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

November 28, 2018

The Honorable Ron Johnson
Chairman
Senate Homeland Security and Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

The Honorable Claire McCaskill
Ranking Member
Senate Homeland Security and Governmental Affairs Committee
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill:

We write to you in advance of your hearing on the nomination of Ronald D. Vitiello to be Assistant Secretary for Immigration and Customs Enforcement (ICE) at the Department of Homeland Security.[1] While the Electronic Privacy Information Center (EPIC) takes no stance on any particular nominee, effective oversight begins with scrutiny during the nomination process. We therefore urge you to consider these issues as you engage with Mr. Vitiello.

I. ICE Must Ensure the Accuracy and Safety of Commercial Databases It Uses

ICE contracts with private companies to build vast databases of personal information that make secret determinations about employment, travel, and criminal investigations. Palantir, a secretive data mining firm, provides "management and analysis software" for key ICE systems.[2] ICE's FALCON and Investigative Case Management (ICM) systems pull together personal data from across the federal government to make determinations about individuals' fitness for employment, travel, or whether those individuals should be investigated by law enforcement.[3] EPIC has filed a FOIA lawsuit against ICE for information on the agency's relationship with Palantir and details of the databases Palantir helped create.[4]

These systems, largely shielded from Congressional oversight, create considerable risk to civil liberties. These databases and private companies' processing decisions are not subject to scrutiny. While ICE conducted a Privacy Impact Assessment, the Assessment specifically found that ICE does not verify the accuracy of the data relied upon by the FALCON database.[5] Despite the

[1] *Business Meeting, Before the S. Homeland Sec. & Governmental Affairs Comm.* (Nov. 28, 2018), https://www.hsgac.senate.gov/hearings/11/20/2018/business-meeting.
[2] Mijente, Who's Behind ICE? The Tech and Data Companies Fueling Deportations 10 (2018), https://mijente.net/wp-content/uploads/2018/10/WHO%E2%80%99S-BEHIND-ICE_-The-Tech-and-Data-Companies-Fueling-Deportations_v3-.pdf.
[3] *See* Jacques Peretti, *Palantir: The 'Special Ops' Tech Giant that Wields as Much Real-World Power as Google*, Guardian (July 30, 2017), https://www.theguardian.com/world/2017/jul/30/palantir-peter-thiel-cia-data-crime-police; Ashlee Vance & Brad Stone, *Palantir, The War on Terror's Secret Weapon*, Bloomberg (Nov. 22, 2011), https://www.bloomberg.com/news/articles/2011-11-22/palantir-the-war-on-terrorssecret-weapon.
[4] EPIC v. ICE, No. 17-2684 (D.D.C. Dec. 15, 2017), https://epic.org/foia/ice/palantir/1-Complaint.pdf.
[5] DHS/ICE/PIA-032(b) FALCON-SA, Privacy Impact assessment Update for the FALCON Search & Analysis System 15 (Oct. 11, 2016), https://www.dhs.gov/sites/default/files/publications/privacy-pia-ice-032-falcons-b-october2016.pdf.

clear dangers of the system, ICE does not provide users any notice that their data is being used or any opportunity to opt-out of the system.[6] Users are therefore subject to risks of data misuse, theft, or breach. ICE further compounds the risk by exempting the databases from many Privacy Act and disclosure requirements, actions EPIC opposed in public comments to the agency.[7]

Before confirming any nominee to lead ICE, Congress should ensure that systems being used to track or make inferences about individuals are accurate, fair, transparent, and secure. Specifically, this committee should ask the nominee:

- What specific steps will ICE take to ensure that data in the FALCON and ICM systems is accurate?
- How does ICE ensure algorithms used to analyze the personal information in these databases do not result in impermissible or illegal bias or profiling?
- What specific security measures does ICE have in place to ensure the massive amounts of individual data is protected from breach, misuse, and theft?
- How does ICE ensure that databases it uses comply with Privacy Act protections?

II. ICE Must Follow Minimum Procedures When Conducting Searches of Mobile Devices at the Border

Searches of cell phones and other electronic devices by border agencies have skyrocketed in recent years. In 2017, U.S. Customs and Border Protection (CBP) searched 30,200 electronic devices of individuals entering and leaving the United States—almost a 60% increase from 2016.[8] Searches of mobile devices are "basic" or "forensic." The government may conduct a "basic" search—where an agent manually searches the device for information—with no suspicion of wrongdoing.

