epic.org

Electronic Privacy Information Center
1718 Connecticut Avenue NW, Suite 200
Washington, DC 20009, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

October 24, 2017

Senator Orrin Hatch, Chairman
Senator Ron Wyden, Ranking Member
U.S. Senate Committee on Finance
219 Dirksen Senate Office Building
Washington, DC 20510-6200

Dear Chairman Hatch and Ranking Member Wyden:

We write to you regarding the nomination of Kevin McAleenan to be Commissioner of U.S. Customs and Border Protection ("CBP"). We have questions regarding (1) whether Kevin McAleenan would use DACA data for purposes unrelated to DACA eligibility; (2) CBP's use of facial recognition technology; (3) CBP's collection of social media information; (4) CBP's proposed exemption of Privacy Act safeguards for a new agency database; and (5) CBP's use of drones to conduct aerial surveillance on American citizens.

The Electronic Privacy Information Center ("EPIC") is a public interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues.[1] EPIC is a leading advocate for civil liberties and democratic values in the information age, and works closely with a distinguished Advisory Board, with specific expertise in the Privacy Act of 1974.[2] EPIC has raised several of the issues described above in comments to the agency and Freedom Information Act cases.

I. Use DACA Data for Purposes Unrelated to DACA Eligibility

After the Department of Homeland Security decision to rescind the Deferred Action for Childhood Arrivals program ("DACA"), EPIC has been paying close attention to the privacy risks associated with the possible misuse of the personal data provided by DACA applicants.[3] The Department of Homeland Security provided assurance in 2012 that personally identifiable information ("PII") provided by DACA applicants would not be disclosed to the CBP "for the purpose of immigration enforcement proceedings unless the individual meets the guidelines for the issuance of a Notice to Appear."[4] This protection was extended to "family members and guardians, in addition to the individual." The 2012 DHS Privacy Impact Assessment describes

[1] *See* EPIC, *About EPIC*, https://epic.org/epic/about.html.
[2] *See* EPIC Advisory Board, https://epic.org/epic/advisory_board.html.
[3] *See* EPIC, *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.
[4] *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.

the information management systems containing DACA applicant's information as "mixed systems" and explicitly states that "any PII that is collected, used, maintained, and/or disseminated in connection with a mixed system by DHS are to be treated as a System of Records subject to the Privacy Act" regardless of immigration status.[5]

Between 2012 and 2017, over 800,000 individuals submitted their personally identifiable biographic and biometric information to DHS for the DACA process.[6] 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.[7]

The Privacy Act of 1974 was enacted to address the privacy risks posed by the collection of personal information by the federal government.[8] The Privacy Act requires government agencies to comply with Fair Information Practices as set out in the 1973 report "Records, Computers and the Rights of Citizens."[9] The Privacy Act establishes a range of rights for data subjects. The Privacy Act also places restrictions on how agencies can share an individual's data with other people and agencies. Finally, the Act lets individuals sue the government for violating its provisions.[10] The Privacy Act is the foundation of privacy protection in the United States.[11]

Instructions for the I-821D form, to be filled by DACA applicants, states specifically that the information provided was "to request consideration of Initial DACA or Renewal of DACA."[12] The form also specifically states that "[i]nformation provided in this request is

---

[5] *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.

[6] 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

[7] *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; and 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.

[8] *See* EPIC, The Privacy Act of 1974, available at https://epic.org/privacy/1974act/; and The Privacy Act of 1974 , 5 U.S.C. § 552a available at https://epic.org/privacy/laws/privacy_act.html.

[9] *See*, EPIC, *The Code of Fair Information Practices*, available at https://epic.org/privacy/consumer/code_fair_info.html

[10] *Id*.

[11] EPIC has also called for Privacy Act modernization - *see*, EPIC, *Supplemental Letter on S. 1732, "Privacy Act EPIC Modernization for the Information Age Act of 2012"* available at https://epic.org/privacy/1974act/EPIC-Supp-S1732-Priv-Act-Modernization.pdf.

