

January 15, 2018

Senator Chuck Grassley, Chairman
Senator Dianne Feinstein, Ranking Member
United States Senate Committee on the Judiciary
224 Dirksen Senate Office Building
Washington, D.C. 20510-6050

RE: Hearing on “Oversight of the United States Department of Homeland Security”

Dear Chairman Grassley and Ranking Member Feinstein:

We write to you regarding the upcoming hearing on “Oversight of the United States Department of Homeland Security.”¹ EPIC is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC is focused on the protection of privacy rights across the federal government, and we are particularly interested in the privacy problems associated with surveillance activities undertaken by the Department of Homeland Security.² EPIC also brought a case against the recently disbanded Presidential Advisory Commission on Election Integrity to prevent the collection of state voter data.

EPIC writes to urge the Senate Judiciary Committee to confirm with Secretary Kirstjen Nielsen that (1) the DHS will not continue the activities of the Presidential Commission; (2) the DHS will respect the privacy rights currently in place for the Deferred Action for Childhood Arrivals (“DACA”) applicants; and (3) biometric programs will not be expanded until transparency obligations are fulfilled and privacy safeguards are established.

I. Privacy of Voter Roll Data

Now that the Presidential Advisory Commission on Election Integrity (“Commission”) has been dissolved,³ it is critical for DHS to make clear that it will not continue the activities of the Commission. White House Director of Information Technology Charles Herndon recently stated that none of the Commission’s “records or data will be transferred to the DHS or another agency.”⁴ However, shortly after the issuance of the Executive Order, former Commission Vice Chair Kris Kobach told several news organizations that he intended to pursue

¹ *Oversight of the United States Department of Homeland Security*, 115th Cong. (2018), S. Comm. On Judiciary, (Jan. 16, 2018), <https://www.judiciary.senate.gov/meetings/oversight-of-the-united-states-department-of-homeland-security>.

² See About EPIC, EPIC.org, <https://epic.org/epic/about.html>.

³ Exec. Order (Jan. 3, 2018), <https://www.whitehouse.gov/presidential-actions/executive-order-termination-presidential-advisory-commission-election-integrity/>.

⁴ Spenser S. Hsu, *White House says it will destroy Trump voter panel data, send no records to DHS*, Wash. Post (Jan. 10, 2018), https://www.washingtonpost.com/local/public-safety/white-house-says-it-will-destroy-trump-voter-panel-data-send-no-records-to-dhs/2018/01/10/e70704a8-f616-11e7-b34a-b85626af34ef_story.html?utm_term=.0783a3a8c290.

the work of the Commission at the DHS.⁵ Mr. Kobach also indicated that the personal data obtained by the Commission would be transferred to the DHS.⁶

Our interest in the resolution of this question is significant. EPIC filed a lawsuit seeking a preliminary injunction to block a demand from the Commission for millions of state voter records.⁷ The Commission failed to conduct and release a Privacy Impact Assessment—as required by the E-Government Act⁸—prior to collecting personal voter data such as social security numbers, addresses, and dates of birth. The Commission's demand for detailed voter records also violates the constitutional right to privacy of millions of Americans.

The voter roll data sought by the Commission included:

- 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.

Last week, EPIC and ten organizations wrote to Secretary Nielsen to seek “your prompt assurance that the Department of Homeland Security has no intention to accept or maintain any personal data from Mr. Kobach or the Presidential Advisory Commission on Election Integrity.”⁹ EPIC and the organizations emphasized that neither Mr. Kobach nor the defunct Commission had any authority to transfer the state voter data to DHS. Moreover, the groups warned that accepting or maintaining personal voter data would “subject the DHS to obligations under the E-

⁵ *Trump disbands Kobach-led voter fraud commission after resistance from states*, Kansas City Star (Jan. 3, 2018), <http://www.kansascity.com/news/politics-government/article192854444.html>; *Kobach says he will advise DHS after election panel's demise*, Associated Press (Jan. 4, 2018), <http://ksnt.com/2018/01/04/kobach-says-he-will-advise-dhs-after-election-panels-demise/>.

⁶ *Trump Disbands Commission on Voter Fraud*, N.Y. Times (Jan. 3, 2018), <https://www.nytimes.com/2018/01/03/us/politics/trump-voter-fraud-commission.html>; *Kris Kobach On What Led to The Disbandment Of Controversial Election Commission*, NPR All Things Considered (Jan. 4, 2018), <https://www.npr.org/2018/01/04/575774092/kris-kobach-on-what-led-to-the-disbandment-of-controversial-election-commission>.

⁷ *EPIC v. Presidential Election Commission*, <https://www.epic.org/privacy/litigation/voter/epic-v-commission/>.

⁸ 44 U.S.C. § 208.

⁹ Letter from EPIC, et al to DHS Secretary Nielsen, concerning State Voter Data and the Presidential Advisory Commission on Election Integrity (Jan. 8, 2018), <https://epic.org/privacy/litigation/voter/epic-v-commission/DHS-Nielsen-Letter-re-Commission-Data.pdf>. The organizations included EPIC, the ACLU, American Oversight, Brennan Center for Justice, Common Cause, Democracy Forward, Lawyers Committee for Civil Rights Under Law, Leadership Conference on Civil and Human Rights, NAACP Legal Defense Fund, Project Democracy, and Public Citizen.

Government Act of 2002, 44 U.S.C. § 3501 note, the Privacy Act of 1974, 5 U.S.C. § 552a, and the Paperwork Reduction Act, 44 U.S.C. §§ 3507–3521.”

The collection of state voter data by the DHS would be an egregious violation of millions of Americans’ privacy.

This Committee should seek assurance from Secretary Nielsen that the DHS will not continue the activities of the Presidential Advisory Commission on Election Integrity.

II. DACA

After the September 5, 2017 Department of Homeland Security memo rescinding the program, EPIC has been paying close attention to the privacy risks associated with the scheduled end of DACA.¹⁰ Between 2012 and 2017, over 800,000 DACA applicants submitted their personally identifiable biographic and biometric information to DHS.¹¹ This information includes birth certificates, employment records, bank records, housing records, transcripts, medical records, religious information, military records, information related to interactions with law enforcement, insurance documents, signatures, descriptive information such as height, weight, and ethnicity, biometric photos, and full fingerprints.¹²

DACA applicants submitted their information to DHS for the exclusive purpose of being considered for deferred action. This disclosure was made with the explicit understanding that their personal information would be subject to Privacy Act protections. When DACA was established in 2012, DHS conducted a Privacy Impact Assessment (“PIA”) for DACA. The PIA gave DACA applicants assurances that their information would not be disclosed to ICE or CBP for the purposes of immigration enforcement.¹³ This protection was extended to “family members and guardians, in addition to the individual.”¹⁴

The memo rescinding DACA fails to address the privacy risks associated with the use of data collected from DACA application. There is no new or updated PIA stating what will happen with the personal data collected for the purposes of determining eligibility for deferred action. In

¹⁰ See EPIC, About EPIC, <https://epic.org/epic/about.html>; Deferred Action for Childhood Arrivals (DACA), <https://www.epic.org/privacy/daca/>; and End of DACA Program Poses Privacy Risks to Dreamers, <https://epic.org/2017/09/end-of-daca-program-poses-priv.html>.

¹¹ Number of Form I-821D, Consideration of Deferred Action for Childhood Arrivals, by Fiscal Year, Quarter, Intake, Biometrics and Case Status Fiscal Year 2012-2017 (March 31), U.S. Citizenship and Immigration Services, https://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/Immigration%20Forms%20Data/All%20Form%20Types/DACA/daca_performancedata_fy2017_qtr2.pdf.

¹² See DHS/USCIS/PIA-045, Privacy Impact Assessment for the Deferred Action for Childhood Arrivals (DACA), available at https://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_uscis_daca.pdf; see also DHS/USCIS/PIA-045(a), Deferred Action for Childhood Arrivals (DACA) – April 2014, available at https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-dacaupdate-april2014_0.pdf.

¹³ See DHS/USCIS/PIA-045, Privacy Impact Assessment for the Deferred Action for Childhood Arrivals (DACA) at 3.3, available at https://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_uscis_daca.pdf.

¹⁴ See DHS/USCIS/PIA-045, Privacy Impact Assessment for the Deferred Action for Childhood Arrivals (DACA) at 7.1, available at https://www.dhs.gov/sites/default/files/publications/privacy/privacy_pia_uscis_daca.pdf.

addition, DHS has failed to make concrete assurances that it will maintain the protections promised in the 2012 PIA and set out usage described in the I-821D form and instructions.¹⁵

Acting Secretary of Homeland Security Elaine Duke stated that DHS would not promise to use DACA applicants' information exclusively for the purposes it was collected.¹⁶ This failure to ensure that information will be used exclusively for the purposes it was disclosed implicates the legal rights set out in the Privacy Act.

Therefore, this committee should seek assurance from Secretary Nielsen that the personal data provided by DACA applicants will be used exclusively for the intended purpose of determining deferred action eligibility, as stated in the original Privacy Impact Assessment for the program

III. Biometric Entry/Exit Tracking System

Customs and Border Protection ("CBP") is currently in the process of implementing a Biometric Entry/Exit Plan that implicates substantial privacy interests of Americans.¹⁷ The biometric entry/exit plan includes several initiatives to test the use of biometrics at entry/exit points within the U.S., including along the southwestern border.¹⁸

The Executive Order, "Protecting the Nation from Foreign Terrorist Entry into the United States," explicitly calls on the CBP to "expedite the completion and implementation of biometric entry exit tracking system."¹⁹ CBP is set to expand the scope of the agency's pilot programs testing the use of facial recognition at exits points from the U.S.²⁰

Facial recognition poses significant threats to privacy and civil liberties. It can be done covertly, remotely, and on a mass scale. Additionally, there are a lack of well-defined federal regulations controlling the collection, use, dissemination, and retention of biometric identifiers. Ubiquitous and near-effortless identification eliminates individual's ability to control their identities and poses a specific risk to the First Amendment rights of free association and free expression.

¹⁵ See Frequently Asked Questions: Rescission Of Deferred Action For Childhood Arrivals (DACA), available at <https://www.dhs.gov/news/2017/09/05/frequently-asked-questions-rescission-deferredaction-childhood-arrivals-daca>.

¹⁶ Sam Sacks, *DHS Chief Can't Promise She Won't Hand Over Dreamer Data to ICE*, truthout.com, (September 28, 2017), <http://www.truth-out.org/news/item/42092-dhs-chief-can-t-promise-she-won-thand-over-dreamer-data-to-ice>.

¹⁷ Dep't of Homeland Security, *Comprehensive Biometric Entry/Exit Plan: Fiscal Year 2016 Report to Congress* (2016), <https://www.dhs.gov/sites/default/files/publications/Customs%20and%20Border%20Protection%20-%20Comprehensive%20Biometric%20Entry%20and%20Exit%20Plan.pdf>.

¹⁸ See, e.g., U.S. Customs and Border Protection, *Biometric Travel Security Initiatives*, <https://www.cbp.gov/travel/biometric-security-initiatives>

¹⁹ Exec. Order No. 13,780 § 8.

²⁰ *Visa Overstays: A Gap in the Nation's Border Security: Hearing Before the Subcomm. on Border & Mar. Sec. of the H. Comm. on Homeland Sec.*, 115th Cong. (2017) (statement of John Wagner, Deputy Exec. Assistant Comm'r, Office of Field Operations, Customs & Border Prot.), available at <https://www.dhs.gov/news/2017/05/23/written-testimony-plcy-cbp-and-ice-house-homeland-securitysubcommittee-border-and>.

The use of facial recognition at the border has real consequences for U.S. citizens as well as non-U.S. citizens. All people entering the U.S., including U.S. passport holders, could be subject to this new screening technique. The CBP should be more transparent and more accountable about its biometric tracking system, which is why EPIC has sued the agency for documents about the program to release to the public.

This Committee should seek assurance from Secretary Nielsen that the facial recognition projects will not be expanded until transparency obligations are fulfilled and privacy safeguards are established.

Conclusion

We ask that this Statement from EPIC be entered in the hearing record. We look forward to working with you on these issues of vital importance to the American public.

Sincerely,

/s/ Marc Rotenberg

Marc Rotenberg
EPIC President

/s/ Christine Bannan

Christine Bannan
EPIC Policy Fellow