In 2013, the Ninth Circuit ruled that the government must have reasonable suspicion to conduct a "forensic" search, where an agent connects another device to conduct a search.[9] Following that decision, CBP updated its policy to require the reasonable suspicion nationwide.[10] Despite this, ICE has failed to follow suit, and has not issued new guidance on mobile device searches at the border. This is troubling since it is often ICE agents who conduct searches of mobile devices. EPIC has sued ICE to gain access to information on warrantless searches at the border.[11]

ICE must adhere to minimum Fourth Amendment standards of suspicion when conducting searches. This committee should ask:

---

[6] *Id.* at 20

[7] Comments of the Electronic Privacy Information Center to the Department of Homeland Security, *Privacy Act of 1974: Implementation of Exemptions; Department of Homeland Security/U.S. Immigration and Customs Enforcement-016 FALCON Search and Analysis System of Records* (June 5, 2017), https://epic.org/apa/comments/EPIC-DHS-FALCON-Database-Comments.pdf.

[8] Press Release, U.S. Customs and Border Protection, CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

[9] United States v. Cotterman, 673 F.3d 1206 (9th Cir. 2012) (en banc).

[10] Press Release, U.S. Customs and Border Protection, CBP Releases Updated Border Search of Electronic Device Directive and FY17 Statistics (Jan. 5, 2018), https://www.cbp.gov/newsroom/national-media-release/cbp-releases-updated-border-search-electronic-device-directive-and.

[11] EPIC, *EPIC Sues ICE Over Technology Used to Conduct Warrantless Searches of Mobile Devices* (Apr. 9, 2018), https://epic.org/2018/04/epic-sues-ice-over-technology-.html.

- What guidance is in place for agents conducting searches of mobile devices at the U.S. border? Will ICE make that guidance public?
- Will ICE publish updated guidance that reflects the reasonable suspicion standard from *Cotterman*? If not, why not?

III. Use of Social Media Profiling

ICE has repeatedly expressed interest in monitoring social media profiles to collect information on immigrants.[12] The agency hired an outside contractor to "monitor public social communications on the Internet," including the public comments sections of the *New York Times*, *Los Angeles Times*, *Huffington Post*, *Drudge*, *Wired*'s tech blogs, and *ABC News*.[13] ICE further sought to establish "extreme vetting" programs that would use secret algorithms to determine visa eligibility.[14] EPIC warned that "the use of information technology to identify individuals that may pose a specific threat to the United States" implicates a "complex problem [that] necessarily involves subjective judgments."[15] Though that program was abandoned,[16] ICE left the door open to develop and implement similar or more intrusive programs, and has continued to contract with surveillance firms to mine social media information.[17] This is especially troubling given the agency's insistence that social media profiles should be exempted from Privacy Act protections.[18]

This committee must ensure that surveillance programs do not encroach the civil liberties and constitutional rights of Americans. Specifically, the committee should ask:

- How does ICE intend to use social media data acquired in this way?
- Who will the social media information be shared with and under what specific circumstances?
- How will ICE prevent at-risk communities from being scrutinized more harshly for exercising their First Amendment rights?
- Will ICE use the social media information to obtain additional data from social media companies?

---

[12] Comments of the Electronic Privacy Information Center to the Department of Homeland Security, *Privacy Act of 1974; System of Records*, EPIC (Oct. 18, 2017), https://epic.org/apa/comments/EPIC-DHS-Social-Media-Info-Collection.pdf.

[13] DHS Social Media Monitoring Documents at 127, 135, 148, 193, https://epic.org/foia/epic-v-dhs-media-monitoring/EPICFOIA-DHS-Media-Monitoring-12-2012.pdf; *see also* Charlie Savage, *Federal Contractor Monitored Social Network Sites*, N.Y. Times (Jan. 13, 2012), http://www.nytimes.com/2012/01/14/us/federal-security-programmonitored-public-opinion.html.

[14] EPIC, *EPIC, Coalition Oppose Government's 'Extreme Vetting' Proposal* (Nov. 16, 2017), https://epic.org/2017/11/epic-coalition-oppose-governme.html.

[15] *Security and Liberty: Protecting Privacy, Preventing Terrorism Before the National Commission on Terrorist Attacks Upon the United States* (Dec. 8, 2003) (statement of Marc Rotenberg, President, Electronic Privacy Information Center), https://epic.org/privacy/terrorism/911commtest.pdf.