[12] Instructions for Consideration of Deferred Action for Childhood Arrivals, under see sections - What is the Purpose of this Form?, When Should I used Form 1-821D?, and USCIS Privacy Act Statement, available at https://www.uscis.gov/sites/default/files/files/form/i-821dinstr.pdf

protected from disclosure to ICE and U.S. Customs and Border Protection (CBP) for the purpose of immigration enforcement proceedings[.]"[13] The I-821D form itself states specifically that applicants "authorize the release of any information from my records that USCIS may need to reach a determination on my deferred action request."[14]

DACA applicants submitted their personal data to DHS for the exclusive purpose of consideration for deferred action. This disclosure was made with the explicit understanding that their personal information would be subject to Privacy Act protections.

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 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. In a September 5, 2017 website update, DHS stated:

> Information provided to USCIS in DACA requests will not be proactively provided to ICE and CBP for the purpose of immigration enforcement proceedings, unless the requestor meets the criteria for the issuance of a Notice To Appear or a referral to ICE under the criteria set forth in USCIS' Notice to Appear guidance (www.uscis.gov/NTA).[15]

Acting Secretary of Homeland Security Elaine Duke stated that DHS will 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.

In addition, the President, in a January 25, 2017 Executive Order, has mandated that "[a]gencies shall, to the extent consistent with applicable law, ensure that their privacy policies exclude persons who are not United States citizens or lawful permanent residents from the protections of the Privacy Act regarding personally identifiable information."[17] This statement, as applied to information provided by DACA applicants and is an assault on established U.S. privacy norms.

---

[13] *Id*. at USCIS Privacy Act Statement, pg. 13.
[14] I-921D, OMB 1615-0124, available at https://www.uscis.gov/i-821d.
[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-deferred-action-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-t-hand-over-dreamer-data-to-ice.
[17] *Enhancing Public Safety in the Interior of the United States* at Sec. 14, 82 FR 8799, *available at* https://www.whitehouse.gov/the-press-office/2017/01/25/presidential-executive-order-enhancing-public-safety-interior-united.

EPIC urges this committee to ask Mr. Kevin McAleenan about the privacy risks resulting from changes to DACA.[18]

- ***Will the personal information provided by DACA applicants be used exclusively for its intended purpose of determining deferred action eligibility, as stated in the 2012 Privacy Impact Assessment for the program?***

- ***Will Privacy Act of 1974 protections be extended to all information collected using I-821D forms, or in connection with the DACA application process?***

- ***Will DHS issue a new or updated Privacy Impact Assessment describing the privacy implications of its decision to rescind DACA and outlining its strategy for insuring that information provided by DACA recipients will be safe from misuse?***

II. CBP Facial Recognition Tracking Systems

The CBP's use of facial recognition technology raises substantial privacy and civil liberties concerns. CBP currently has multiple programs using facial recognition technology[19] and recently announced a new pilot program at JFK airport.[20] EPIC filed a complaint against CBP, seeking records concerning the CBP's use of facial recognition to implement a biometric entry/exit program at airports and other ports of entry.[21] EPIC is concerned that the CBP's biometric entry/exit tracking system lack proper privacy safeguards and maintains that the public should be fully informed about these systems. Without access to relevant records, EPIC and the public cannot assess the level to which the biometric entry/exist systems used and developed by the CPB safeguard and respect individual privacy.

The increasing use of facial recognition by law enforcement also implicates personal security. Improper collection, storage, and use of personal data produces identity theft, misidentifications, and infringement on constitutional rights. An individual's ability to control access to his or her identity, including determining when to reveal it, is an essential aspect of personal security and privacy. The use of facial recognition technology erodes that ability. Additionally, facial recognition technology can be done covertly, even remotely, and on a mass scale.

There is little that individuals can do to prevent collection on one's image. Participation in society involves exposing one's face. Ubiquitous and near effortless identification eliminates individual's ability to control their identities and poses a special risk to the First Amendment rights of free association and free expression, particularly to those who engage in lawful protests.

---

[18] *President Donald J. Trump Restores Responsibility and the Rule of Law to Immigration*, *available at* https://www.whitehouse.gov/the-press-office/2017/09/05/president-donald-j-trump-restores-responsibility-and-rule-law/.
[19] *EPIC v. CBP (Biometric Entry/Exit Program),* https://epic.org/foia/dhs/cbp/biometric-entry-exit/default.html.
[20] U.S. Customs and Border Protection, *CBP Deploys Facial Recognition Biometric Technology at 1 TSA Checkpoint at JFK Airport* (Oct. 11, 2017), https://www.cbp.gov/newsroom/national-media-release/cbp-deploys-facial-recognition-biometric-technology-1-tsa-checkpoint.
[21] *EPIC v. CBP*, Case No. 17-1438, https://epic.org/foia/cbp/biometric-tracking/1-Complaint.pdf.

The CBP's increasing use of biometrics on Americans has far-reaching implications for First Amendment freedoms.

EPIC urges this committee to ask Mr. Kevin McAleenan about the CBP's current and future uses of facial recognition technology.

- ***How exactly do these biometric tracking systems work?***
- ***What were the detail findings of the reports associated with the various pilot programs?***
- ***How expansive will the biometric entry-exit program become?***
- ***Will these biometric tracking systems move beyond ports of entry like airports?***
- ***How will CBP ensure that the collection and use of biometric data will not expand beyond the original purpose?***
- ***What privacy and civil liberties protections are currently in place?***

III. Social Media Information

The collection of social media information by CBP raises several concerns: whether it is necessary, whether it undermines First Amendment protected activities, and whether safeguards are in place to ensure oversight. EPIC has submitted comments in response to two recent proposals concerning social media: DHS's proposal to add social media information to an individual's Alien File[22] and CBP's proposal to ask visa applicants for their social media identifiers.[23]

The lack of transparency surrounding CBP's collection of social media information increases the prospect of abuse, mission creep, and targeting of marginalized groups. CBP has stated that the agency will use the social media identifiers for "vetting purposes, as well as applicant contact information."[24] Little additional information is provided. It is not clear how the CBP intends to use the social media identifiers. Other federal agencies have a history of using social media for controversial purposes. For example, DHS has monitored social and other media for dissent and criticism of the agency.[25] CBP has provided no details of how the agency will tailor the use of social media identifiers to ensure their use does not expand beyond the stated purpose or prevent the targeting of individuals merely engaged in First Amendment protected activities.

---

[22] Comments of EPIC, Department of Homeland Security, *Privacy Act of 1974; System of Records [Docket No. DHS-2017-0038]* (Oct. 18, 2017), https://epic.org/apa/comments/EPIC-DHS-Social-Media-Info-Collection.pdf.

[23] Comments of EPIC, Customs and Border Protection, *Agency Information Collection Activities: Electronic Visa Update System [Docket No. 2017-08505]* (May 30, 2017), https://epic.org/apa/comments/EPIC-CBP-Social-Media-ID-Collection-Comments.pdf.

[24] *Notice of request for public comment on "Agency Information Collection Activities: Electronic Visa Update System,"* 82 Fed. Reg. 19,380 (Apr. 27, 2017).

[25] Marc Rotenberg, President and Ginger McCall, EPIC Open Government Project Director, *Statement for the Record for Hearing on DHS Monitoring of Social Networking and Media: Enhancing Intelligence Gathering and Ensuring Privacy*, 1-3, Feb. 16, 2012, https://epic.org/privacy/socialmedia/EPIC-Stmnt-DHS-Monitoring-FINAL.pdf.

The indiscriminate scrutiny of social media accounts chills First Amendment protected activities. Freedom of speech and expression are core civil liberties that extend to non-U.S. citizens.[26] CBP states that obtaining social media identifiers, presumably to view user accounts, will provide more information to be used in the vetting process.[27] However, the proposal assumes that social media provides an accurate picture of a person and those they are close with. People connect with others on social media for many reasons. Often individuals connect to people on social media who have completely different perspectives and world views. Many individuals have made posts on social media which they later regret and may not be an actual reflection of who they are.[28] Social media does not necessarily reflect who a person truly is and taking posts out of context has the potential to wrongly deny people entry because of an inside joke or posturing that CBP does not understand from viewing certain information in isolation.[29] Government programs that threaten important First Amendment rights are immediately suspect and should only be undertaken where the government can demonstrate a compelling interest that cannot be satisfied in other way.[30] Government programs that scrutinize online comments, dissent, and criticism for the purpose of vetting visitors prior to entry into the U.S. send a chilling message to all users of social media—which increasingly provides important forums to share ideas, engage in debates, and explore new ideas.

The demand for an individual's personal identifier raises particular privacy concerns because this particular type of personal information is the key that ties together discrete bits of personal data. A social media identifier is not private in the sense that it is a secret. But the collection of a social media identifier by the government does raise privacy concerns because it enables enhanced profiling and tracking of individuals. In this way a social media identifier functions in the same way as a Social Security Number, the collection and use of which the U.S. has sought to regulate precisely because of the concern that it leads to government profiling.[31] Furthermore, an individual has no way of knowing who in the government may be tracking them

---

[26] *See* David Cole, *Are Foreign Nationals Entitled to the Same Constitutional Rights as Citizens?*, 25 T. Jefferson L. Rev. 367-388 (2003) ("foreign nationals are generally entitled to the equal protection of the laws, to political freedoms of speech and association, and to due process requirements of fair procedure where their lives, liberty, or property are at stake.").

[27] *Notice of request for public comment on "Agency Information Collection Activities: Electronic Visa Update System,"* 82 Fed. Reg. 19,380 (Apr. 27, 2017).

[28] Alyssa Giacobbe, *6 ways social media can ruin your life*, BOSTON GLOBE, May 21, 2014, https://www.bostonglobe.com/magazine/2014/05/21/ways-social-media-can-ruin-your-life/St8vHIdqCLk7eRsvME3k5K/story.html.

[29] Mateescu et. al., *Social Media Surveillance*; Brandon Giggs, *Teen failed for Facebook 'joke' is released*, CNN, Jul. 13, 2013 (discussing a teenager who was arrested after making a "threat" that, when viewed in context, appears to be sarcasm), http://www.cnn.com/2013/07/12/tech/social-media/facebook-jailed-teen/; Ellie Kaufman, *Social Media Surveillance Could have a Devastating Impact on Free Speech. Here's Why.*, MIC, Jan. 19, 2016, https://mic.com/articles/132756/social-media-surveillance-could-have-a-devastating-impact-on-free-speech-here-s-why.

[30] *See, e.g.*, *NAACP v. Button*, 83 S. Ct. 328 (1963); *Citizens United v. Fed. Election Comm'n*, 130 S. Ct. 876 (2010).

[31] Testimony of Marc Rotenberg, Computer Professionals for Social Responsibility, "Use of Social Security Number as a National Identifier," Before the Subcomm. on Social Security of the House Comm. on Ways and Means, 102d Cong., 1st Sess. 71 (February 27, 1991). republished Marc Rotenberg, "The Use of the Social Security Number as a National Identifier," *Computers & Society,* vol. 22, nos. 2, 3, 4 (October 1991); Privacy Act of 1974, 5 U.S.C. §552a (2016).

and for how long that surveillance could continue. What is initially presented as a way to vet visa applicants can turn into unwarranted, large scale surveillance of innocent people.

EPIC urges this Committee to ask Mr. Kevin McAleenan about the transparency, First Amendment, and privacy implications associated with the collection and analysis of social media information by CBP.

- ***Will the CBP monitor social media accounts for speech that is critical of U.S. policy? Will mere dissent constitute grounds for denying entry into the U.S.?***
- ***Will alien visitors who provide their social media identifiers open up their social network associations to scrutiny?***
- ***How long will social media identifiers be retained and who will they be shared with?***
- ***How will the CBP prevent Muslim and Arab Americans from being scrutinized more harshly?***
- ***What information will the social media identifiers be combined with?***
- ***Will CBP use the social media identifiers to obtain additional information about the applicant from social media companies?***
- ***Will applicants be informed if the information obtained from their social media accounts led to the denial of their application?***

IV. CBP's New Intelligence Database

CBP and DHS have recently proposed a rule that would establish a new system of records titled "DHS/CBP-024 CBP Intelligence Records System (CIRS) System of Records" and exempt that system from the Privacy Act.[32] According to the Notice of Proposed Rulemaking, "some of the information in CRS relates to official DHS national security, law enforcement, immigration, and intelligence activities" and the exemptions are needed "to protect information relating to DHS activities from disclosure to subjects or others related to these activities."[33] This does not explain why it is necessary to exempt this system of records.

The Privacy Act of 1974 was enacted to address the privacy risks posed by the collection of personal information by the federal government.[34] The Privacy Act requires government agencies to comply with Fair Information Practices as set out in the 1973 report "Records, Computers and the Rights of Citizens."[35] The Privacy Act establishes a range of rights for data subjects. The Privacy Act also places restrictions on how agencies can share an individual's data

[32] 6 C.F.R. pt. 5, https://www.gpo.gov/fdsys/pkg/FR-2017-09-21/pdf/2017-19717.pdf.
[33] *Id.*
[34] *See* EPIC, The Privacy Act of 1974, available at https://epic.org/privacy/1974act/; and The Privacy Act of 1974 , 5 U.S.C. § 552a available at https://epic.org/privacy/laws/privacy_act.html.
[35] *See*, EPIC, *The Code of Fair Information Practices*, available at https://epic.org/privacy/consumer/code_fair_info.html

with other people and agencies. Finally, the Act lets individuals sue the government for violating its provisions.[36] The Privacy Act is the foundation of privacy protection in the United States.[37]

- ***In the absence of Privacy Act protections, how does CBP plan to protect the privacy of American citizens and others?***
- ***How does CBP plan to protect the privacy of third parties?***
- ***Who will have access to this new system of records?***
- ***Will this new system of records contain social media information and, if so, how will it be used?***

V. Aerial Surveillance of American Citizens

The consequences of increased government surveillance through the use of drones are troubling. The ability to link facial recognition capabilities on drone cameras to databases containing facial biometrics increases the First Amendment risks for would-be political dissidents. In addition, the use of drones implicates significant Fourth Amendment interests and well established common law privacy rights. With special capabilities and enhanced equipment, drones are able to conduct far-more detailed surveillance, obtaining high-resolution picture and video, peering inside high-level windows, and through solid barriers, such as fences, trees, and even walls.

The House Homeland Security Committee recently passed the "Border Security for America Act,"[38] which would dramatically expand CBP's surveillance capabilities along the northern and southern borders of the U.S. The bill seeks "to achieve situational awareness and operational control of the border," with drones, biometric databases, and other surveillance tools. The Border Security Act would establish a biometric exit data system at US airports, seaports, and land ports. Biometric data would be combined with other Federal databases. The Privacy Act normally limits the government's ability to collect personal data, but this bill would exempt the Department of Homeland Security from compliance with the Privacy Act. Previous EPIC FOIA lawsuits have revealed that border surveillance by drones would capture imagery, data, and wifi data of US citizens.[39]

EPIC urges this committee to ask Mr. Kevin McAleenan about the CBP's use of drones.

- ***Will CBP link images collected by drones with facial biometrics in CBP or DHS databases?***
- ***In the absence of Privacy Act provisions, how will CBP ensure that the privacy of individuals is protected?***

---

[36] *Id*.
[37] EPIC has also called for Privacy Act modernization - *see*, EPIC, *Supplemental Letter on S. 1732, "Privacy Act EPIC Modernization for the Information Age Act of 2012"* available at https://epic.org/privacy/1974act/EPIC-Supp-S1732-Priv-Act-Modernization.pdf.
[38] H.R. 4548.
[39] EPIC, Spotlight on Surveillance: October 2014, https://epic.org/privacy/surveillance/spotlight/1014/drones.html/.

We ask that this Statement from EPIC be entered in the hearing record. EPIC looks forward to working with the Committee 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

/s/ *Jeramie Scott*
Jeramie Scott
EPIC National Security Counsel

/s/ *Siri Nelson*
Siri Nelson
EPIC Fellow