, requirements:
      a. Nature, purpose, use and sharing of information collected . Agencies should follow existing policies (issued in OMB Memorandum 99-18) concerning notice of the nature, purpose, use and sharing of information collected via the Internet, as modified below:
         i. *Privacy Act information.* When agencies collect information subject to the Privacy Act, agencies are directed to explain what portion of the information is maintained and retrieved by name or personal identifier in a Privacy Act system of records and provide a Privacy Act Statement either:
            1. at the point of collection, or
            2. via link to the agency's general Privacy Policy[18].
         ii. *"Privacy Act Statements."* Privacy Act Statements must notify users of the authority for and purpose and use of the collection of information subject to the Privacy Act, whether providing the information is mandatory or voluntary, and the effects of not providing all or any part of the requested information.
         iii. *Automatically Collected Information (site management data).* Agency Privacy Policies must specify what information the agency collects automatically (i.e., user's IP address, location, and time of visit) and identify the use for which it is collected (i.e., site management or security purposes).
         iv. *Interaction with children:* Agencies that provide content to children under 13 and that collect personally identifiable information from these visitors should incorporate the requirements of the Children's Online Privacy Protection Act ("COPPA") into their Privacy Policies (see Attachment C)[19].
         v. *Tracking and customization activities.* Agencies are directed to adhere to the following modifications to OMB Memorandum 00-13 and the OMB follow-up guidance letter dated September 5, 2000:
            1. *Tracking technology prohibitions:*

a. agencies are prohibited from using persistent cookies or any other means (e.g., web beacons) to track visitors' activity on the Internet except as provided in subsection (b) below;
b. agency heads may approve, or may authorize the heads of sub-agencies or senior official(s) reporting directly to the agency head to approve, the use of persistent tracking technology for a compelling need. When used, agency's must post clear notice in the agency's privacy policy of:
    - the nature of the information collected;
    - the purpose and use for the information;
    - whether and to whom the information will be disclosed; and
    - the privacy safeguards applied to the information collected.
c. agencies must report the use of persistent tracking technologies as authorized for use by subsection b. above (see section VII)[20].

2. *The following technologies are not prohibited:*
    a. Technology that is used to facilitate a visitor's activity within a single session (e.g., a "session cookie") and does not persist over time is not subject to the prohibition on the use of tracking technology.
    b. Customization technology (to customize a website at the visitor's request) if approved by the agency head or designee for use (see v.1.b above) and where the following is posted in the Agency's Privacy Policy:
        - the purpose of the tracking (i.e., customization of the site);
        - that accepting the customizing feature is voluntary;
        - that declining the feature still permits the individual to use the site; and
        - the privacy safeguards in place for handling the information collected.
    c. Agency use of password access to information that does not involve "persistent cookies" or similar technology.

vi. *Law enforcement and homeland security sharing:* Consistent with current practice, Internet privacy policies may reflect that collected information may be shared and protected as necessary for authorized law enforcement, homeland security and national security activities.

b. *Security of the information*[21]. Agencies should continue to comply with existing requirements for computer security in administering their websites[22] and post the following information in their Privacy Policy:
    i. in clear language, information about management, operational and technical controls ensuring the security and confidentiality of personally identifiable records (e.g., access controls, data storage procedures, periodic testing of safeguards, etc.), and
    ii. in general terms, information about any additional safeguards used to identify and prevent unauthorized attempts to access or cause harm to information and systems. (The statement should be at a level to inform the public that their information is being protected while not compromising security.)

E. *Placement of notices.* Agencies should continue to follow the policy identified in OMB Memorandum 99-18 regarding the posting of privacy policies on their websites. Specifically, agencies must post (or link to) privacy policies at:
1. their principal web site;
2. any known, major entry points to their sites;
3. any web page that collects substantial information in identifiable form.

F. ***Clarity of notices.*** Consistent with OMB Memorandum 99-18, privacy policies must be:
1. clearly labeled and easily accessed;
2. written in plain language; and
3. made clear and easy to understand, whether by integrating all information and statements into a single posting, by layering a short "highlights" notice linked to full explanation, or by other means the agency determines is effective.

IV. Privacy Policies in Machine-Readable Formats

A. ***Actions.***
1. Agencies must adopt machine readable technology that alerts users automatically about whether site privacy practices match their personal privacy preferences. Such technology enables users to make

an informed choice about whether to conduct business with that site.
2. OMB encourages agencies to adopt other privacy protective tools that become available as the technology advances.

