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

to the

FEDERAL AVIATION ADMINISTRATION

Operation of Small Unmanned Aircraft Systems Over People

[Docket No.: FAA–2018–1087; Notice No.18–07]

April 15, 2019

By notice published February 13, 2019, the Federal Aviation Administration ("FAA") published a notice for proposed rulemaking amending restrictions for small, unmanned aircraft, also known as "drones", operating over people and at night, and invited public comments.[1]

EPIC submits these comments to the FAA to: (1) reiterate the 2012 obligation the FAA has ignored to create privacy regulation for drones; (2) emphasize that the need for such regulation has only grown since that time; and (3) urge the establishment of a remote identification requirement that would broadcast location, course, purpose, operator identifying and contact information, and any 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.[2] For well over a decade, EPIC has maintained expertise on privacy, safety, and security concerns related to drones and has

[1] *Operation of Small Unmanned Aircraft Systems Over People*, 84 Fed. Reg. 3856-3907 (Feb. 13, 2019), https://www.federalregister.gov/documents/2019/02/13/2019-00732/operation-of-small-unmanned-aircraft-systems-over-people.
[2] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.

prominently advocated for better regulation of the national airspace related to these threats.[3] 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.[4]

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.[5] 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."[6] EPIC also testified to legislative bodies on the "unique threat to privacy" posed by drones[7] because "[t]he technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology."[8]

---

[3] 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/.

[4] 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.

[5] 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.

[6] 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.

[7] *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.

[8] 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).

EPIC has also specifically recommended that drones broadcast location, course, and purpose.[9] 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.[10]

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.[11]

I. The FAA has yet to address drone privacy, despite a Congressional mandate and repeated agency acknowledgement of the importance of privacy and civil liberties issues raised by drones.

The FAA Modernization and Reform Act of 2012 specifically mandated the creation of a "comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system."[12] In particular, Congress required the FAA to articulate "how the rulemaking will define the acceptable standards for operation and certification of civil unmanned aircraft systems."[13] Congress also required that the comprehensive plan outline "the best methods to enhance the technologies and subsystems necessary to achieve the safe and routine operation of civil unmanned aircraft systems in the national airspace system."[14] Further,

[9] 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.
[10] *Id.* at 11.
[11] *Id.*
[12] 49 U.S.C. § 44802(a)(1).
[13] 49 U.S.C. § 44802(a)(2)(A)(i).
[14] 49 U.S.C. § 44802(a)(2)(B).

Congress ordered the FAA—"not later than 18 months after" submission of the Comprehensive Plan—to publish "a notice of proposed rulemaking to implement the recommendations of the [comprehensive] plan required under subsection (a)(1)."[15]

Less than two weeks after the FAA Modernization and Reform Act of 2012 was signed into law, in February 2012, EPIC and over one hundred organizations, experts, and members of the public petitioned the FAA to conduct a notice and comment rulemaking related to the privacy and civil liberties impact of drones.[16]

In September 2013, the FAA finalized its Comprehensive Plan for drone integration, and stated, "Important non-safety related issues, such as privacy and national security, need to be taken into consideration as UAS [drones] are integrated into the NAS [national airspace]."[17] The Comprehensive Plan also specifically acknowledged, "as the demand for UAS increases, concerns regarding how UAS will impact existing aviation grow stronger, especially in terms of safety, *privacy*, frequency crowding, and airspace congestion."[18]

In November 2013, the FAA published a roadmap for the integration of drones into the airspace.[19] The Roadmap stated:

> The FAA is responsible for developing plans and policy for the safe and efficient use of the United States' navigable airspace. This responsibility includes coordinating efforts with national security and privacy policies so that the integration of UAS into the NAS is done in a manner that supports and maintains

[15] 49 U.S.C. § 44802(b)(2).
[16] 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.
[17] Joint Planning and Dev. Office, *Unmanned Aircraft Systems (UAS) Comprehensive Plan A Report on the Nation's UAS Path Forward*, 4 (Sept. 2013), available at https://www.faa.gov/about/plans_reports/congress/media/UAS_Comprehensive_Plan.pdf.
[18] *Id.* at 5 (emphasis added).
[19] Fed. Aviation Admin., U.S. Dep't of Transp., Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap (1st ed. 2013), available at https://www.faa.gov/uas/resources/policy_library/media/uas_roadmap_2013.pdf.

> the United States Government's ability to secure the airspace and addresses privacy concerns.[20]

Further, the Roadmap correctly asserted the expanded use of drones "raises questions as to how to accomplish UAS integration in a manner that is consistent with privacy and civil liberties considerations."[21]

In November 2014, the FAA responded to EPIC's petition for rulemaking on privacy concerns, asserting that the agency would consider the issues raised in our petition in an upcoming rulemaking.[22] That rulemaking came three months later when the FAA published a Notice of Proposed Rulemaking for the Operation and Certification of Small Unmanned Aircraft Systems, but contrary to what EPIC was led to believe, the proposed rulemaking specifically placed privacy concerns outside the scope of consideration, effectively denying EPIC's petition.[23] The FAA continues to simultaneously shirk any responsibility for addressing the privacy risks raised by drones, yet point out the importance of addressing drone privacy issues.

As recently as July 2018, the FAA continued to emphasize the importance of privacy, stating in the agency's updated Roadmap: "Much work must also be done to develop the standards necessary to support UAS certification processes. In addition to the technological and operational challenges posed by UAS integration, there are additional policy questions raised by UAS use, including security — both physical and cyber — and privacy."[24]

---

[20] *Id.* at 9.
[21] *Id.* at 11.
[22] Letter from Lirio Liu, Director, Office of Rulemaking, Fed. Aviation Admin., to Marc Rotenberg, EPIC Exec. Director (Nov. 26, 2014), available at https://epic.org/privacy/drones/FAA-Privacy-Rulemaking-Letter.pdf.
[23] *Operation and Certification of Small Unmanned Aircraft Systems*, 80 Fed. Reg. 9544 (Feb. 23, 2015), https://www.govinfo.gov/content/pkg/FR-2015-02-23/pdf/2015-03544.pdf.
[24] Fed. Aviation Admin., U.S. Dep't of Transp., *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap (Second Edition)*, 4-5 (July 30, 2018), available at https://www.faa.gov/uas/resources/policy_library/media/Second_Edition_Integration_of_Civil_UAS_NAS_Roadmap_July%202018.pdf.

Nevertheless, the FAA has failed to act on privacy, and once again placed drone privacy out-of-bounds from the public rulemaking process,[25] despite the agency's publications to Congress that echo the significance of privacy in this space.

II. The need for drone privacy regulation has only grown over time.

Back in 2014, 63% of Americans thought "opening U.S. airspace to drones would be a change for the worse," and only 22% said it would be a change for the better.[26] Nonetheless, drones already occupy American skies, but largely hover above regulation, despite a documented desire for accountability of drones in the airspace. A 2017 Pew survey determined that 59% of Americans polled had seen a drone in action, "[b]ut while drones… are more prevalent than they were a few years ago, many have reservations about where and under what circumstances their use should be allowed."[27]

Research shows that Americans specifically want *privacy* regulation of drones: In another recent behavioral sciences study, "the most popular [drone] policies were those that protected personal privacy."[28] Further, participants were nearly evenly divided as to which risks were most concerning: privacy (49.9%) and safety (50.1%).[29]

The Pew study showed "roughly half the public (54%) thinks drones should not be allowed to fly near people's homes. Just 11% think this should be allowed, while 34% think it is

[25] 84 Fed. Reg. 3893-3894.
[26] Andrea Caumont and Aaron Smith, *From teleportation to robot servants: Americans' predictions and dreams for the future*, Pew Research Center (Apr. 17, 2014), https://www.pewresearch.org/fact-tank/2014/04/17/from-teleportation-to-robot-servants-americans-predictions-and-dreams-for-the-future/.
[27] 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/.
[28] 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_regulation_to_the_current_legal_framework.
[29] *Id.* at 7.

