epic.org

Electronic Privacy Information Center
1519 New Hampshire Avenue NW
Washington, DC 20036, USA

+1 202 483 1140
+1 202 483 1248
@EPICPrivacy
https://epic.org

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

Joined By

Center for Digital Democracy
Constitutional Alliance
Consumer Action
Patient Privacy Rights
World Privacy Forum

to the

FEDERAL AVIATION ADMINISTRATION

Notice of Proposed Rulemaking: Remote Identification of Unmanned Aircraft Systems

[Docket No. FAA-2019-1100]

March 2, 2020

By notice published December 31, 2019, the Federal Aviation Administration ("FAA") issued a notice of proposed rulemaking regarding the remote identification of unmanned aircraft systems ("UAS" or "drones").[1] We note that this rulemaking arises at a time of growing concern about the deployment of drones in the United States, and the specific recognition that foreign adversaries conduct surveillance of the American public through commercial drones that the FAA has failed to regulate.[2]

---

[1] *Notice of Proposed Rulemaking: Remote Identification of Unmanned Aircraft Systems*, 84 Fed. Reg. at 72471 (Dec. 31, 2019) [hereinafter *Drone ID Proposed Rule*].
[2] Paul Mozur, *Drone Maker D.J.I. May be Sending Data to China, U.S. Officials Says,* N.Y. Times (Nov. 29, 2017), https://www.nytimes.com/2017/11/29/technology/dji-china-data-drones.html. Indeed, while the FAA has allowed industry lobbyists to stop regulatory initiatives that would safeguard the privacy of Americas, *EPIC FAA Petition* (Mar. 8, 2012), https://epic.org/privacy/litigation/apa/faa/drones/, other federal agencies have moved

The Electronic Privacy Information Center ("EPIC"), joined by the above named organizations, submit these comments to the FAA to recommend that (1) the drone ID information for all drones be publicly accessible in near real time via a smartphone app while the drone is aloft; (2) the drone ID information for all drones includes the location of the drone while in flight, the purpose of the drone, and the drone's surveillance capabilities; (3) privacy safeguards are implemented for recreational users; and (4) the FAA conduct a Privacy Impact Assessment on the privacy risks of increased drone surveillance.

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 since 2005.[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]

---

aggressively to protect the public interest. Lisa Friedman and David McCabe, *Interior Dept. Grounds Its Drones Over Chinese Spying Fears: The order formalizes a decision last year to ground the federal agency's drones pending an internal security investigation,* N.Y. Times (Jan. 29, 2020), https://www.nytimes.com/2020/01/29/technology/interior-chinese-drones.html.

[3] EPIC, *About EPIC* (2019), 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), https://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.

EPIC has submitted many comments to the FAA explaining the necessity of active broadcast of drone information.[6] In 2015, 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 drones[8] because "[t]he technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology."[9]

EPIC has specifically recommended that drones broadcast location and purpose.[10] EPIC wrote in 2015 that:

---

[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.

[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.

> 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]

EPIC's recommendations have now been adopted by the European Union and constitute international standards for the regulation of drones. EPIC applauds the FAA's publication of a proposed rule to require the remote identification of drones in the U.S. But EPIC urges the FAA to ensure that the drone ID information, proposed in the rule, is made available in real or near real time to the public and includes relevant information to allow the public to understand the purpose of a drone in their vicinity, the surveillance capabilities of the drone, and to obtain the actual identity of the operator of the drone.

I. Drone identification information must be readily available to the public and should include the purpose, location, course, and surveillance capabilities of the drone as well as the identity of the actual operator of the drone

The FAA's proposed rule envisions two categories of remote identification: standard remote identification and limited remote identification.[13] Standard identification requires the broadcasting of drone ID information directly from the drone while also sending that information to a Remote ID UAS service supplier ("Remote ID USS").[14] The proposed rule requires the

[11] *Id.* at 11.
[12] *Id.*
[13] Drone ID Proposed Rule at 72471.
[14] *Id.* at 72439.

broadcast capability to be functioning at takeoff and during the flight of the drone.[15] The following elements are to be part of the drone ID information that is actively broadcasted while in flight as well as transmitted to a Remote ID USS via an internet connection:

