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

March 5, 2019

The Honorable Bennie G. Thompson, Chairman
The Honorable Mike Rogers, Ranking Member
U.S. House Committee on Homeland Security
H2-176 Ford House Office Building
Washington, DC 20515

Dear Chairman Thompson and Ranking Member Rogers:

We write to you regarding the hearing "The Way Forward on Border Security."[1] 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.[2] EPIC is focused on the protection of individual privacy rights, and we are particularly interested in the privacy problems associated with surveillance.[3]

There are several border security proposals now before Congress that implicate the privacy rights of Americans. These practices include cell phone searches, scanning social media, and aerial drones.

EPIC writes to warn that enhanced surveillance at the border will almost certainly sweep up the personal data of U.S. citizens. Before there is any increased deployment of surveillance systems at the U.S. border, an assessment of the privacy implications should be conducted. Additionally, deployment of surveillance technology should be accompanied by new policy and procedures and independent oversight to protect citizens' rights. And any law enforcement agency that uses surveillance tools should comply with all applicable laws, including open government obligations. The privacy assessments, policies and procedures, and oversight mechanisms should all be made public.

The American Bar Association recently adopted a new policy on privacy rights and border searches.[4] The policy "urges the federal judiciary, Congress, and the Department of Homeland Security to enact legislation and adopt policies to protect the privacy interests of those crossing the

[1] *The Way Forward on Border Security*, U.S. House Comm. on Oversight and Gov't Reform (Mar. 6, 2019), https://homeland.house.gov/hearings-and-markups/hearings/way-forward-border-security.
[2] *See About EPIC*, EPIC.org, https://epic.org/epic/about.html.
[3] EPIC, *EPIC Domestic Surveillance Project,* https://epic.org/privacy/surveillance/, Statement of EPIC, "*Unmanned Aircraft Systems: Innovation, Successes, and Challenges,*" Hearing Before S. Comm. on Commerce, Sci., and Trans., United States Senate, Mar. 13, 2017, https://epic.org/testimony/congress/EPIC-SCOM-Drones-Mar2017.pdf; *The Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing Before the S. Judiciary Comm.,* 113th Cong. (2013) (statement of Amie Stepanovich, Director, EPIC Domestic Surveillance Project), https://epic.org/privacy/testimony/EPIC-Drone-Testimony-3-13-Stepanovich.pdf; Comments *of EPIC to DHS*, Docket No. DHS-2007-0076 CCTV: Developing Privacy Best Practices (2008), https://epic.org/privacy/surveillance/epic_cctv_011508.pdf.
[4] A.B.A., Resolution 107A (2019), https://www.americanbar.org/content/dam/aba/images/news/2019mymhodres/107a.pdf.

border by imposing standards for searches and seizures of electronic devices, protection of attorney-client privilege, the work product doctrine, and lawyer-client confidentiality."

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—almost a 60% increase from 2016.[5] Searches of mobile devices are "basic" or "forensic." Under current policy, the government may conduct a "basic" search—where an agent manually searches the device for information—with no suspicion of wrongdoing of the person whose device is subject to search.

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.[6] Following that decision, CBP updated its policy to require the reasonable suspicion nationwide.[7] Despite this change, Immigration and Customs Enforcement (ICE) has failed to issue 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.[8]

ICE should adhere to minimum Fourth Amendment standards of suspicion when conducting searches, particularly followed the Supreme Court's recent decisions in *Carpenter v. U.S. and Riley v. California*.[9]

Use of Social Media Profiling

DHS has repeatedly expressed interest in monitoring social media profiles to collect information on immigrants.[10] The department 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*.[11] DHS further sought to establish "extreme vetting" programs that would use secret algorithms to determine visa

---

[5] 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.
[6] United States v. Cotterman, 673 F.3d 1206 (9th Cir. 2012) (en banc).
[7] 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.
[8] 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.
[9] *Carpenter v. United States*, 138 S. Ct. 2206 (2018) (cell phone location records are protected under Fourth Amendment); *Riley v. California*, 134 S. Ct. 2473 (2014) (a warrantless search of a cell phone during an arrest violates the Fourth Amendment.)
[10] 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.
[11] 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.

eligibility.[12] 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."[13] Though that program was abandoned,[14] 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.[15] This is especially troubling given the agency's insistence that social media profiles should be exempted from Privacy Act protections.[16]

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?
- Who will obtain the data and under what circumstances?
- How will ICE prevent at-risk communities from being scrutinized more harshly for exercising their First Amendment rights?
- Will ICE obtain additional personal data from social media companies?
- Does the agency plan to conduct Privacy Impact Assessments prior to undertaking new data collection efforts?

Drones at the Border

Customs and Border Protection (CBP) is already deploying aerial drones with facial recognition technology at the border.[17] In 2013, records obtained by EPIC under the Freedom of Information Act also showed that the CBP is operating drones in the United States capable of intercepting electronic communications.[18] The records obtained by EPIC also indicate that the ten Predator B drones operated by the agency have the capacity to recognize and identify a person on the ground.[19] The documents were provided in response to a request from EPIC for information about the Bureau's use of drones across the country. The agency has made the Predator drones available to