B. ***Reporting Requirement.*** Agencies must develop a timetable for translating their privacy policies into a standardized machine-readable format. The timetable must include achievable milestones that show the agency's progress toward implementation over the next year. Agencies must include this timetable in their reports to OMB (see Section VII).

V. Privacy Policies Incorporated by this Guidance

In addition to the particular actions discussed above, this guidance reiterates general directives from previous OMB Memoranda regarding the privacy of personal information in federal records and collected on federal web sites. Specifically, existing policies continue to require that agencies:

A. assure that their uses of new information technologies sustain, and do not erode, the protections provided in all statutes relating to agency use, collection, and disclosure of personal information;
B. assure that personal information contained in Privacy Act systems of records be handled in full compliance with fair information practices as set out in the Privacy Act of 1974;
C. evaluate legislative proposals involving collection, use and disclosure of personal information by the federal government for consistency with the Privacy Act of 1974;
D. evaluate legislative proposals involving the collection, use and disclosure of personal information by any entity, public or private, for consistency with the Privacy Principles;
E. ensure full adherence with stated privacy policies.

VI. Agency Privacy Activities/Designation of Responsible Official

Because of the capability of information technology to capture and disseminate information in an instant, all federal employees and contractors must remain mindful of privacy and their obligation to protect information in identifiable form. In addition, implementing the privacy provisions of the E-Government Act requires the cooperation and coordination of privacy, security, FOIA/Privacy Act and project officers located in disparate organizations within agencies. Clear leadership and authority are essential.

Accordingly, this guidance builds on policy introduced in Memorandum 99-05 in the following ways:

A. Agencies must:
   1. inform and educate employees and contractors of their responsibility for protecting information in identifiable form;
   2. identify those individuals in the agency (e.g., information technology personnel, Privacy Act Officers) that have day-to-day responsibility for implementing section 208 of the E-Government Act, the Privacy Act, or other privacy laws and policies.
   3. designate an appropriate senior official or officials (e.g., CIO, Assistant Secretary) to serve as the agency's principal contact(s) for information technology/web matters and for privacy policies. The designated official(s) shall coordinate implementation of OMB web and privacy policy and guidance.
   4. designate an appropriate official (or officials, as appropriate) to serve as the "reviewing official(s)" for agency PIAs.

B. OMB leads a committee of key officials involved in privacy that reviewed and helped shape this guidance and that will review and help shape any follow-on privacy and web-privacy-related guidance. In addition, as part of overseeing agencies' implementation of section 208, OMB will rely on the CIO Council to collect information on agencies' initial experience in preparing PIAs, to share experiences, ideas, and promising practices as well as identify any needed revisions to OMB's guidance on PIAs.

VII. Reporting Requirements

Agencies are required to submit an annual report on compliance with this guidance to OMB as part of their annual E-Government Act status report. The first reports are due to OMB by December 15, 2003. All agencies that use information technology systems and conduct electronic information collection activities must complete a report on compliance with this guidance, whether or not they submit budgets to OMB.

Reports must address the following four elements:

A. *Information technology systems or information collections for which PIAs were conducted.* Include the mechanism by which the PIA was made publicly available (website, Federal Register, other), whether the PIA was made publicly available in full, summary form or not at all (if in summary form or not at all, explain), and, if made available in conjunction with an ICR or SOR, the publication date.
B. *Persistent tracking technology uses.* If persistent tracking technology is authorized, include the need that

compels use of the technology, the safeguards instituted to protect the information collected, the agency official approving use of the tracking technology, and the actual privacy policy notification of such use.

C. *Agency achievement of goals for machine readability*: Include goals for and progress toward achieving compatibility of privacy policies with machine-readable privacy protection technology.

D. *Contact information*. Include the individual(s) (name and title) appointed by the head of the Executive Department or agency to serve as the agency's principal contact(s) for information technology/web matters and the individual (name and title) primarily responsible for privacy policies.

Attachment B
E-Government Act of 2002
Pub. L. No. 107-347, Dec. 17, 2002

SEC. 208. PRIVACY PROVISIONS.

A. PURPOSE. — The purpose of this section is to ensure sufficient protections for the privacy of personal information as agencies implement citizen-centered electronic Government.

