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

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

Joined By

CONSUMER ACTION
PATIENT PRIVACY RIGHTS
PRIVACY TIMES

to the

FEDERAL AVIATION ADMINISTRATION

External Marking Requirement for Small Unmanned Aircraft

[Docket No. FAA–2018–1084, Amdt. No. 48– 2]

March 15, 2019

By notice published February 13, 2019, the Federal Aviation Administration ("FAA")

issued an interim final rule requiring all small unmanned aircraft to display the aircraft's unique

registration number externally and invited public comments.[1] Prior to this amendment, small,

unmanned aircraft owners were permitted to hide the registration number within an enclosed

compartment as long as it was accessible without the use of tools.[2]

EPIC submits these comments to the FAA to (1) express support for the FAA's decision

to require external display of registration numbers; (2) insist the agency adopt regulation

requiring small unmanned aircraft actively broadcast location, course, purpose, and registration

---

[1] *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.
[2] *Id.* at 3671

Defend Privacy. Support EPIC.

information for remote identification; and (3) request that the agency also require operators to register and broadcast surveillance capabilities.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.[3] For well over a decade, EPIC has maintained expertise on privacy, safety, and security concerns related to drones and has prominently advocated for better regulation of the national airspace related to these threats.[4] In 2012, EPIC, joined by more than one hundred experts and organizations, petitioned the FAA to undertake a rulemaking to establish privacy regulations prior to the deployment of commercial drones in the national airspace. In the Petition, EPIC described the many ways in which the deployment of drones would threaten important privacy interests.[5]

EPIC has repeatedly submitted comments to the FAA recommending that drone registration include disclosure of surveillance capabilities and explaining the necessity of active broadcast of registration information.[6] In earlier comments, EPIC stated "[t]he widespread deployment of drones in the United States is one of the greatest privacy challenges facing the Nation."[7] EPIC also testified to legislative bodies on the "unique threat to privacy" posed by

---

[3] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.

[4] EPIC, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones* (2019), https://epic.org/privacy/drones/; EPIC, *Spotlight on Surveillance: Unmanned Planes Offer New Opportunities for Clandestine Government Tracking* (Aug. 2005), https://epic.org/privacy/surveillance/spotlight/0805/.

[5] Petition from EPIC, et al., to Michael P. Huerta, Acting Adm'r, Fed. Aviation Admin. (Mar. 8, 2012), available at https://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.

[6] EPIC, *Comments of the Electronic Privacy Information Center to the Federal Aviation Administration of the Department of Transportation Docket No. FAA-2013-0061: Unmanned Aircraft System Test Site Program* 10 (Apr. 23, 2013), https://epic.org/apa/comments/EPIC-Drones-Comments-2013.pdf; EPIC, Comments on the *Clarification of the Applicability of Aircraft Registration Requirements for Unmanned Aircraft Systems (UAS) and Request for Information Regarding Electronic Registration for UAS*, Federal Aviation Admin. Docket No. FAA-2015-4378], 9-11 (Nov. 12, 2016), https://epic.org/privacy/drones/EPIC-FAA-Drone-Reg-Comments.pdf.

[7] EPIC, Comments on the *Operation and Certification of Small Unmanned Aircraft Systems*, Federal Aviation Admin. Docket No. FAA-2015-0150, 5 (Apr. 24, 2015), https://epic.org/privacy/litigation/apa/faa/drones/EPIC-FAA-NPRM.pdf.

drones[8] because "[t]he technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology."[9]

EPIC has also specifically recommended that drones broadcast location, course, and purpose.[10] EPIC wrote earlier that:

> passive registration does nothing to address the privacy risks posed by drones in the national airspace, which undermines the safe integration of drones into the national airspace. Drones should be required to broadcast their registration information to allow members of the public and law enforcement officials to easily identify the operator and responsible party.[11]

EPIC also wrote at the time:

> Because drones present substantial privacy and safety risks, EPIC recommends that any drone operating in the national airspace system include a mandatory GPS tracking feature that would always broadcast the location of a drone when aloft (latitude, longitude, and altitude), course, speed over ground, as well as owner identifying information and contact information.[12]

I.   The External Display of Registration Numbers is a Start

EPIC supports the FAA proposal to amend the rule to require that drone registration numbers be displayed externally. Beyond the safety risks from requiring physical inspection of a drone,[13] allowing drone operators to hide the number within a compartment means that a drone

---

[8] *Use of Unmanned Aerial Vehicles (Drones): Hearing Before the S. Majority Policy Comm. of the General Assembly of Pennsylvania*, 1-2 (2016) (statement of Jeramie D. Scott, EPIC National Security Counsel), https://epic.org/privacy/drones/EPIC-Drone-Testimony-20160315.pdf; *Crimes – Unmanned Aircraft Systems – Unauthorized Surveillance: Hearing Before the H. Judiciary Comm. of the General Assembly of Maryland*, 435th 1-2 (2015) (statement of Jeramie D. Scott, EPIC National Security Counsel), https://epic.org/privacy/testimony/EPIC-Statement-House-Bill-620.pdf*; Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?: Hearing Before the H. Subcommittee on Oversight, Investigations, and Management of the Comm. on Homeland Sec.*, 112th Cong. 4 (2012) (statement of Amie Stepanovich, EPIC Association Litigation Counsel), https://epic.org/privacy/testimony/EPIC-Drone-Testimony-7-12.pdf.
[9] EPIC National Security Counsel Jeramie D. Scott, Statement for the Rec. of the H. Judiciary Committee of the Gen. Assemb. of Md., *In Support of House Bill 620: "Crimes – Unmanned Aircraft Systems – Unauthorized Surveillance"*, 1 (Mar. 17, 2015).
[10] EPIC, Comments on the *Clarification of the Applicability of Aircraft Registration Requirements for Unmanned Aircraft Systems (UAS) and Request for Information Regarding Electronic Registration for UAS*, Federal Aviation Admin. Docket No. FAA-2015-4378 (Nov. 12, 2015), https://epic.org/apa/comments/EPIC-FAA-Drone-Reg-Comments.pdf.
[11] *Id.* at 11.
[12] *Id.*
[13] 84 Fed. Reg. 3671.

could not be identified while in operation. As such, the drone cannot be identified unless the drone has crashed or otherwise fallen to the ground. This hardly protects against unauthorized surveillance by paparazzi, private detectives, commercial entities, stalkers, and criminals, and encourages dangerous or unlawful self-help remedies (e.g. shooting down drones[14]).

Unfortunately, this modest step does not improve the situation much—the small registration numbers, wherever stamped, are unlikely to be visible while the drone operates. And remarkably the FAA has not even bothered to propose a minimum size for registration numbers as is routinely required on a ship's hull or a plane's fuselage. Registration numbers on a ship's hull "must be at least Three (3) inches in height."[15] Under FAA jurisdiction, the size of the registration markings for fixed-wing aircraft must generally be at least 12 inches high.[16] Even gliders and experimental aircraft must display marks of at least three inches.[17]

The failure of the FAA to even consider the height requirements and visibility of a registration number on a drone underscore the need for the agency to require the active transmission of registration information, in addition to course, location, and velocity.

II.   The FAA Must Go Further and Mandate Active Broadcast of Location, Course, and Purpose

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 still does little to solve this problem. Solutions exist.[18] To increase accountability of drone operators,

---

[14] James Vincent, *Judge Rules Kentucky Man Had The Right To Shoot Down His Neighbor's Drone*, The Verge (Oct. 28, 2015), https://www.theverge.com/2015/10/28/9625468/drone-slayer-kentucky-cleared-charges.
[15] **BoatUS, *Boat Documentation Requirements,* https://www.boatus.com/boatgraphics/uscg-requirements.asp**
[16] 14 C.F.R. 45.29(b)(1) (size of marks).
[17] 14 C.F.R. 45.29(b)(1) (ii), (iii) (size of marks).
[18] *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.").

the FAA Reauthorization Act of 2018 requires the FAA to consider and develop remote

identification for drones.[19] As the FAA Aviation Rulemaking Committee Working Group 1

("Working Group") pointed out, "placing a sticker or FAA registration number on the UAS 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."[20] Passive identification does not go far

enough—the FAA must require active remote identification.

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, similar to the Automated Identification System ("AIS") for

commercial vessels.[21]

The FAA Working Group has already recognized several means of identifying drones in

real-time, such as the integration of a direct broadcast method known as C2 that features high

ease of compliance, high readiness for implementation, strong operational performance and

security, and low cost for implementation.[22] The Working Group has also identified several

additional means of achieving remote identification via direct broadcast with slightly steeper

---

[19] *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).

[20] 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

[21] *See* 80 F.R. 5281, amending 33 C.F.R. § 164.46. The ADS-B standard is intended to provide sense and avoid capability for aircraft and may also be deployed for drones. However, it is not designed to provide information about UAS location, course, and speed to the general public. By contrast, information about vessels equipped with AIS is available to the public through freely available apps.

[22] *See* Aviation Rulemaking Comm., Fed. Aviation Admin., ARC Recommendations Final Report: Appendix B Working Group 1 Report 37–41 (2017), https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf.

hurdles to implementation.[23] Private companies have also demonstrated the feasibility of remote identification. Intel publicly demonstrated its "Open Drone ID" that uses Bluetooth 4.2 broadcast packs and Bluetooth 5 advertising extensions to broadcast the drone's "unique ID, location, direction, altitude, speed, make/model, base location, and other related data."[24] Wing, AirMap, and Kittyhawk also demonstrated remote identification of drones using a network-based remote ID application utilizing the open-source InterUSS platform.[25]

Recognizing the need for remote ID, the FAA has already requested unmanned aircraft system service suppliers ("USS") to submit input to "establish the operational framework (requirements and criteria) for Remote ID USS and provide supporting data to airspace users as necessary for collaboration and safe operations."[26] FAA has also stated in recent notices that:

> the FAA is cognizant of the importance of various stakeholders to be able to identify small UAS to mitigate safety concerns that operations may present. Because of the importance of this particular issue, the FAA plans to finalize its policy concerning remote identification of small UAS, by way of rulemaking, standards development or other activities that other Federal agencies may propose—prior to finalizing the proposed changes in this rule that would permit operations of small UAS over people and operations at night.[27]

EPIC agrees the FAA must conduct a rulemaking on Remote ID and adds that privacy considerations should be included in that rulemaking as well as any others on drone policy.

---

[23] *See, e.g.*, *id.* at 13–17 (ADS-B transceivers); *id.* at 18–22 (low power radio frequency).
[24] Mike Rees, *Intel Demonstrates Remote Drone Identification Solution*, Unmanned Sys. Tech. (Aug. 20, 2018), https://www.unmannedsystemstechnology.com/2018/08/intel-announces-new-open-standard-for-remote-drone-identification.
[25] Malek Murison, AirMap, Kittyhawk, and Wing Demonstrate InterUSS Remote ID Solution, DroneLife (Jan. 17, 2019), https://dronelife.com/2019/01/17/airmap-kittyhawk-and-wing-demonstrate-interuss-remote-id-solution.
[26] Fed. Aviation Admin., *FAA UAS Remote Identification Request for Information (RFI)-Data Exchange Strategies and Demonstrations for UAS Remote Identification* 2 (Jan. 31, 2019), https://faaco.faa.gov/index.cfm/announcement/view/32514.
[27] *Operation of Small Unmanned Aircraft Systems Over People*, 84 Fed. Reg. 3861 (Feb. 13, 2019), https://www.govinfo.gov/content/pkg/FR-2019-02-13/pdf/2019-00732.pdf. *See also Safe and Secure Operations of Small Unmanned Aircraft Systems*, 84 Fed. Reg. 3733, https://www.govinfo.gov/content/pkg/FR-2019-02-13/pdf/2019-00758.pdf.

The agency's practice of placing privacy concerns outside the scope of drone rulemakings[28] does not align with public opinion. In a recent behavioral sciences study, "the most popular [drone] policies were those that protected personal privacy."[29] Further, participants were nearly evenly divided as to which risks were most concerning: privacy (49.9%) and safety (50.1%).[30] As such, the FAA should cease its practice of excluding privacy concerns in drone policy formation.

III.   The FAA Must Require Drone Operators to Register and Broadcast Surveillance Capabilities

Drones are surveillance platforms able to carry a multitude of different data-collection technologies including high-definition cameras, geolocation devices, cellular radios and disruption equipment, sensitive microphones, thermal imaging devices, and LIDAR.[31] Drones can also be equipped to enable facial recognition, scan license plates, and identify nearby cell phones and other mobile devices.[32] The public should not be left to wonder what surveillance devices are enabled on a drone flying above their heads. Drone operators should be required to broadcast this information and not permitted to suppress the broadcast. If the capabilities of the drone are altered, the drone operators should be required to update his or her registration.

Operators of any drone carrying video surveillance technology should make clear at registration surveillance capabilities, including resolution and zoom range of any camera as well

---

[28] 84 Fed. Reg. 3893. *See also Operation and Certification of Small Unmanned Aircraft Systems*, 80 Fed. Reg. 9552 (Feb. 23, 2015), https://www.govinfo.gov/content/pkg/FR-2015-02-23/pdf/2015-03544.pdf.

[29] Adam Zwickle, Hillary B. Farber, and Joseph A. Hamm, *Comparing public concern and support for drone regulation to the current legal framework*, Behav. Sci. Law. 2018, 1 (May 23, 2018), available at https://www.researchgate.net/publication/326381803_Comparing_public_concern_and_support_for_drone_regulati on_to_the_current_legal_framework.

[30] *Id.* at 7.

[31] Richard M. Thompson II, Cong. Research Serv., R43965, *Domestic Drones and Privacy: A Primer* 3 (2015).

[32] *Id.*

as any capabilities like facial recognition[33] or license plate recognition.[34] Operators of any drone carrying audio surveillance technologies should be required to make clear at registration specific capabilities to capture and record audio communications. Operators of any drone carrying technology to engage in interception of signal communication, human recognition at a distance, or other advanced surveillance techniques, should be required at the time of registration to detail the capabilities and the anticipated use. Drones must be required to actively broadcast all of this information, too.

Conclusion

The FAA's proposal to require external markings on drones is a very, very small step in the direction of promoting accountability for drones. 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.

Respectfully submitted,

Electronic Privacy Information Center
Consumer Action
Patient Privacy Rights
Privacy Times

---

[33] *See*, e.g., April Glaser, *The Next Frontier of Police Surveillance Is Drones*, Slate (June 7, 2018), https://slate.com/technology/2018/06/axon-and-dji-are-teaming-up-to-make-surveillance-drones-and-the-possibilities-are-frightening.html.
[34] Julian Dasilva, Ricardo Jimenez, Roland Schiller, and Sanja Zivanovic Gonzalez, *Unmanned Aerial Vehicle-based Automobile License Plate Recognition System for Institutional Parking Lots*, 15 Systemics, Cybernetics and Informatics 39 (2015).