- The drone serial number or the session ID assigned by the Remote ID USS
- The latitude and longitude of the control station
- The latitude and longitude of the drone
- The barometric pressure altitude of the control station
- The barometric pressure altitude of the drone
- A Coordinated Universal Time timestamp
- Indicator of the emergency status (e.g. lost link, downed aircraft, etc.)[16]

The limited remote identification only requires the sending of drone ID information to a Remote ID USS through an internet connection and does not require the drone to actively broadcast the drone ID information.[17] Additionally, the limited remote identification does not require the latitude and longitude of the drone nor the barometric pressure altitude of the drone to be part of the drone ID information.[18]

a. All drones subject to the remote drone ID requirement should include the drone location, purpose, and surveillance capabilities

The current requirements for the limited remote identification do not require the location information of the drone to be included. This is a mistake. The location of the drone (e.g. latitude, longitude, and altitude) is necessary to assist in determining whether a drone is or was engaged in unsafe or privacy invasive activities.

Similarly, broadcasting/transmitting the purpose of the drone in real or near real time helps the public and authorities determine whether a drone is engaged in proper activities. The purpose of the drone should indicate whether the drone is recreational, commercial, or

[15] *Id.* at 72443.
[16] *Id.* at 72445.
[17] *Id.* at 72439.
[18] *Id.* at 72446.

government. Commercial drones should specify supplementary details (e.g. commercial-delivery, commercial-infrastructure inspection, commercial-media, etc.). Government drones should not be exempted from the remote drone ID. All drones operated by federal agencies should be required to transmit their actual drone ID. The alternative will lead to the secretive, mass surveillance of the American public.

Along with the purpose, the drone's surveillance capabilities should be readily available. Facial recognition or license plate reader capabilities should be stated explicitly and be made publicly available. Similarly, if a drone has audio sensors, an infrared camera, or thermal imaging capabilities that should also be publicly available. This is particularly important for commercial drones that may, in addition to a primary purpose such as delivery, engage also in surveillance of private property and the general public.

Requiring a standard way for drones to provide the public the drone's location, purpose, and capability will go a long way to relieve some of the privacy concerns that the public have about drones in the airspace.[19]

b. To address safety and privacy issues, the FAA should mandate public disclosure of surveillance capabilities in drone ID information in real time via a mobile app

The European Union has recognized that drones pose risks to security, privacy, and personal data.[20] In response, the European Commission established regulations setting out manufacturing and operating requirements for drones in the EuroZone.[21] The Commission enacted an EU-wide requirement that drones broadcast certain information including the operator

[19] *See* A. Michael Froomkin & Zac Colangelo, *Self-Defense Against Robots and Drones*, 48 Conn. L. Rev. 1, 59-61 (2015).
[20] Commission Implementing Regulation 2019/947 of 24 May 2019 on the rules and procedures for the operation of unmanned aircraft, 2019 O.J. (L152) 46d, https://eur-lex.europa.eu/eli/reg_impl/2019/947/oj.
[21] Commission Delegated Regulation (EU) 2019/945 of 12 March 2019 on unmanned aircraft systems and on third-country operators of unmanned aircraft systems, 2019 O.J. (L152).

registration number, drone serial number, geographic position and height of the drone, and location of the operator.[22] Importantly, the EU requirement mandates that the broadcast signal must be receivable by mobile devices.[23] The EU Drone Regulation applies to virtually any drone operating within the EU, regardless of where the drone was made or where it launched. The Commission's regulation sets an international norm that drones broadcast key information. Citizens of the EU now have a means of identifying the operator of drones posing safety or privacy hazards and resolving disputes with the operator.

In the U.S., the public should also have the ability to identify drones and connect the drone with the operator when warranted. Unidentified drones are a real problem and have crashed into a living room,[24] fallen into the stands at a crowded baseball stadium,[25] harassed students at a college track meet,[26] collided with landmarks,[27] and brought down powerlines.[28] In these cases drones posed a serious threat to the public, but the operators could not be identified.