B. PRIVACY IMPACT ASSESSMENTS.—

1. RESPONSIBILITIES OF AGENCIES.—
   a. IN GENERAL.—An agency shall take actions described under subparagraph (b) before—
      i. developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form; or
      ii. initiating a new collection of information that—
         1. will be collected, maintained, or disseminated using information technology; and
         2. 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.
   b. AGENCY ACTIVITIES. —To the extent required under subparagraph (a), each agency shall—
      i. conduct 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.
   c. SENSITIVE INFORMATION. —Subparagraph (b)(iii) may be modified or waived for security reasons, or to protect classified, sensitive, or private information contained in an assessment.
   d. COPY TO DIRECTOR. —Agencies shall provide the Director with a copy of the privacy impact assessment for each system for which funding is requested.
2. CONTENTS OF A PRIVACY IMPACT ASSESSMENT. —
   a. IN GENERAL. —The Director shall issue guidance to agencies specifying the required contents of a privacy impact assessment.
   b. GUIDANCE. — The guidance shall—
      i. ensure that a privacy impact assessment is commensurate with the size of the information system being assessed, the sensitivity of information that is in an identifiable form in that system, and the risk of harm from unauthorized release of that information; and
      ii. require that a privacy impact assessment address—
         1. what information is to be collected;
         2. why the information is being collected;
         3. the intended use of the agency of the information;
         4. with whom the information will be shared;
         5. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
         6. how the information will be secured; and
         7. whether a system of records is being created under section 552a of title 5, United States Code, (commonly referred to as the 'Privacy Act').
3. RESPONSIBILITIES OF THE DIRECTOR.—The Director shall—
   a. develop policies and guidelines for agencies on the conduct of privacy impact assessments;
   b. oversee the implementation of the privacy impact assessment process throughout the Government; and
   c. require agencies to conduct privacy impact assessments of existing information systems or ongoing collections of information that is in an identifiable form as the Director determines appropriate.

C. PRIVACY PROTECTIONS ON AGENCY WEBSITES. —

1. PRIVACY POLICIES ON WEBSITES. —
   a. GUIDELINES FOR NOTICES. —The Director shall develop guidance for privacy notices on agency websites used by the public.
   b. CONTENTS. —The guidance shall require that a privacy notice address, consistent with section 552a of title 5, United States Code—
      i. what information is to be collected;
      ii. why the information is being collected;
      iii. the intended use of the agency of the information;
      iv. with whom the information will be shared;
      v. what notice or opportunities for consent would be provided to individuals regarding what information is collected and how that information is shared;
      vi. how the information will be secured; and
      vii. the rights of the individual under section 552a of title 5, United States Code (commonly referred to as the 'Privacy Act'), and other laws relevant to the protection of the privacy of an individual.
2. PRIVACY POLICIES IN MACHINE-READABLE FORMATS. — The Director shall issue guidance requiring agencies to translate privacy policies into a standardized machine-readable format.

D. DEFINITION. —In this section, 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.

Attachment C

This attachment is a summary by the Federal Trade Commission of its guidance regarding federal agency compliance with the Children's Online Privacy Protection Act (COPPA).

The hallmarks of COPPA for purposes of federal online activity are (i) notice of information collection practices (ii) verifiable parental consent and (iii) access, as generally outlined below:

- Notice of Information Collection Practices

  Agencies whose Internet sites offer a separate children's area and collect personal information from them must post a clear and prominent link to its Internet privacy policy on the home page of the children's area and at each area where it collects personal information from children. The privacy policy should provide the name and contact information of the agency representative required to respond to parental inquiries about the site. Importantly, the privacy policy should inform parents about the kinds of information collected from children, how the information is collected (directly, or through cookies), how the information is used, and procedures for reviewing/deleting the information obtained from children.

  In addition, the privacy policy should inform parents that only the minimum information necessary for participation in the activity is collected from the child.In addition to providing notice by posting a privacy policy, notice of an Internet site's information collection practices must be sent directly to a parent when a site is requesting parental consent to collection personal information from a child. This direct notice should tell parents that the site would like to collect personal information from their child, that their consent is required for this collection, and how consent can be provided. The notice should also contain the information set forth in the site's privacy policy, or provide an explanatory link to the privacy policy.

- Verifiable Parental Consent

  With limited exceptions, agencies must obtain parental consent before collecting any personal information from children under the age of 13. If agencies are using the personal information for their internal use only, they may obtain parental consent through an e-mail message from the parent, as long as they take additional steps to increase the likelihood that the parent has, in fact, provided the consent. For example, agencies might seek confirmation from a parent in a delayed confirmatory e-mail, or confirm the parent's consent by letter or phone call[23].

  However, if agencies disclose the personal information to third parties or the public (through chat rooms or message boards), only the most reliable methods of obtaining consent must be used. These methods include: (i) obtaining a signed form from the parent via postal mail or facsimile, (ii) accepting and verifying a credit card number in connection with a transaction, (iii) taking calls from parents through a toll-free telephone

number staffed by trained personnel, or (iv) email accompanied by digital signature.

Although COPPA anticipates that private sector Internet operators may share collected information with third parties (for marketing or other commercial purposes) and with the public (through chat rooms or message boards), as a general principle, federal agencies collect information from children only for purposes of the immediate online activity or other, disclosed, internal agency use. (Internal agency use of collected information would include release to others who use it solely to provide support for the internal operations of the site or service, including technical support and order fulfillment.) By analogy to COPPA and consistent with the Privacy Act, agencies may not use information collected from children in any manner not initially disclosed and for which explicit parental consent has not been obtained. Agencies' Internet privacy policies should reflect these disclosure and consent principles.

COPPA's implementing regulations include several exceptions to the requirement to obtain advance parental consent where the Internet operator (here, the agency) collects a child's email address for the following purposes: (i) to provide notice and seek consent, (ii) to respond to a one-time request from a child before deleting it, (iii) to respond more than once to a specific request, e.g., for a subscription to a newsletter, as long as the parent is notified of, and has the opportunity to terminate a continuing series of communications, (iv) to protect the safety of a child, so long as the parent is notified and given the opportunity to prevent further use of the information, and (v) to protect the security or liability of the site or to respond to law enforcement if necessary.

Agencies should send a new notice and request for consent to parents any time the agency makes material changes in the collection or use of information to which the parent had previously agreed. Agencies should also make clear to parents that they may revoke their consent, refuse to allow further use or collection of the child's personal information and direct the agency to delete the information at any time.

- Access

At a parent's request, agencies must disclose the general kinds of personal information they collect online from children as well as the specific information collected from a child. Agencies must use reasonable procedures to ensure they are dealing with the child's parent before they provide access to the child's specific information, e.g., obtaining signed hard copy of identification, accepting and verifying a credit card number, taking calls from parents on a toll-free line staffed by trained personnel, email accompanied by digital signature, or email accompanied by a PIN or password obtained through one of the verification methods above.

In adapting the provisions of COPPA to their Internet operations, agencies should consult the FTC's web site at http://www.ftc.gov/privacy/privacyinitiatives/childrens.html or call the COPPA compliance telephone line at (202) 326-3140.

Attachment D

Summary of Modifications to Prior Guidance

This Memorandum modifies prior guidance in the following ways:

* Internet Privacy Policies (Memorandum 99-18):

- must identify when tracking technology is used to personalize the interaction, and explain the purpose of the feature and the visitor's option to decline it.

- must clearly explain when information is maintained and retrieved by personal identifier in a Privacy Act system of records; must provide (or link to) a Privacy Act statement (which may be subsumed within agency's Internet privacy policy) where Privacy Act information is solicited.

- should clearly explain an individual's rights under the Privacy Act if solicited information is to be maintained in a Privacy Act system of records; information about rights under the Privacy Act may be provided in the body of the web privacy policy or via link to the agency's published systems notice and Privacy Act regulation or other summary of rights under the Privacy Act (notice and explanation of rights under other privacy laws should be handled in the same manner).

- when a Privacy Act Statement is not required, must link to the agency's Internet privacy policy explaining the purpose of the collection and use of the information (point-of-collection notice at agency option).

- must clearly explain where the user may consent to the collection or sharing of information and must notify users of any available mechanism to grant consent.
- agencies must undertake to make their Internet privacy policies "readable" by privacy protection technology and report to OMB their progress in that effort.
- must adhere to the regulatory requirements of the Children's Online Privacy Protection Act (COPPA) when collecting information electronically from children under age 13.

*Tracking Technology (Memorandum 00-13):

- prohibition against tracking visitors' Internet use extended to include tracking by any means (previous guidance addressed only "persistent cookies").? authority to waive the prohibition on tracking in appropriate circumstances may be retained by the head of an agency, or may be delegated to (i) senior official(s) reporting directly to the agency head, or to (ii) the heads of sub-agencies.? agencies must report the use of tracking technology to OMB, identifying the circumstances, safeguards and approving official.
- agencies using customizing technology must explain the use, voluntary nature of and the safeguards applicable to the customizing device in the Internet privacy policy.
- agency heads or their designees may approve the use of persistent tracking technology to customize Internet interactions with the government.

* Privacy responsibilities (Memorandum 99-05)

- agencies to identify individuals with day-to-day responsibility for implementing the privacy provisions of the E-Government Act, the Privacy Act and any other applicable statutory privacy regime.
- agencies to report to OMB the identities of senior official(s) primarily responsible for implementing and coordinating information technology/web policies and privacy policies.

---

1. Agencies may, consistent with individual practice, choose to extend the protections of the Privacy Act and E-Government Act to businesses, sole proprietors, aliens, etc.
2. Information in identifiable form is defined in section 208(d) of the Act as "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." Information "permitting the physical or online contacting of a specific individual" (see section 208(b)(1)(A)(ii)(II)) is the same as "information in identifiable form."
3. Clinger-Cohen Act of 1996, 40 U.S.C. 11101(6).
4. Clinger-Cohen Act of 1996, 40 U.S.C. 11103.
5. In addition to these statutorily prescribed activities, the E-Government Act authorizes the Director of OMB to require agencies to conduct PIAs of existing electronic information systems or ongoing collections of information in identifiable form as the Director determines appropriate. (see section 208(b)(3)(C)).
6. Information in identifiable form about government personnel generally is protected by the Privacy Act of 1974. Nevertheless, OMB encourages agencies to conduct PIAs for these systems as appropriate.
7. Consistent with agency requirements under the Federal Information Security Management Act, agencies should: (i) affirm that the agency is following IT security requirements and procedures required by federal law and policy to ensure that information is appropriately secured, (ii) acknowledge that the agency has conducted a risk assessment, identified appropriate security controls to protect against that risk, and implemented those controls, (iii) describe the monitoring/testing/evaluating on a regular basis to ensure that controls continue to work properly, safeguarding the information, and (iv) provide a point of contact for any additional questions from users. Given the potential sensitivity of security-related information, agencies should ensure that the IT security official responsible for the security of the system and its information reviews the language before it is posted.
8. PIAs that comply with the statutory requirements and previous versions of this Memorandum are acceptable for agencies' FY 2005 budget submissions.
9. Section 208(b)(1)(C).
10. See 44 USC Chapter 35 and implementing regulations, 5 CFR Part 1320.8.
11. Item 1 of the Supporting Statement reads: "Explain the circumstances that make the collection of information necessary. Identify any legal or administrative requirements that necessitate the collection. Attach a copy of the appropriate section of each statute and regulation mandating or authorizing the collection of information."
12. Item 2 of the Supporting Statement reads: "Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information

received from the current collection."

13. Item 2 of the Supporting Statement reads: "Indicate how, by whom, and for what purpose the information is to be used. Except for a new collection, indicate the actual use the agency has made of the information received from the current collection."
14. Item 10 of the Supporting Statement reads: "Describe any assurance of confidentiality provided to respondents and the basis for the assurance in statute, regulation, or agency policy."
15. Section 208(c)(1)(B)(v).
16. Section 208(c)(1)(B)(vii).
17. Section 208(c)(1)(B)(i-iv).
18. When multiple Privacy Act Statements are incorporated in a web privacy policy, a point-of-collection link must connect to the Privacy Act Statement pertinent to the particular collection.
19. Attachment C contains a general outline of COPPA's regulatory requirements. Agencies should consult the Federal Trade Commission's COPPA compliance telephone line at (202)-326-3140 or website for additional information at: http://www.ftc.gov/privacy/privacyinitiatives/childrens.html.
20. Consistent with current practice, the agency head or designee may limit, as appropriate, notice and reporting of tracking activities that the agency has properly approved and which are used for authorized law enforcement, national security and/or homeland security purposes.
21. Section 208(c)(1)(B)(vi).
22. Federal Information Security Management Act of 2002 (Title III of P.L. 107-347), OMB's related security guidance and policies (Appendix III to OMB Circular A-130, "Security of Federal Automated Information Resources") and standards and guidelines development by the National Institute of Standards and Technologies.
23. This standard was set to expire in April 2002, at which time the most verifiable methods of obtaining consent would have been required; however, in a Notice of Proposed Rulemaking, published in the Federal Register on October 31, 2001, the FTC has proposed that this standard be extended until April 2004. 66 Fed. Reg. 54963.