OK in certain circumstances but not others."[30] Further, only 24% of respondents thought that drones should be allowed "[a]t events, like concerts or rallies," while 45% thought they should not be allowed. These statistics are directly relevant to the proposal to allow drones to operate over people, and ought to be taken into account.

In line with what EPIC has repeatedly said since the FAA Modernization and Reform Act of 2012 was passed and keeping with the public's clear desire for legal limits to the use of drones and accountability for operators, Senator Markey has reiterated his call for privacy protections and introduced legislation to do so:

> Privacy cannot be an afterthought as the FAA seeks to make it easier and safer for commercial drones to take flight… Drones have the capability to collect treasure troves of sensitive personal information using technologies like facial recognition and automated license plate readers, yet the FAA has failed to establish any baseline privacy protections, despite its obligation to integrate drones into the national airspace. This neglect of American's right to privacy in the age of drones is unacceptable. Congress must man the controls, which is why I will be reintroducing my Drone Aircraft Privacy and Transparency Act to protect the public from these potential flying spies in the skies.[31]

State legislatures echo the importance of privacy regulation for the integration of drones into the airspace. As of September 2018, "State legislatures across the country are debating if and how UAS [drone] technology should be regulated, taking into account the benefits of their use, privacy concerns and their potential economic impact. So far, 41 states have enacted laws addressing UAS and an additional three states have adopted resolutions."[32] For instance, Colorado mandated a public safety study which includes consideration of privacy concerns.[33]

---

[30] 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/.

[31] Statement of Sen. Markey, *Senator Markey Calls for Privacy Protections in Wake of FAA Drone Proposal*, (Jan. 15, 2019), available at https://www.markey.senate.gov/news/press-releases/senator-markey-calls-for-privacy-protections-in-wake-of-faa-drone-proposal.

[32] National Conference of State Legislatures, *Current Unmanned Aircraft State Law Landscape* (Sept. 10, 2018), http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.

[33] Colo. Rev. Stat. 24-33.5-1228(2.5)(c)(I)(B), available at http://leg.colorado.gov/bills/hb17-1070.

New Jersey law recognizes particular crimes of drone surveillance and specifically addresses the use of drones to violate restraining orders.[34] South Dakota modified unlawful surveillance law to include "Intentionally us[ing] a drone to photograph, record, or otherwise observe another person in a private place where the person has a reasonable expectation of privacy[.]"[35] And Connecticut's Office of Legislative Research conducted a study, exclusively devoted to privacy implications of drones, back in 2014.[36]

How is it that, in 2019, the FAA continues to ignore its responsibility to regulate drones with respect to individual privacy? The 52-page proposed rule dedicates a mere five paragraphs to privacy, simply claiming it is beyond the scope of their authority. As emphasized above, that is simply not true.[37]

III. The FAA must implement meaningful privacy protections prior to allowing drone operation over people and at night.

EPIC has repeatedly called for remote, broadcast ID.[38] 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),

[34] N.J. Pub. L. 2017, Ch. 315(2)(f) ftp://www.njleg.state.nj.us/20162017/AL17/315_.HTM.
[35] S.D. Codified L. § 22-21-1(3), https://sdlegislature.gov/Statutes/Codified_Laws/DisplayStatute.aspx?Type=Statute&Statute=22-21-1.
[36] Timothy Bleasdale, Ofc. of Legis. Research, Conn. Gen. Assemb., 2014-R-0137, *Privacy Protections Implicated by the Domestic Use of Unmanned Aerial Vehicles or Drones* (May 12, 2014), https://www.cga.ct.gov/2014/rpt/pdf/2014-R-0137.pdf.
[37] 84 Fed. Reg. 3893-3894.
[38] 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, 2015), available at https://epic.org/apa/comments/EPIC-FAA-Drone-Reg-Comments.pdf; EPIC, Comments on *External Marking Requirement for Small Unmanned Aircraft*, Fed. Aviation Admin. Docket No. FAA-2018-1084, Amdt. 48-2, 4-8 (Mar. 15, 2019), available at https://epic.org/apa/comments/EPIC-Coalition-Comments-FAA-Drone-ID-Mar2019.pdf.

course, speed over ground, as well as owner identifying information and contact information, similar to the Automated Identification System ("AIS") for commercial vessels.[39]

Further, 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.[40] Drones can also be equipped to enable facial recognition, scan license plates, and identify nearby cell phones and other mobile devices.[41] 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.

Without mandating broadcast of identifying information, location, course, purpose, and surveillance capabilities, drones should not be further integrated into the airspace in the ways the proposed rule suggests.

a. Drones operating over people must be required to register and broadcast identifying information and surveillance capabilities.

The section proposing regulation of drones to allow for operations over people lays out three categories of drones, based on physical characteristics and potential for harm from direct impact, and presents associated restrictions corresponding to each category. Category 1 drones

[39] *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.
[40] Richard M. Thompson II, Cong. Research Serv., R43965, *Domestic Drones and Privacy: A Primer* 3 (2015).
[41] *Id.*

are any drones that weigh .55 pounds or less.[42] According to the proposed rule, drones in Category 1 can fly over people with no restrictions.[43]

Drones weighing over .55 pounds fall into one of two categories. Category 2 includes drones "designed, upon impact with a person, not to result in an injury as severe as the injury that would result from a transfer of 11 ft-lbs of kinetic energy from a rigid object."[44] Additionally, there can't be any exposed portion that would lacerate skin, and the drone cannot have an FAA-identified safety defect with "more than a low probability of causing a casualty."[45] All that is required for a Category 2 drone to fly over people is for the manufacturer to show compliance.[46]

Category 3 is largely the same, however, there is a higher injury threshold for impact or safety defects.[47] There are additional limitations for Category 3 drones flying over people: Flying over open-air assemblies of people is prohibited, and "[t]he operations would have to be within or over a closed- or restricted-access site and anyone within that site would have to be notified that a small unmanned aircraft may fly over them."[48]

Under the proposed rule, drones .55 pounds or under can be operated over people without any additional restrictions as a condition of flying over people because they "pose a low risk of injury."[49] These restrictions completely ignore the implications of drones flying overhead beyond risk of direct physical injury. There are numerous drones under a half-pound outfitted with

[42] 84 Fed. Reg. 3858.
[43] *Id.*
[44] 84 Fed. Reg. 3858.
[45] *Id.*
[46] *Id.*
[47] 84 Fed. Reg. 3858-59.
[48] 84 Fed. Reg. 3859.
[49] 84 Fed. Reg. 3858.

cameras,[50] and even some with facial recognition,[51] readily available. The research to support the rule only relates to harms from direct impact.[52] Research on drones' potential for privacy violations should also be considered:

> Privacy torts present the most difficult, but also some of the most important, justifications for self-defense against robots. Invasions of privacy can result in very significant harms… That said, there are significant issues with how a person facing a robot could know what it is capable of[.][53]

The FAA does not currently require drones to broadcast their surveillance capabilities, so even the most prudent privacy-minded person has no way of knowing if the drone hovering overhead, regardless of weight, is outfitted with invasive surveillance technology. According to a Pew Research study, one in four Americans would be nervous if they saw a drone near their home, and one in ten would be angry or scared.[54]

Legal research supports this conclusion:

> I have in mind the effect on citizens of drones flying around United States cities. These machines are disquieting. Virtually any robot can engender a certain amount of discomfort, let alone one associated in the mind of the average American with spy operations or targeted killing. If you will pardon the inevitable reference to 1984, George Orwell specifically describes small flying devices that roam neighborhoods and peer into windows. Yet one need not travel to Orwell's Oceania… to encounter one of these machines.[55]

---

[50] Joshua Goldman, *Best toy drones you can buy right now*, CNET (Apr. 14, 2016), https://www.cnet.com/news/best-toy-drones/ (listing 8 drones that weigh less than .55 lbs.).
[51] Zerotech, *ZEROTECH Introduces Advanced Features for DOBBY Pocket Drone at CES 2017*, PR Newswire (Jan. 9, 2017) https://www.prnewswire.com/news-releases/zerotech-introduces-advanced-features-for-dobby-pocket-drone-at-ces-2017-300387694.html ("Despite weighing a mere 7 ounces (199 grams) and taking advantage of not need to register in American, DOBBY combines the best-in-class technology characteristic of high-performance drones, including facial recognition and target tracking[.]"); Hover, *Hover Camera Passport*, https://gethover.com/hover-camera-passport (The 242-gram drone can "track your face or body and accompany your journey.") (last accessed Mar. 21, 2019).
[52] 84 Fed. Reg. 3871.
[53] A. Michael Froomkin and P. Zak Colangelo, *Self-Defense Against Robots and Drones*, 48 Conn. L. Rev. 1, 30 (2015), available at https://repository.law.miami.edu/cgi/viewcontent.cgi?article=1061&context=fac_articles.
[54] 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/.
[55] M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 Stan. L. Rev. Online 29, 32 (2011).

Drone surveillance capability registration and active broadcast is particularly important, given the proposed rule even explicitly anticipates the drones falling into this virtually unregulated category will be used for photography.[56]

EPIC argues that many of the rules for Category 3 drones should apply to all drones. For instance, flying over open-air assemblies of people is prohibited for these larger drones.[57] EPIC approves of this prohibition and further argues some modified version of this rule should apply to all drone operations over people, not just Category 3. For the other categories, there should be a permit requirement to operate over an assembly of people. This would allow for press or photography drones to document historic scenes or events, but still provide accountability. Unrestricted use of drones over protests, without identification or attribution, could have a chilling effect on free expression.

"The operations would have to be within or over a closed- or restricted-access site and anyone within that site would have to be notified that a small unmanned aircraft may fly over them."[58] Some version of this rule should apply to all drones flying over people. There needs to be advance warning or notification provided to folks if a drone will operate over them. This should apply to public events, as well as closed sites.

None of the three categories address potential for harms unrelated to direct impact with a drone. To that end, EPIC recommends remote, broadcast ID should be required for *all drones at all times*, but especially whenever a drone flies over people. The proposed rule acknowledges that remote ID must be addressed, "by way of rulemaking, standards development, or other

[56] 84 Fed. Reg. 3871.
[57] 84 Fed. Reg. 3859.
[58] 84 Fed. Reg. 3859.

activities that other Federal agencies may propose—prior to finalizing the proposed changes in this rule[.]"[59]

Broadcast ID should be mandated for all drones at all times. EPIC further 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, as well as all surveillance capabilities.

Broadcast ID would make the notification requirements proposed for Category 3 drones easier to satisfy as well. Just as there are apps where you can track where manned aircraft and sea vessels are, you should be able to track drones in an area through broadcast ID. This app could provide push notifications of drone operations happening overhead in real-time, as well as notifications of when you are entering an area where a permit has been obtained to fly a drone. Like previous comments stated, the broadcast should include identifying information, location information, and all surveillance capabilities.

The FAA "proposes requiring a remote pilot ensure his or her small unmanned aircraft is properly labeled before conducting any operations over people. A clear and legible label [indicating which category the drone falls under] will enable a remote pilot, an inspector, or a member of the public to identify the types of operations a small UAS may conduct."[60] This is clearly unrealistic. When a drone is in the air, it is extremely unlikely that a remote pilot, an inspector, or a member of the public would be able to tell if the drone was operating within the restrictions on its category. You can't read a label on a tiny object flying over your head.

[59] 84 Fed. Reg. 3861.
[60] 84 Fed. Reg. 3886.

The privacy harms associated with drones are real[61] and only get more severe as technology advances. The virtually unregulated drones in Category 1 can have facial recognition and high-grade camera equipment, which opens them up to covert stalking.[62] Drones have also been linked to hate crimes,[63] and there are reports they have been used to film ATMs.[64]

The category scheme, as proposed, completely ignores the differences in surveillance capabilities of drones,[65] which should be a critical factor in deciding which drones may operate where and under what terms. Direct physical contact is only one facet of the larger spectrum of harms caused by drones.

EPIC agrees the final rule should expressly prohibit flying drones over people in moving vehicles.[66]

---

[61] 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, 6-7 (Nov. 12, 2015), available at https://epic.org/apa/comments/EPIC-FAA-Drone-Reg-Comments.pdf, stating "Paparazzi, private detectives, commercial entities, stalkers, and criminals can all use drones to collect sensitive personal data. There have already been cases where private individuals discover drones with cameras deployed outside their homes and windows, even those far above ground level. Others have found drones hovering over them outside to capture images of their private activities. There have also been reports from people concerned they are being sexually harassed by drone operators. These cases are likely to increase dramatically if privacy rules are not established."

[62] Allison Branley and Rebecca Armitage, *Perpetrators using drones to stalk victims in new age of technology fuelled harassment*, ABC News (Sept. 30, 2018), https://www.abc.net.au/news/2018-10-01/drones-used-to-stalk-women-in-new-age-of-harassment/10297906 (describing a woman being stalked by her ex-husband via drone, "Kim is one of many victims being stalked and harassed using a new generation of technology… She lives in fear, in a virtual prison, to keep her children safe.");

[63] Hannah Boland, *Police say drones being used to vandalise homes and stalk victims, as reports of incidents surge*, Telegraph (Feb. 23, 2019), https://www.telegraph.co.uk/technology/2019/02/23/police-say-drones-used-vandalise-homes-stalk-victims-reports/ (noting an increase in drone incidents in UK police reports of 40% from 1,700 in 2016 to 2,400 in 2018, and "[t]hey included cases where drones were linked to stalking and harassment, as well as to hate crimes.").

[64] David Mercer, *Revealed: Drones used for stalking and filming cash machines in the UK*, SkyNews (Feb. 23, 2019), https://news.sky.com/story/police-warn-drone-users-after-incidents-soar-by-40-in-two-years-11637695, ("Gwent Police said a person had complained in 2018 that a drone was used to film them while they were naked. The force also received reports of a drone filming a cash machine[.]").

[65] Only the section discussing modifications that could result in a change of to disqualify a drone from a particular category addresses camera or other payloads not previously approved. 84 Fed. Reg. 3860. Nonetheless, the proposed rule later clarifies that this is only an issue if the weight changes with the replacement of the camera. 84 Fed. Reg. 3885.

[66] 84 Fed. Reg. 3860.

b. Drones operating at night must also be required to register and broadcast identifying information and surveillance capabilities.

The proposed rule allows for night operations without a permit but requires anti-collision lighting. 84 F.R. 3856, 3868. EPIC agrees anti-collision lighting is essential for night-time operations, when visibility is much lower without lighting. The proposed rule asks whether position lighting should be required for flying at night. EPIC argues it should be. Position/navigation lights, required for manned aircraft and marine vessels, are important to drone safety and improve detection as well. Anti-collision lights help make a drone visible to other aircraft, but position/navigation lights convey more information, such as position and direction of motion.[67] This is important to collision-avoidance, and also does a better job of indicating to others when a drone is nearby or overhead.

Still, position and anti-collision lighting does not do enough. Remote, broadcast ID is essential, especially at night when visibility is lower. EPIC disagrees with allowing night operations without any anti-collision or position-lighting, pursuant to the proposed waiver requirements. The proposed rule simply requires, "applicants to establish that operating at night without an anti-collision light (or with a light that is visible at a distance of less than 3 statute miles) would not reduce the level of safety of the operation." 84 F.R. 3869.

The waiver process must take into account where the remote pilot will fly, who will be in that area, and what surveillance capabilities the drone has. Lighting for drones does more than just avoid collisions with other aircraft, it serves as some notice (though not sufficient notice) that there is a drone nearby. Given that broadcast ID is still not required, drones must not be allowed to operate at night, without proper lighting. Otherwise, the night is primetime for drone harassment and criminal activity, as drones will be nearly impossible to spot. Even with

[67] *Navigation light*, Merriam-Webster, https://www.merriam-webster.com/dictionary/navigation%20light.

broadcast ID, lights should be required to put individuals on notice who do not have an app to track drones or have not checked the app yet.

c. Requiring drone operators to present credentials to law enforcement does not provide enough accountability, broadcast ID is necessary.

"The FAA proposes amending § 107.7 to require remote pilots to present their remote pilot in command certificates to the Administrator, authorized representatives of the National Transportation Safety Board (NTSB) or Transportation Security Administration (TSA), or any Federal, State, or local law enforcement officer, upon request from any such officials." 84 F.R. 3891.

EPIC agrees that there must be accountability for drone operators, but this does not go far enough. Broadcast ID does a much better job of addressing this problem—any person who is being bothered or harassed may determine who the drone belongs to, where it is, and report it accordingly. As drone technology advances, drone operators can be difficult and sometimes impossible to track down. Many hobby drones can be operated with a cellphone or fly autonomously.[68] Without a tell-tale remote control, how would a person recognize a pilot from another bystander, especially when the operator is intentionally trying to hide his or her identity? Further, as drone range gets longer, and long-range drones get cheaper, finding operators is increasingly difficult. Drones with up to 800-meter-range are available for less than $300, and more expensive drones can operate up to 7000 meters away.[69]

[68] *How to Buy a Drone in 2018: Buying Guide*, CNET, https://www.cnet.com/topics/drones/buying-guide/ (lists several drones controlled by smartphone) (last accessed Mar. 21, 2019); Hover, *Hover Camera Passport*, https://gethover.com/hover-camera-passport (advertises "Truly Autonomy Flight") (last accessed Mar. 21, 2019).
[69] Douglas James, *18 Drones with the Longest Control Range [Sorted in 3 Categories], DronesGlobe* (Dec. 4, 2017), http://www.dronesglobe.com/guide/long-range-drones/; *UPair One Plus 2.7K Drone Mobile APP Version RC Quadcopter Remote Helicopter with Follow Me Mode Aerial UAV*, Amazon, https://www.amazon.com/Monitor-Quadcopter-Function-Photography-Beginner/dp/B06Y2XLH4D/ref=as_li_ss_tl (drone with 800 meter range listed at $295.99 on Mar. 21, 2019).

EPIC also acknowledges that while drones do not have a reasonable expectation of privacy, their operators do. To that end, EPIC insists on proper safeguards for the information contained in the drone registry.[70]

Conclusion

Since 2012, the FAA has shirked its responsibility to produce meaningful privacy regulation for aerial drones. Over this period, the surveillance capabilities of drones have increased, as have reports of misuse as well as public concern. The FAA is already under intense scrutiny for its failure to effectively safeguard the public interest.[71]

Before drones are allowed to operate over people or at night, it is essential that the FAA regulations ensure that drones broadcast location, course, purpose, operator identifying and contact information, and any surveillance capabilities at all times.

Respectfully submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Jeramie D. Scott
Jeramie D. Scott
EPIC Senior Counsel

/s/ Ellen Coogan
Ellen Coogan
EPIC Domestic Surveillance Fellow

---

[70] 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, 12-16 (Nov. 12, 2015), available at https://epic.org/apa/comments/EPIC-FAA-Drone-Reg-Comments.pdf, stating "The FAA should restrict the release and use of the personal information it collects from hobbyist drone registrants[,]" and "The FAA should explicitly limit and focus its collection of registrants' data."

[71] *See, e.g.,* Jack Nicas, David Gelles and James Glanz, *Changes to Flight Software on 737 Max Escaped F.A.A. Scrutiny*, N.Y. Times, Apr. 11, 2019, at A1 https://www.nytimes.com/2019/04/11/business/boeing-faa-mcas.html