---

[22] *Id* Annex Part II ¶ (12).
[23] *Id*.
[24] Eyewitness News, *Drone crashes into Manhattan apartment, shatters window*, abc7ny.com (Feb. 27, 2017), https://abc7ny.com/news/drone-crashes-into-manhattan-apartment-shatters-window/1774826/.
[25] Marissa Payne, *MLB will 'monitor the situation' after drone nearly takes out fans at Padres game*, Wash. Post (May 23, 2017), https://www.washingtonpost.com/news/early-lead/wp/2017/05/23/mlb-bans-drones-in-ballparks-after-one-nearly-takes-out-fans-at-padres-game/.
[26] Caleb Ragan, *Drone drops water balloons at Division 1 track prelims*, L.A. Times (May 13, 2017), https://www.latimes.com/sports/highschool/varsity-times/la-sp-high-school-sports-drone-attack-htmlstory.html.
[27] Jessica Lee, *Drone hits Seattle's huge Ferris wheel; SPD investigating*, Seattle Times (*last updated* Nov. 12, 2015 at 3:59pm), https://www.seattletimes.com/seattle-news/drone-hits-seattles-huge-ferris-wheel-spd-investigating/; Jessica Lee, *Watch: Drone crashes into Space Needle during New Year's Eve fireworks setup*, Seattle Times (*last updated* Jan. 11, 2017 at 9:00pm), https://www.seattletimes.com/photo-video/video/watch-drone-crashes-into-space-needle-during-new-years-eve-fireworks-setup/ (operator was eventually found).
[28] Joseph Serna, *Drone knocks out power to hundreds of West Hollywood residents*, L.A. Times (Oct. 27, 2015), https://www.latimes.com/local/lanow/la-me-ln-drone-power-west-hollywood-20151027-story.html.

As a result, crimes went unsolved and individual operators—either malicious or dangerously unskilled—avoided repercussions.

More recently, a mysterious fleet of drones have been spotted in Colorado, Nebraska, and Kansas.[29] The drones have unnerved local residents who have no idea why the drones are flying in their area, who owns them, or what surveillance capabilities the drones may have.[30] To this day local authorities have not been able to explain the presents of the drones.

Regardless of the final implementation of the means to broadcast/transmit the remote drone ID information, that information should be made available in real time to the public and should be easily accessible via a mobile app for any drone that has the ability to record human activity. Currently, there is no requirement for the limited remote identification information collected by a Remote ID USS to be made available to the public in real or near real time. Additionally, there is no requirement to make the drone ID information broadcasted by drones under the standard identification requirement to be easily accessible. The FAA states that the agency "anticipates that the message elements related to any standard remote identification UAS or limited remote identification UAS are publicly available information and may be accessed by any person able to receive a broadcast or who has access to a Remote ID USS."[31] This is simply not enough. The FAA must not only ensure that the drone ID information for both the standard remote identification and limited remote identification requirements is "publicly available" but also that the information is readily and easily accessible via a mobile app in real or near real time.

---

[29] Janet Shamlian, *FBI investigating drone swarms startling residents in three states*, CBS News (Jan. 6, 2020), https://www.cbsnews.com/news/mysterious-drone-swarms-3-states-fbi-investigation-latest-updates-today-2020-01-06/.

[30] *Id.*

[31] Drone ID Proposed Rule at 72471.

A remote drone ID requirement that requires drones to broadcast certain, relevant information and is readily available to the public will allow the public to assess the use of drones and to identify misuse. The remote drone ID requirement will also significantly reduce the identification problem by allowing any bystander to identify the drone's registration information and owner with their mobile device. Thus, there would be a record available to allow both law enforcement and private citizens to resolve drone incidents without resorting to dangerous self-help remedies.[32] In order to preserve this ability, the FAA should avoid "session IDs" that would mask the identity of drone operators.

II. The FAA needs to implement privacy safeguards for recreational drone users and consider the privacy implications of increased drone surveillance on the public

The FAA's current proposed rule fails to fully consider the privacy implications for recreational drone operators who will be required to provide drone ID information to Remote ID USS' as well as the privacy implications for the public at large as more drones enter the airspace.

a. The FAA should require privacy protections for drone ID information collected from recreational drone users by Remote ID USS'

According to the proposed rule, the Remote ID USS will "collect the identification and location in real-time from in-flight [drones]."[33] The proposed rule also requires the Remote ID USS to retain drone ID information for at least six months. The proposed rule states that, "although some Remote ID USS may choose to offer their services for free, Remote ID USS may have a variety of business models and may require a subscription, payment, or personal information to access that Remote ID USS."[34] The FAA assures us that the agency "would not

[32] *See* 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.
[33] Drone ID Proposed Rule at 72439.
[34] *Id.* at 72484.