---

[12] EPIC, *EPIC, Coalition Oppose Government's 'Extreme Vetting' Proposal* (Nov. 16, 2017), https://epic.org/2017/11/epic-coalition-oppose-governme.html.
[13] *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.
[14] EPIC, *ICE Abandons "Extreme Vetting" Software to Screen Visa Applicants* (May 18, 2018), https://epic.org/2018/05/ice-abandons-extreme-vetting-s.html.
[15] *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.
[16] 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.
[17] Russel Brandom, *The US Border Patrol is trying to build face-reading drones*, The Verge, Apr. 6, 2017, http://www.theverge.com/2017/4/6/15208820/customs-border-patrol-drone-facial-recognition-silicon-valley-dhs; Dept. of Homeland Security, *Other Transaction Solicitation (OTS) HSHQDC-16-R-00114 Project: Small Unmanned Aircraft Systems (sUAS) Capabilities*, Jul. 15, 2016, https://www.fbo.gov/spg/DHS/OCPO/DHS-OCPO/HSHQDC-16-R-00114/listing.html.
[18] EPIC, *EPIC FOIA - US Drones Intercept Electronic Communications and Identify Human Targets*, Feb. 28, 2013, https://epic.org/2013/02/epic-foia---us-drones-intercep.html (record received available at https://epic.org/privacy/drones/EPIC-2010-Performance-Specs-1.pdf.)
[19] *Performance Spec for CBP UAV System,* Bureau of Customs and Border Patrol, https://epic.org/privacy/drones/EPIC-2005-Performance-Specs-2.pdf.

other federal, state, and local agencies. The records obtained by EPIC raise questions about the agency's compliance with federal privacy laws and the scope of domestic surveillance.

Following the revelations about drone surveillance at the border, EPIC, joined by thirty organizations and more than a thousand individuals, petitioned CBP to suspend the domestic drone surveillance program, pending the establishment of concrete privacy regulations.[20] The petition stated that "the use of drones for border surveillance presents substantial privacy and civil liberties concerns for millions of Americans across the country." *Any authorization granted to CBP to conduct surveillance at the border must require compliance with federal privacy laws and regulations for surveillance tools, including drones.*

Much of this surveillance technology could, in theory, be deployed on manned vehicles. However, drones present a unique threat to privacy. Drones are designed to maintain a constant, persistent eye on the public to a degree that former methods of surveillance were unable to achieve. The technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology. Small, unmanned drones are already inexpensive; the surveillance capabilities of drones are rapidly advancing; and cheap storage is readily available to maintain repositories of surveillance data.[21] Drones "represent an efficient and cost-effective alternative to helicopters and airplanes," but their use implicates significant privacy interests.[22] As the price of drones "continues to drop and their capabilities increase, they will become a very powerful surveillance tool."[23] *The use of drones in border security will place U.S. citizens living on the border under ceaseless surveillance by the government.*

The Supreme Court has not yet considered the limits of drone surveillance under the Fourth Amendment, though the Court held twenty years ago that law enforcement may conduct manned aerial surveillance operations from as low as 400 feet without a warrant.[24] No federal statute currently provides adequate safeguards to protect privacy against increased drone use in the United States. However, some border states do limit warrantless aerial surveillance. In 2015, the Supreme Court of New Mexico held that the Fourth Amendment prohibits the warrantless aerial surveillance of, and interference with, a person's private property.[25] Accordingly, there are substantial legal and constitutional issues involved in the deployment of aerial drones by law enforcement agencies that need to be addressed.

A 2015 Presidential Memorandum on drones and privacy required that all federal agencies to establish and publish drone privacy procedures by February 2016.[26] Emphasizing the "privacy, civil

---

[20] EPIC, *Domestic Drones Petition*, https://epic.org/drones_petition/.
[21] *See generally* EPIC, *Drones: Eyes in the Sky*, Spotlight on Surveillance (2014), https://www.epic.org/privacy/surveillance/spotlight/1014/drones.html.
[22] M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 Stan. L. Rev. Online 29, 30 (Dec. 12, 2011); *See also* Jeffrey Rosen, *Symposium Keynote Address*, 65 Rutgers L. Rev. 965, 966 (2013) ("[A]s police departments increasingly begin to use drone technologies to track individual suspects 24/7, or to put areas of the country under permanent surveillance, this possibility of 24/7 tracking will become increasingly real.").
[23] Bruce Schneier, *Surveillance And the Internet of Things*, Schneier on Security (May 21, 2013), https://www.schneier.com/blog/archives/2013/05/the_eyes_and_ea.html.
[24] *See Florida v. Riley*, 488 U.S. 445 (1989) (holding that a police helicopter flying more than 400 feet above private property is not a search).
[25] *State v. Davis,* 360 P.3d 1161 (N.M. 2015); *see* Brief of *Amicus Curiae* EPIC, *id., available at* https://epic.org/amicus/drones/new-mexico/davis/State-v-Davis-Opinion.pdf.
[26] President Barack Obama, *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (Feb.

rights, and civil liberties concerns" raised by the technology,[27] President Obama ordered agencies to ensure that any use of drones by the federal government in U.S. airspace comply with "the Constitution, Federal law, and other applicable regulations and policies."[28]

However, the DHS has failed to produce reports required by the 2015 Presidential Memorandum. EPIC has submitted a FOIA request for DHS' policies and reports required under the Presidential Memorandum, but the DHS has failed to respond.[29]

As surveillance technology becomes increasingly invasive, it is critical that the Homeland Security Committee ensure that individuals' rights are protected. We ask that this letter 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/ *Caitriona Fitzgerald*
Caitriona Fitzgerald
EPIC Policy Director

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

15, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.
[27] *Id.* at § 1(e).
[28] *Id.* at § 1.
[29] EPIC, *EPIC v. DHS (Drone Policies)*, https://epic.org/foia/dhs_2/epic_v_dhs_drone_policies.html.