Exhibit 6

Privacy error ×

Not Secure https://safe.amrdec.army.mil/safe/Welcome.aspx

Your connection is not private

Attackers might be trying to steal your information from **safe.amrdec.army.mil** (for example, passwords, messages, or credit cards). NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some system information and page content to Google to help detect dangerous apps and sites. Privacy policy

Back to safety

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. _____

CERTIFICATION BY MARC ROTENBERG IN SUPPORT OF THE PLAINTIFF'S EMERGENCY MOTION FOR A TEMPORARY RESTRAINING ORDER

Pursuant to LCvR 65.1(a) of the Rules of the United States District Court for the District of Columbia, I, Marc Rotenberg, certify that I have provided Defendants advance notice of this Emergency Motion for a Temporary Restraining Order by contacting, on the morning of Monday, July 3, 2017, Marcy Berman, Assistant Branch Director of the Federal Programs Branch, Civil Division, United States Department of Justice; Daniel Van Horn, Chief of the Civil Division in the United States Attorney's Office for the District of Columbia; and Daniel Bensing, a senior attorney in the Federal Programs Branch, Civil Division, United States Department of Justice. I have provided copies of all pleadings and papers filed in the action to Ms. Berman, who stated that she would forward said pleadings and papers to the appropriate attorney in the Federal Programs Branch.

These efforts are in addition to service to be effected on defendants by overnight mail as described in the Certificate of Service accompanying this Motion pursuant to LCvR 5.4(d).

Respectfully Submitted,

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

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

From: **Marc Rotenberg** rotenberg@epic.org
Subject: Re: TRO - EPIC v. Commission, et al (demand for state voter records)
Date: July 3, 2017 at 11:59 AM
To: Berman, Marcia (CIV) Marcia.Berman@usdoj.gov, Shapiro, Elizabeth (CIV) Elizabeth.Shapiro@usdoj.gov
Cc: Alan Butler butler@epic.org, John Davisson davisson@epic.org

Thanks, Marcy,

We will send you the TRO papers shortly and will be filing with the district court clerk this afternoon.

EPIC Senior Counsel Alan Butler is also on this matter.

–Marc Rotenberg

On Jul 3, 2017, at 11:10 AM, Berman, Marcia (CIV) <Marcia.Berman@usdoj.gov> wrote:

Hi Marc – I'm following up on this message to Dan Bensing and Dan Van Horn. You can send me the TRO papers, and I'll forward them to the appropriate attorney in Fed. Programs.

Thanks -- Marcy

Marcy Berman
Assistant Branch Director
U.S. Department of Justice, Civil Division
Federal Programs Branch
(202) 514-2205

From: Ricketts, Jennifer D (CIV)
Sent: Monday, July 03, 2017 11:06 AM
To: Berman, Marcia (CIV) <MBerman@civ.usdoj.gov>; Shapiro, Elizabeth (CIV) <EShapiro@CIV.USDOJ.GOV>
Cc: Griffiths, John (CIV) <jgriffit@CIV.USDOJ.GOV>
Subject: FW: TRO - EPIC v. Commission, et al (demand for state voter records)
Importance: High

From: Van Horn, Daniel (USADC) [mailto:Daniel.VanHorn@usdoj.gov]
Sent: Monday, July 03, 2017 10:26 AM
To: Ricketts, Jennifer D (CIV) <jrickett@CIV.USDOJ.GOV>
Subject: FW: TRO - EPIC v. Commission, et al (demand for state voter records)
Importance: High

Here's the email we just discussed:

From: Marc Rotenberg [mailto:rotenberg@epic.org]
Sent: Monday, July 3, 2017 10:14 AM
To: Van Horn, Daniel (USADC) <DVanHorn@usa.doj.gov>; Bensing, Daniel (CIV) <Daniel.Bensing@usdoj.gov>
Cc: Alan Butler <butler@epic.org>; Caitriona Fitzgerald <fitzgerald@epic.org>; John Davisson <davisson@epic.org>

Subject: Fwd: TRO - EPIC v. Commission, et al (demand for state voter records)
Importance: High

Daniel Van Horn, Chief
Civil Division
Washington, DC

Dear Mr. Van Horn,

We are forwarding a communication sent earlier today to Daniel Bensing regarding a motion we plan to file in D.D.C, seeking emergency relief,. regarding the Presidential Advisory Commission on Election Integrity.

Marc Rotenberg

Begin forwarded message:

From: Marc Rotenberg <rotenberg@epic.org>
Subject: TRO - EPIC v. Commission, et al (demand for state voter records)
Date: July 3, 2017 at 10:09:39 AM EDT
To: Daniel Bensing <daniel.bensing@usdoj.gov>
Cc: Alan Butler <butler@epic.org>, John Davisson <davisson@epic.org>, Caitriona Fitzgerald <fitzgerald@epic.org>

Dear Mr. Bensing,

EPIC is filing suit today against a group of agencies and defendants within the Executive Office of the President, including the Presidential Commission on Election Integrity and the Office of the Vice President. We intend to seek emergency relief and a TRO/Preliminary Injunction.

We would like to establish a line of communication with the attorney at DOJ who will be handling this matter, so that we can ensure that the Defendants have sufficient notice to appear. Can you let us know who would be the appropriate contact in your office or in the DC U.S. Attorneys office.

Sincerely,

Marc Rotenberg, President
EPIC
D.C. Bar # 422825
202-415-6788

CERTIFICATE OF SERVICE

I, Marc Rotenberg, hereby certify that on July 3, 2017, I will cause one copy of the foregoing Emergency Motion for Temporary Restraining Order, including the Memorandum of Points and Authorities and associated attachments, to be served on each of the following via overnight mail:

United States Attorney for the District of Columbia
c/o Civil Process Clerk
Department of Justice
555 4th St., N.W.
Washington, D.C. 20530

Attorney General of the United States
Department of Justice 950
Pennsylvania Ave., N.W.
Washington, D.C. 20530

Presidential Advisory Committee on Election Integrity
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Michael Pence
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Kris Kobach
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Executive Office of the President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

Office of the Vice President of the United States
The White House
1600 Pennsylvania Avenue, N.W.
Washington, D.C. 20500

General Services Administration
1800 F Street, N.W.
Washington, D.C. 20405

Respectfully Submitted,

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

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.

Case: 1:17-cv-01320
Assigned To : Kollar-Kotelly, Colleen
Assign. Date : 7/3/2017
Description: TRO/PI

[PROPOSED] TEMPORARY RESTRAINING ORDER

Upon consideration of Plaintiff's Emergency Motion 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 Privacy Impact Assessment, as required by federal law, E-Government Act of 2002, Pub. L. 107–347, 116 Stat. 2899 (codified as amended at 44 U.S.C. § 3501 note);

It appearing to the Court that Plaintiff is likely to succeed on the merits of its action, that it will suffer irreparable injury if the requested relief is not issued, that Defendants will not be harmed if the requested relief is issued, and that the public interest favors the entry of such an order, it is, therefore,

ORDERED that Plaintiff's application for a Temporary Restraining Order is hereby GRANTED;

ORDERED that Defendants immediately halt collection of voter roll data from state election officials;

ORDERED that Defendants immediately delete and disgorge any voter roll data already collected or hereafter received;

ORDERED, in accordance with Fed. R. Civ. P. 65(c) and *NRDC v. Morton*, 337 F. Supp. 167, 169 (D.D.C. 1971), *aff'd on other grounds*, 458 F.2d 827 (D.C. Cir. 1972) (bonds for injunctive relief may be reduced when plaintiff initiates a public interest litigation), that this injunction shall be effective upon Plaintiff's giving of security in the amount of $10 by depositing that amount with the Clerk of Court; and

ORDERED, in accordance with Fed. R. Civ. P. 65(b), that this temporary restraining order shall expire ten days after its entry upon the docket, unless extended for good cause shown.

Date: _____

Time: _____

_____

United States District Judge