have access to information collected by Remote ID USS other than the remote identification information required by this rule," but provides little assurance about how the Remote ID USS will use the information they are collecting. In the Privacy Impact Assessment, the FAA suggest that the agency will take into account privacy when creating agreements with the Remote USS ID and the Remote ID USS might be subject to the Privacy Act and other federal laws.[35]

The FAA proposed rule fails require any meaningful privacy protections for recreational drone users related to the collection, use, dissemination, or retention of the drone ID information by Remote ID USS'. Recreational drone users will be at the mercy of Remote ID USS as the current rule stands since they are required to provide their drone ID information to a Remote ID USS and may be required to provide more than that if the Remote ID USS so chooses. It is quite likely that the Remote ID USS offerings for recreational users will be limited to a few large companies who will seek to monetize the data collected from thousands of recreational drone users. The FAA should commit to strict privacy protections for Drone ID information collected by Remote ID users that limit the use of the information to the purpose of collection and requires the data to be purged after the information is retained for the required six months.

b. The FAA should conduct a comprehensive Privacy Impact Assessment that accounts for the risks of increased drone surveillance of the public

The Privacy Impact Assessment written in conjunction with this proposed rule fails to address the risks of increased drone surveillance on the public. Undoubtedly, the risk of drone surveillance will go up as the FAA pushes forward with the integration of drones into the airspace.

[35] U.S. Department of Transportation, *Privacy Impact Assessment: Federal Aviation Administration Remote Identification of Unmanned Aircraft Systems Proposed Rule*, 5, *available at* https://www.regulations.gov/document?D=FAA-2019-1100-0016.

Drones are aerial surveillance platforms and most drones are capable of conducting surveillance undetected. DJI's Mavic drones make possible dramatic video from a birds-eye view, but the drone is capable of widespread mass surveillance. The Mavic 2 Pro boast the ability to shoot in 4K and can transmit 1080p video as far as 8 km.[36] Additionally the Mavic 2 Pro is equipped with low-noise propellers, 2x optical zoom, and the ability to avoid objects in its path and track objects.[37]

As the commercial use of drones increases, drone features and capabilities will expand, especially if the FAA allows drones to operate beyond visual line of sight, at night, and in densely populated areas. Amazon was granted a patent outlining the use of the company's delivery drones for "surveillance as a service."[38] The patent contemplates audio and chemical sensors as well as night vision and thermal cameras.[39]

Defense contractors are already angling to integrate their large military-grade drones with their capability to fly continuously for over 40 hours into the U.S. airspace over cities to provide surveillance for police departments.[40] In the near future, commercial drones will be flying over densely populated areas with an array of sophisticated surveillance equipment. We urge the FAA

---

[36] DJI, *Mavic 2 Specs*, https://www.dji.com/mavic-2/info#specs (last visited Feb. 26, 2020).
[37] *Id.*
[38] U.S. Patent No. 10,313,638 (filed June 12, 2015); *See also* Jon Porter, *Amazon patents 'surveillance as a service' tech for its delivery drones*, The Verge (June 21, 2019), https://www.theverge.com/2019/6/21/18700451/amason-delivery-drone-surveillance-home-security-system-patent-application.
[39] *Id.*
[40] *See* Candice Bernd, *Large Military-Grade Drones Could Soon Be Flying Over Your Backyard*, Truthout (Jan. 16, 2020), https://truthout.org/articles/large-military-grade-drones-could-soon-be-flying-over-your-backyard/; *See also* Patrick Tucker, *Look for Military Drones to Begin Replacing Police Helicopters by 2025*, Defense One (Aug. 28, 2017), https://www.defenseone.com/technology/2017/08/look-military-drones-replace-police-helicopters-2025/140588/.

to conduct a PIA to begin to address the impact of increased drone surveillance on the American public.

Conclusion

The FAA's proposed rule to require remote drone ID is a step in the direction of drone accountability. EPIC supports the requirement for remote drone ID, but also urges the FAA to make clear the right of the public to access the drone ID, including the purpose, location, and course of the drone, as well as its surveillance capabilities and the identity of the actual operator, in real or near real time while the drone is aloft. This should be a minimal requirement for the safe and secure operation of drones in the United States.

Respectfully submitted,

Center for Digital Democracy
Constitutional Alliance
Consumer Action
Electronic Privacy Information Center (EPIC)
Patient Privacy Rights
World Privacy Forum