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

May 6, 2019

The Honorable Roger Wicker, Chairman
The Honorable Maria Cantwell, Ranking Member
U.S. Senate Committee on Commerce, Science, and Transportation
512 Dirksen Senate Office Building
Washington, DC 20510

Dear Chairman Wicker and Ranking Member Cantwell:

In advance of the upcoming hearing on "New Entrants in the National Airspace: Policy, Technology, and Security Issues for Congress",[1] we write to inform you of EPIC's ongoing work to establish privacy safeguards and identification requirements for the deployment of drones in the National Airspace (NAS). The Federal Aviation Administration (FAA) must: 1) issue regulations on drone privacy, and 2) mandate the remote identification of drones. Further delay jeopardizes the security, safety, and privacy of Americans.

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"), has petitioned the FAA to establish limits on surveillance by drones, and has sued the FAA for its failure to establish privacy safeguards to protect Americans.[2] EPIC sued the FAA for the agency's failure to establish drone privacy safeguards.[3] EPIC has also filed suit 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.[4] That FAA committee has routinely ignored its own survey data that makes clear that Americans are concerned about the surveillance risks associated with drones.[5]

[1] *New Entrants in the National Airspace: Policy, Technology, and Security Issues for Congress*, 116th Cong. (2019), S. Comm. on Commerce, Sci., and Trans., https://www.commerce.senate.gov/public/index.cfm/2019/5/new-entrants-in-the-national-airspace-policy-technology-and-security-issues-for-congress (May 8, 2019).
[2] *EPIC v. FAA*, No. 15-1075 (D.C. Cir. May 10, 2016); *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/.
[3] *EPIC v. FAA*, https://epic.org/privacy/litigation/apa/faa/drones/.
[4] *EPIC v. Drone Advisory Committee*, https://epic.org/privacy/litigation/faca/epic-v-drone-advisory-committe/.
[5] Drone Advisory Committee survey, EPIC (obtained via FOIA), https://epic.org/privacy/litigation/faca/epic-v-drone-advisory-committe/Drone-Advisory-Committee-survey-sept-2016.pdf.

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.[6]

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 survey found that a majority of Americans object to drones flying near private homes.[7] However, in recent years individual drone use has soared, and the FAA predicts that 7 million drones will be sold by 2020.[8] As drone use increases so do the risks to privacy and safety.

Drones are now regularly equipped with high definition cameras that increase the ability of a user to conduct domestic surveillance.[9] The DJI Inspire 2 is a high-end, commercially available hobbyist drone about the size of a small desktop printer and weighs less than eight pounds, yet it can transmit high definition video to an operator over four miles away and can live-stream that video.[10] Even lower-end hobbyist drones costing less than $100 can stream live video. The Hubsan X4 H502E DESIRE, a drone that can fit in the palm of your hand, utilizes a front facing high definition camera with 720P resolution that can stream live video up to 200 meters away.[11] Drones can be used to view individuals inside their homes and can facilitate the harassment and stalking of unsuspecting victims.[12] Drones can also be modified with tools that can enable them to gather personal information using infrared cameras, heat sensors, GPS, automated license plate readers, and facial recognition devices.[13]

---

[6] *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. Department of Transportation - Drone Registration Task Force*, EPIC, http://epic.org/foia/dot/drones/taskforce/.

[7] Paul Hitlin, *8% of Americans say they own a drone, while more than half have seen one in operation,* Pew Research Center (Dec. 19, 2017), https://www.pewresearch.org/fact-tank/2017/12/19/8-of-americans-say-they-own-a-drone-while-more-than-half-have-seen-one-in-operation/.

[8] *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.

[9] Petition for Rulemaking Submitted by EPIC, Mar. 8, 2012, https://epic.org/apa/lawsuit/EPIC-FAA-Drone-Petition-March-8-2012.pdf; Univ. of Wash. Tech. and Pub. Policy Clinic, *Domestic Drones: Technical and Policy Issues* 12 (2013), https://www.law.washington.edu/clinics/technology/reports/droneslawan policy.pdf.

[10] DJI, *Inspire 2*, http://www.dji.com/inspire-2/info#specs.

[11] Hubsan, *X4 H502E DESIRE*, https://www.hubsanus.com/shop/h502e.html.

[12] Petition for Rulemaking Submitted by EPIC, *supra* note 8.

[13] *Id.*; Ciara Bracken-Roche et al., Surveillance Studies Centre, *Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada* 46 (Apr. 30, 2014), http://www.sscqueens.org/sites/default/files/Surveillance_Drones_Report.pdf; Mary Papenfuss, *Utah Couple Arrested Over 'Peeping Tom' Drone,* Huffington Post (Feb. 17, 2017), http://www.huffingtonpost.com/entry/peeping-tom-drone_us_58a6847fe4b045cd34c03e56.

