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

June 12, 2018

The Honorable Ron Johnson, Chairman
The Honorable Claire McCaskill, Ranking Member
U.S. Senate Committee on Homeland Security & Government Affairs
340 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Johnson and Ranking Member McCaskill:

In advance of the upcoming business meeting regarding "S. 2836, the Preventing Emerging Threats Act of 2018: Countering Malicious Drones,"[1] we write to inform you of EPIC's ongoing work to establish oversight for the use of unmanned aircraft, by both the government and the private sector. in the United States. EPIC believes that strong privacy and safety rules are vital for the safe integration of drones in the National Air Space. Before Congress grants the Department of Homeland Security expanded powers to take actions against drones in the National Airspace, it is imperative that Congress establishes drone privacy safeguards that limit the risk of massive and ongoing public surveillance. The present course is simply not sustainable.

EPIC is a public-interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has taken a particular interest in the unique privacy problems of Unmanned Aerial Vehicles (UAVs or "drones"). EPIC has brought a series of open government cases against the DHS and the Department of Defense to determine the use of drones by the federal government in the United States.[2] EPIC's cases have determined that drones operated by the DHS intercept private communications, conduct human identification at a distance, and may include military payloads.[3] EPIC's case against the DoD regarding JLENS found that the Army stationed a blimp just north of Washington, DC with the aim of conducting comprehensive aerial surveillance.[4] That program was later discontinued after the blimp broke free from its tether, took down power lines, and ended up in a forest in western Pennsylvania.[5]

It is our understanding that the DHS has failed to complete and publish the Privacy Impact Assessment required by the 2015 Presidential memorandum.[6]

---

[1] *Business Meeting*, 115th Cong. (2018), S. Comm. on Homeland Security & Governmental Affairs, https://www.hsgac.senate.gov/hearings/business-meeting-06/13/2018 (June 13, 2018).
[2] *EPIC v. DHS,* Case No. 18-545 (D.D.C. filed March 8. 2018).
[3] 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.
[4] *EPIC v. Army*, 1:14-cv-00776 (BAH) (D.D.C. filed May 6, 2014), https://www.epic.org/foia/army/.
[5] Matthew Brown, *JLENS blimp returns to Earth in Central Pennsylvania; military recovery 'in progress'*, Baltimore Sun (Oct. 28, 2015), http://www.baltimoresun.com/news/maryland/harford/aberdeen-havre-de-grace/bs-md-jlens-blimp-loose-20151028-story.html.
[6] President Barack Obama, *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (Feb.

EPIC has also sued the FAA for its failure to establish privacy safeguards to protect Americans.[7] EPIC is now proceeding in the U.S. Court of Appeals of the D.C. Circuit against the FAA for the agency's failure to establish drone privacy safeguards.[8] EPIC has also sued to enforce the transparency obligations of the Drone Advisory Committee, a body created by the FAA to study and make recommendations on U.S. drone policy.[9]

EPIC has also pursued several open government matters regarding the FAA's decision making process, which appears intended to purposefully avoid the development of meaningful privacy safeguards.[10]

Aerial Drones: A Unique Privacy Threat

Drones pose a unique threat to privacy. 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. A Pew Research Center and Smithsonian Magazine survey found that 63% of Americans objected to the idea of giving personal and commercial drones permission to fly through most U.S. airspace.[11] However, in recent years individual drone use has soared, and the FAA predicts that 7 million drones will be sold by 2020.[12] As drone use increases so do the risks to privacy and safety.

DHS and Other Federal Agencies Have Failed to Publish Drone Policies and Procedures

A 2015 Presidential Memorandum on drones and privacy required that all federal agencies to establish and publish drone privacy procedures by February 2016.[13] Emphasizing the "privacy, civil

---

15, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[7] *EPIC v. FAA*, No. 15-1075 (D.C. Cir. Filed Mar. 31, 2015); *See also Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, EPIC, https://epic.org/privacy/drones/; *See also* EPIC, *EPIC v. FAA, Challenging the FAA's Failure to Establish Drone Privacy Rules,* https://epic.org/privacy/litigation/apa/faa/drones/

[8] *EPIC v. FAA*, https://epic.org/privacy/litigation/apa/faa/drones/.

[9] EPIC v. Drone Advisory Committee, https://epic.org/privacy/litigation/faca/epic-v-drone-advisory-committe/default.html.

[10] *EPIC FOIA: Drone Industry Cozied Up to Public Officials* (Dec. 21, 2016), EPIC, https://epic.org/2016/12/epic-foia-drone-industry-cozie.html. EPIC v. DOT, No. 16-634 (D.C. Cir. Filed Apr. 4, 2016), https://epic.org/foia/dot/drones/taskforce/1-Complaint.pdf; *EPIC v. Department of Transportation - Drone Registration Task Force*, EPIC, http://epic.org/foia/dot/drones/taskforce/.

[11] Aaron Smith, *U.S. Views of Technology and the Future,* Pew Research Center, Apr. 17, 2014, http://www.pewinternet.org/2014/04/17/us-views-of-technology-and-the-future/.

[12] Sally French, *Drone Sales in the U.S. More Than Doubled In The Past Year,* Market Watch, May 28, 2016, http://www.marketwatch.com/story/drone-sales-in-the-us-more-than-doubled-in-the-past-year-2016-05-27; *FAA Aerospace Forecast: Fiscal Years 2016-2036*, FAA, 2016, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2016-36_FAA_Aerospace_Forecast.pdf.

[13] President Barack Obama, *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems* (Feb. 15, 2015), https://obamawhitehouse.archives.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

rights, and civil liberties concerns" raised by the technology,[14] 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."[15]

However, the DHS and other federal agencies have failed to produce reports required by the 2015 Presidential Memorandum. EPIC has filed a FOIA lawsuit against DHS for the agency's policies and reports required under the Presidential Memorandum. The case is currently ongoing. *EPIC urges the committee to ask DHS Deputy General Counsel, Hayley Chang, and FBI Assistant Director, Scott Brunner, whether their agencies have complied with the 2015 Presidential Memorandum?*

If the agency has completed the requirements, the agency should report should be publicly available. If the agency has not established policies and procedures for the use of drones, then we recommend no further action be taken on S. 2836 until the report is completed.

DHS Authority to Detect, Identify, Monitor, Track, Disrupt, and Seize Drones

S. 2836 gives the Department of Homeland Security enormous authority to detect, identify, monitor, track, disrupt, and even seize drones, but does not address the legal standard to exercise this authority. Does DHS need a warrant or exigent circumstances in order to act? This issue is not addressed in the bill.

Further, transparency is necessary for adequate oversight. The public reporting requirement regarding the use of the powers outlined in S. 2836 should require:

- A detailed description of every single instance where actions were taken under this bill, including:
    - Who authorized the actions, including if the actions were requested by any particular state or local entity;
    - The actions taken including whether the drone was tracked, seized, and/or if force was used to disable, damage or destroy the drone. Additionally, whether the operator was warned or communications were intercepted, acquired, or accessed;
    - If communications were retained and the nature of those communications;
    - What perceived threat the drone posed; and
    - Whether the drone was ultimately determined to actually be a threat.
    - Whether the property seized was returned to the owner or retained by the government

S. 2836 gives expanded powers to federal agencies to exert control over drones deemed a threat, yet the FAA has not taken any steps to address the day-to-day privacy threats drones pose to the American public and DHS has failed to inform the public of the agency's drone policies and

[14] *Id.* at § 1(e).
[15] *Id.* at § 1.

procedures. It's imperative Congress show the ability to hold these agencies to account before granting expanded authority.

Conclusion

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/ *Jeramie Scott*
Jeramie Scott
EPIC National Security Counsel

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

/s/ *Christine Bannan*
Christine Bannan
EPIC Administrative Law and Policy Fellow