[16] EPIC, *ICE Abandons "Extreme Vetting" Software to Screen Visa Applicants* (May 18, 2018), https://epic.org/2018/05/ice-abandons-extreme-vetting-s.html.

[17] *See* Chantal Da Silva, *ICE Just Launched a $2.4M Contract with a Secretive Data Surveillance Company that Tracks You in Real Time*, Newsweek (June 7, 2018), https://www.newsweek.com/ice-just-signed-24m-contract-secretive-data-surveillance-company-can-track-you-962493.

[18] EPIC, *CBP Plans to Exempt Social Media Data from Legal Protections* (Sept. 22, 2017), https://epic.org/2017/09/cbp-plans-to-exempt-social-med.html.

IV. Ensure Privacy Protections for Individuals in the DACA Program

Since a DHS memo rescinded DACA, EPIC has followed closely the privacy risks associated with the scheduled end of the program.[19] DACA was established in 2012.[20] The 2012 DHS Privacy Impact Assessment (PIA) for DACA assured that information provided by individuals in DACA requests is "protected from disclosure to ICE and CBP for the purpose of immigration enforcement proceedings" except in special circumstances.[21] This protection was extended to family members and guardians of applicants. Between 2012 and 2017, over 800,000 DACA applicants submitted their personally identifiable biographic and biometric information to DHS.[22] 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.[23]

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 protections. The memo rescinding DACA fails to address the privacy risks associated with using data collected from DACA application. There is no new or updated PIA stating what will happen with the personal data collected to determine eligibility for deferred action. In addition, DHS has failed to make concrete assurances it will maintain the protections promised in the 2012 PIA and set out usage described in the I-821D form and instructions. Former Acting Secretary of Homeland Security Elaine Duke explicitly stated that DHS would not promise to use DACA applicants' information exclusively for the purposes it was collected.[24]

This committee should ensure that DACA applicants receive the privacy protections to which they are entitled. Specifically, the committee should ask:

---

[19] See EPIC, *Deferred Action for Childhood Arrivals (DACA)*, https://www.epic.org/privacy/daca/; EPIC, *End of DACA Program Poses Privacy Risks to Dreamers* (Sept. 20, 2017), https://epic.org/2017/09/end-of-daca-program-poses-priv.html.

[20] Memorandum from Janet Napolitano, Secretary, DHS to David Aguilar, Acting Comm'r, CBP, et al., "Exercising Prosecutorial Discretion with Respect to Individuals Who Came to the United States as Children," https://www.dhs.gov/xlibrary/assets/s1-exercising-prosecutorial-discretionindividuals-who-came-to-us-as-children.pdf.

[21] *See* DHS/USCIS/PIA-045, Privacy Impact Assessment for the Deferred Action for Childhood Arrivals (DACA) at 3.3 (Aug. 15, 2012), https://www.dhs.gov/sites/default/files/publications/privacy_pia_uscis_daca_0.pdf [hereinafter 2012 DACA PIA].

[22] U.S. Citizenship and Immigration Servs., 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 (June 30), https://www.uscis.gov/sites/default/files/USCIS/Resources/Reports%20and%20Studies/Immigration%20Forms%20Data/All%20Form%20Types/DACA/daca_performancedata_fy2017_qtr3.pdf.

[23] *See* 2012 DACA PIA, *supra* note 21; DHS/USCIS/PIA-045(a), Deferred Action for Childhood Arrivals (DACA) (Apr. 17, 2014), https://www.dhs.gov/sites/default/files/publications/privacy-pia-uscis-dacaupdate-april2014_0.pdf.

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

- Will the personal information provided by DACA applicants be used exclusively for its intended purpose of determining deferred action eligibility, as stated in the original Privacy Impact Assessment for the program?
- Will ICE issue a new or updated PIA 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?

As surveillance technology becomes increasingly powerful and pervasive, it is critical that the Homeland Security and Governmental Affairs Committee ensure that individuals' rights are protected.

We appreciate the Committee's attention to this issue and ask that this statement be entered into the hearing record. EPIC looks forward to continuing to work with the Committee on issues of vital importance to the American public.

Sincerely,

/s/ *Marc Rotenberg*
Marc Rotenberg
EPIC President

/s/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

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

/s/ *Jeff Gary*
Jeff Gary
EPIC Legislative Fellow