Drones also pose risks to security and cybersecurity. Close calls between drones and traditional aircraft have risen significantly as their use becomes more widespread.[14] Furthermore, the very features that make drones easy to operate also make them susceptible to cyberattacks.[15] Hackers have the ability to exploit weaknesses in drone software to take over operation of a drone and access the camera and microphones.[16]

The United States Defense of Department is well aware of the risks of commercial drones. According to an internal memo, dated May 23, 2018, from the Secretary of Defense regarding Unmanned Aerial Vehicle Systems Cybersecurity Vulnerabilities, the "DoD Inspector General found that DoD has not implemented an adequate process to access cybersecurity risks associated with using commercial-off-the-shelf (COTS) Unmanned Aerial Systems (UAS)."[17] As a consequence, the Secretary instructed:

- "Effectively immediately, you must suspend purchases of COTS UAS for operational use until the DoD develops a strategy to adequately assess and mitigate the risks associated with their use.

- "(U/FOUO) In addition you must suspend the use of COTS UASs until the DoD identifies and fields a solution to mitigate known cybersecurity risks."

The DoD decision follows a letter to the Secretary from Senator Chris Murphy outlining concerns about drones manufactured by DJI, the largest distributor of commercial drones in the United States.[18] According to Senator Murphy, at least three separate agencies have found that the commercial unmanned aerial systems (UAS) from the Chinese drone manufacturer pose a potential national security threat.

The privacy risks of drones, as well as the safety and security vulnerabilities, underscore the need for the FAA to develop drone privacy regulations. *We urge the Committee to press the FAA to issue regulations on drone privacy, particularly following a ban by the Department of Defense on the purchase and use of commercial-off-the-shelf drones.*.

---

[14] Alan Levin, *Drone-Plane Near misses, Other Incidents Surge 46% in U.S.,* Bloomberg (Feb. 23, 2017), https://www.bloomberg.com/news/articles/2017-02-23/drone-plane-near-misses-other-incidents-surged-46-in-u-s.

[15] Dom Galeon, *As Drones Become Tools of War, Companies Turn to Hacking Them*, Futurism (Feb. 20, 2018), https://futurism.com/drone-hack-technology; Kacey Deamer, *How Can Drones Be Hacked? Let Us Count the Ways,* Live Science, Jun. 10, 2016, http://www.livescience.com/55046-how-can-drones-be-hacked.html.

[16] Wang Wei, *You Can Hijack Nearly Any Drone Mid-Flight Using This Tiny Gadget,* The Hacker News (Oct. 27, 2016), http://thehackernews.com/2016/10/how-to-hack-drone.html.

[17] Haye Kestello, *Department of Defense bans the purchase of commercial-over-the-shelf UAS, including DJI drones effective immediately*, DroneDJ, July 7, 2018, https://dronedj.com/2018/06/07/department-of-defense-bans-the-purchase-of-commercial-over-the-shelf-uas-including-dji-drones/

[18] Senator Chris Murphy, *Following Security Threats, Murphy Calls on Sec. Mattis to Ban Defense Department Use of Foreign-Made Commercial Drones: These vulnerabilities pose a tremendous national security risk… and without a trusted domestic source of unmanned aerial systems, we will continue to be vulnerable."* (May 8, 2018), https://www.murphy.senate.gov/newsroom/press-releases/following-security-threats-murphy-calls-on-sec-mattis-to-ban-defense-department-use-of-foreign-made-commercial-drones-and-instead-support-us-drone-manufacturers

The FAA Has Failed to Implement the Requirements of the FAA Modernization Act

The FAA has failed to take the action mandated by Congress. The FAA Modernization Act required the FAA to create a Comprehensive Plan to integrate drones into the National Airspace and subsequently conduct a notice and comment rulemaking. In the Plan, the FAA identified privacy as an important issue to address, acknowledging that "as demand for [drones] increases, concerns regarding how [drones] will impact existing aviation grow stronger, especially in terms of safety, privacy, frequency crowding, and airspace congestion."[19]

Under the FAA Modernization Act, Congress required the FAA to implement the recommendations of the Comprehensive Plan via a public rulemaking within 46 months of the enactment of the Act. The FAA identified privacy as an important issue directly related to domestic drones, yet the agency has failed to address privacy in the agency's only public rulemaking on drones in the National Airspace.[20] Indeed it has been over 60 months and the FAA has failed to implement the rulemaking that addresses the issues identified in the Comprehensive Plan, including privacy, as required by Congress.[21]

The FAA Has Failed to Conduct the Required Drone Privacy Report

Soon after the FAA's Comprehensive Plan identified privacy as an important drone integration issue, the agency was ordered by Congress to conduct a drone privacy report, which the agency failed to do. In the 2014 Consolidated Appropriations Act, Congress required the FAA to conduct a drone privacy study, stating:

> Without adequate safeguards, expanded use of UAS and their integration into the national airspace raise a host of concerns with respect to the privacy of individuals. For this reason, the FAA is directed to conduct a study on the implications of UAS integration into national airspace on individual privacy.[22]

The report specifically required the FAA to study "how the FAA can address the impact of widespread use of UAS on individual privacy as it prepares to facilitate the integration of UAS into the national airspace."[23] The report was to be submitted to Congress within 18 months of enactment of that appropriations bill and completed "well in advance of the FAA's schedule for developing final regulations on the integration of UAS into the national airspace."[24] Nearly 63 months since the bill was enacted, the FAA has failed to produce the report. Furthermore, EPIC obtained documents

---

[19] Joint Planning and Dev. Office, Fed. Aviation Admin., *Unmanned Aircraft Systems (UAS) Comprehensive Plan: A Report on the Nation's UAS Path Forward* 4 (2013), https://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf.
[20] Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42,063 (June 28, 2016) (codified at 14 C.F.R. pts. 21, 43, 61, 91, 101, 107, 119, 133, and 183).
[21] FAA Modernization and Reform Act of 2012, Pub. L. 112-95 § 332, 126 Stat. 73-75.
[22] See Explanatory Statement, Consolidated Appropriations Act of 2014, H.R. 3547, 113thCong., Division L at 6 (Jan. 14, 2014), https://www.congress.gov/congressional-record/2014/01/15/house-section/article/H475-2
[23] *Id.*
[24] *Id.*

through a Freedom of Information Act request that suggested that the FAA has no intention of complying with Congress' directive to produce a report.[25]

EPIC urges this Committee to ask the FAA why the agency has failed to take steps to protect the public from the privacy risks posed by drones. Any privacy and security risks are no longer hypothetical and the longer the FAA waits to issue comprehensive privacy rules, the longer the public is at risk.

Remote Identification of Drones

The Federal Aviation Administration recently published an interim final rule that will require a visible registration number on the exterior of drones.[26] Previously, registration numbers could be hidden inside drones. While EPIC agrees external marking are preferable to hidden identifiers, EPIC said the rule did not go far enough. In comments to the FAA, EPIC wrote, "Because drones present substantial privacy and safety risks, EPIC recommends that the FAA require any drone operating in the national airspace system to broadcast location when aloft (latitude, longitude, and altitude), course, speed over ground, as well as owner identifying information and contact information[.]"[27] EPIC also suggested the agency require operators register and broadcast surveillance capabilities.

As Senators Thune and Markey wrote to the FAA last week "remote identification will enhance safety, security, and privacy."[28] The Senators noted that the FAA was to issue regulations or guidance on remote identification by July 2018, but, nearly a year after that deadline, no such regulations or guidance has been issued by the FAA.

Currently, individuals cannot hold drone operators accountable because it is essentially impossible to identify the drone or the operator of a drone. The modified registration scheme proposed by the FAA still does little to solve this problem. Solutions exist.[29] To increase accountability of drone operators, the FAA Reauthorization Act of 2018 requires the FAA to consider and develop remote identification for drones.[30] As the FAA Aviation Rulemaking Committee Working Group 1 pointed out, "placing a sticker or FAA registration number on the UAS

---

[25] https://epic.org/privacy/litigation/apa/faa/drones/EPIC-16-07-20-FAA-FOIA-20160921-Production.pdf.
[26] *External Marking Requirement for Small Unmanned Aircraft*, 84 Fed. Reg. 3669-3673 (Feb. 13, 2019), https://www.federalregister.gov/documents/2019/02/13/2019-00765/external-marking-requirement-for-small-unmanned-aircraft.
[27] Comments of EPIC et al. to the Federal Aviation Admin., *External Marking Requirement for Small Unmanned Aircraft* (Mar. 15, 2019), https://epic.org/apa/comments/EPIC-Coalition-Comments-FAA-Drone-ID-Mar2019.pdf.
[28] Letter from Sen. Edward J. Markey and Sen. John Thune to the Honorable Elaine Chao, Secretary, U.S. Dept. of Trans. (Apr. 29, 2019), https://www.markey.senate.gov/imo/media/doc/Remote%20Indentification.pdf.
[29] *See, e.g.,* Isabella Lee, *FAA Issues Request for Information (RFI) from Industry Partners Interested in Developing Remote ID and Unmanned Traffic Management (UTM) Systems* (Jan. 24, 2019) https://uavcoach.com/remote-id-faa-rfi/ ("Remote ID development and testing has already begun in the private and commercial sector.").
[30] *See* Federal Aviation Administration Reauthorization Act of 2018, Pub. L. No. 115-254, § 376(b)(2), (c)(3)(A) 132 Stat. 3186, 3305–06 (2018) (directing the FAA to develop a plan for the implementation of unmanned aircraft systems traffic management (UTM) services that, *inter alia*, permit the testing of remote identification and that assess the risks raised and mitigation means required to remotely identify drones).

will not provide remote ID and tracking, as it would be nearly impossible to read a registration number on a UAS that is more than a few feet away."[31] Passive identification does not go far enough—the FAA must require active remote identification. The FAA should mandate remote identification and ensure also that drones routinely broadcast course, location, and other relevant operational information. Drones should simply not continue to fly above the laws that protect public safety.

The Committee should urge the FAA to complete a rulemaking on remote ID and to include privacy considerations in that rulemaking.

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 Senior Counsel

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

[31] Aviation Rulemaking Comm., Fed. Aviation Admin., ARC Recommendations Final Report: Appendix B Working Group 1 Report 42 (2017), https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf