epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

U.S. DEPARTMENT OF TRANSPORTATION,
FEDERAL AVIATION ADMINISTRATION

Clarification of the Applicability of Aircraft Registration Requirements for Unmanned Aircraft Systems (UAS) and Request for Information Regarding Electronic Registration for UAS

[Docket No. FAA-2015-4378]
November 12, 2015

By notice published on October 22, 2015, the Federal Aviation Administration ("FAA") solicited public comments on options for a "streamlined, electronic-based registration system" for drones.[1] The Department of Transportation ("DOT") has convened a drone task force to draft recommendations for the drone registry.[2] The FAA solicited public comments to help inform the task force recommendations.[3]

[1] Clarification of the Applicability of Aircraft Registration Requirements for Unmanned Aircraft Systems (UAS) and Request for Information Regarding Electronic Registration for UAS, 80 Fed. Reg. 63,912, 63,914.
[2] Fed. Aviation Admin., *Huerta Announces UAS Registration Task Force Members* (Oct. 29, 2015, 9:54 AM), https://www.faa.gov/news/updates/?newsId=84125.
[3] EPIC notes that that none of the twenty-five drone task force members are experts in privacy nor represent the privacy interests of Americans who will be subject to increased surveillance by drones.

Accordingly, the Electronic Privacy Information Center ("EPIC") submits these comments to the FAA regarding drone registration. In summary, (1) EPIC supports the drone registration requirement; (2) EPIC recommends that drone registration information should be broadcast while drones are operating; (3) EPIC recommends drone registration requirements that detail each drone's capabilities for surveillance, including data collection and data storage; (4) EPIC does not support exemption for any drone that transits in the national airspace system; and (5) EPIC recommends limits on the use and disclosure of personal information obtained for drone registration.

I. EPIC's Interests

EPIC is a non-profit research and educational organization established in 1994 to focus public attention on emerging human rights issues, and to defend privacy, freedom of expression, and democratic values.[4] The EPIC Advisory Board is comprised of experts in law, technology and public policy.[5] EPIC has led the charge for strong drone privacy rules in the United States.[6] EPIC provides authoritative reports on drone privacy and security.[7]

EPIC has repeatedly warned the FAA of the privacy and civil liberties risks posed by the deployment of drones in the United States. In 2012, EPIC, joined by more than one hundred experts and organizations, petitioned the FAA to undertake a rulemaking to

[4] *About EPIC*, https://epic.org/epic/about.html (2015).
[5] *EPIC Advisory Board*, https://epic.org/epic/advisory_board.html(2015). *See, e.g.,* Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN.L.REV. ONLINE 29 (2011).
[6] EPIC, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones* (2015), https://epic.org/privacy/drones/; EPIC, *EPIC v. Army – Surveillance Blimps* (2015), https://epic.org/foia/army/; EPIC, *Spotlight on Surveillance –DRONES: Eyes in the Sky* (2014), https://epic.org/privacy/surveillance/spotlight/1014/drone.html; EPIC, *Spotlight on Surveillance – Unmanned Planes Offer Opportunities for Clandestine Government Tracking* (2005), https://epic.org/privacy/surveillance/spotlight/0805.
[7] *Id*.

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.[8] Earlier this year, EPIC sued the FAA for denying EPIC's petition, and the matter is currently before the U.S. Court of Appeals for the District of Columbia Circuit.[9] In addition to the 2012 Petition, in 2013 EPIC provided extensive comments to the Agency, urging the FAA to establish privacy standards for drone operators at FAA designated drone test sites.[10]

EPIC has also testified before Congress regarding the need to adopt comprehensive legislation to limit drone surveillance in the United States. EPIC has informed Congress and state legislatures of the unique threats drones pose to personal privacy, the inadequacy of the current privacy safeguards, and the importance of addressing privacy and civil liberties risks prior to the integration of drones into the NAS.[11]

Although the FAA has, in violation of law, failed to establish any rules to safeguard the privacy interests of the American public, EPIC wishes to make clear at the

---

[8] Letter 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 [hereinafter *EPIC 2012 Petition*].

[9] *EPIC v. FAA*, No. 15-1075 (D.C. Cir. filed Mar. 31, 2015). The D.C. Circuit has ruled against the agency's motion to dismiss.

[10] *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 (2013), *available at* https://epic.org/privacy/drones/EPIC-Drones-Comments-2013.pdf.

[11] *See, e.g.*, *Crimes – Unmanned Aircraft Systems – Unauthorized Surveillance, Hearing on H.D. 620 Before the H. Jud. Comm. of the General Assembly of Maryland* (2015) (statement of Jeramie D. Scott, National Security Counsel, EPIC); *The Future of Drones in America: Law Enforcement and Privacy Considerations Hearing Before the S. Judiciary Comm.*, 113th (2013) (statement of Amie Stepanovich, Director of the Domestic Surveillance Project, EPIC), *available at* https://epic.org/privacy/testimony/EPIC-Drone-Testimony-3-13-Stepanovich.pdf.

outset that we support the agency's effort to establish registration requirements for the operation of drones in the United States. EPIC believes this is an absolutely essential requirement to establish accountability for the use of autonomous surveillance devices in the United States.

II. Scope of the Drone Registration Registry

The Transportation Department currently requires commercial drone operators and drone test site operators to register their drones. To date, the Department has not required hobbyist drone operators to register. But to "create a culture of accountability and responsibility among all [drone] operators," the Department has now determined that "registration of all [drones] is necessary to enforce personal accountability while operating an aircraft."[12]

The proposed drone registry will help identify drone operators that operate drones in impermissible ways and aid the Department in taking enforcement actions against drone violations.[13] In the current proceeding, the Department requests information on the best methods to establish an electronic drone registry, drone registry data collection, and unique drone identifiers, among other registry considerations. 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] 80 Fed. Reg. 63,913.
[13] *Id*. at 63,914.

similar to the Automated Identification System ("AIS") for commercial vessels.[14] Any drone carrying video surveillance technology would be required to make clear at registration the specific capabilities, including resolution, frame rate, and zoom range. Any drone carrying audio surveillance technologies would be required to make clear at registration specific capabilities to capture and record audio communications or broadcast. Any drone carrying technology to engage in interception of signal communication, human recognition at a distance, or other advanced surveillance techniques, would be required at the time of registration to detail the capabilities and the anticipated use.

Any change in the functional capability of a drone through the adoption of new capabilities or the deployment of a payload that is different from that stated at the time of the initial registration would require change in the registration information prior to use.

And while drones have no expectation of privacy, hobbyist operators do. Accordingly, the FAA should implement privacy safeguards to protect hobbyist personal information collected for the registry. The FAA should incorporate EPIC's drone registry recommendations below.

III. Drones greatly expand existing privacy threats and create new methods of invading privacy.

Drones are capable of conducting persistent surveillance at a distance, collecting a

[14] *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.

great deal of detailed and sensitive personal data.[15] As EPIC explained in its 2012 Petition, "[w]ith special capabilities and enhanced equipment, drones are able to conduct far more detailed surveillance, obtaining high resolution picture and video, peering inside high level windows, and through solid barriers, such as fences, trees, and even walls."[16] Drones can also frequently operate without detection due to their size and design.[17]

The enhanced surveillance capabilities drones enable raise significant Fourth Amendment implications,[18] but the privacy threats are not limited to government use. Paparazzi, private detectives, commercial entities, stalkers, and criminals can all use drones to collect sensitive personal data.[19] There have already been cases where private individuals discover drones with cameras deployed outside their homes and windows, even those far above ground level.[20] Others have found drones hovering over them

---

[15] See Noel McKeegan, *Raven UAV Demonstrates 30-hour Persistent Surveillance,* GizMag (Apr. 2, 2009) http://www.gizmag.com/raven-uav-demonstrates-30-hour-persistent-surveillance/11385/; *See also U.S. Army Unveils 1.8 Gigapixel Camera Helicopter Drone*, BBC News Technology (Mar. 8, 2012), http://www.bbc.com/news/technology-16358851 (describing the ability to track individuals over 65 square miles from an altitude of 20,000 feet using high resolution cameras).

[16] *EPIC 2012 Petition* at 4.

[17] Jennifer Lynch, *Are Drones Watching You*, Electronic Frontier Foundation (Jan. 10, 2012), https://www.eff.org/deeplinks/2012/01/drones-are-watching-you.

[18] Congressional Research Service, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses* (Sept. 6, 2012) http://www.fas.org/sgp/crs/natsec/R42701.pdf

[19] A. Michael Froomkin & Zak Colangelo, *Self-defense Against Robots* 32 (2014), available at http://works.bepress.com/amichael_froomkin/2.

[20] *See, e.g.,* Michael Marois, Bloomberg News, *Creeps Embrace a New Tool: Peeping Drones* (May 5, 2015 5:00am) http://www.bloomberg.com/news/articles/2015-05-05/creeps-embrace-a-new-tool-peeping-drones; Laura Sydell, NPR, *As Drones Fly In Cities And Yards, So Do The Complaints* (May 12, 2014) http://www.npr.org/sections/alltechconsidered/2014/05/12/311154242/as-drones-fly-in-cities-and-yards-so-do-the-complaints; Capitol Hill Seattle Blog, *CHS X-Files: Capitol Hill Drone Pilot Spotted, Glowing Orbs, Phone Thief on Wheels* (May 8, 2013) http://www.capitolhillseattle.com/2013/05/chs-x-files-capitol-hill-drone-pilot-spotted-glowing-orbs-phone-thief-on-wheels/.

outside to capture images of their private activities.[21] There have also been reports from people concerned they are being sexually harassed by drone operators.[22] These cases are likely to increase dramatically if privacy rules are not established.[23]

The privacy threats are not limited to illegal and criminal conduct, many companies are moving towards using drones to collect data on individuals in public space. One marketing firm has already tested using drones to collect cellphone location data for location-based advertising.[24] This bulk collection of individuals' location data poses privacy threats, including tracking consumers' movements, and also safety threats.

States Have Enacted Legislation in Response to Drive Privacy Threats

So far the FAA has not established drone privacy protections, but states have stepped into the void to provide some protections. At least twenty states[25] have passed laws that protect citizens' privacy by restricting and regulating the use of drones, seven of

---

[21] *See* California State Legislature, Assembly Committee on Privacy and Consumer Protection, Hearing on AB 856 (May 5, 2015), p.2. ("Paparazzi…have used drones for years to invade the privacy and capture images of public persons in their most private of activities.") https://leginfo.legislature.ca.gov/faces/billAnalysisClient.xhtml?bill_id=201520160AB856.

[22] *See, e.g.,* Julie Balise, The Technology Chronicle, *Woman Claims Drone Harassed Her at Virginia Beach* (May 16, 2014, 4:23pm) http://blog.sfgate.com/techchron/2014/05/16/woman-claims-drone-harassed-her-at-virginia-beach/.

[23] Congressional Research Service, *Integration of Drones into Domestic Airspace: Selected Legal Issues* (Apr. 4, 2013) http://www.fas.org/sgp/crs/natsec/R42940.pdf.

[24] Kelsey D. Atherton, *Marketing Drones Scanned Los Angeles for Cellphone Location Data*, Popular Science (Feb. 26, 2015), http://www.popsci.com/marketing-drones-scanned-la-cellphone-location-data.

[25] Bills passed in Alaska, HB 255 (2014); Arkansas, HB 1349 (2015) and HB 1770 (2015); California, AB 856 (2015); Florida, SB 92 (2013); Idaho, SB 1134 (2013); Illinois, SB 1587 (2013) and SB 2937 (2014); Indiana, HB 1009 (2014); Iowa, HF 2289 (2014); Louisiana, HB 1029 (2014); Maine, LD 25 (2015); Mississippi, SB 2022 (2015); Montana, SB 196 (2013); North Carolina, SB 744 (2014); North Dakota, HB 1328 (2015); Oregon, HB 2710 A (2013); Tennessee, SB 1777 (2014) and SB 1892 (2014); Texas, HB 912 (2013) and HB 2167 (2015); Utah, SB 167 (2014) and HB 296 (2015); Virginia, HB 2012 (2013) and SB 1331 (2013); and Wisconsin SB 196 (2014) all contain one or more provisions limiting the use of drones in ways that protect privacy.

which include criminal sanctions for invasions of privacy stemming from drone use.[26] Some of these laws are designed to expand existing crimes such as "peeping Tom" statutes to include drone use,[27] while other states have created new crimes specifically related to the use of drones.[28]

At least eight states have created private rights of action for individuals who have had their privacy violated by unlawful drone use.[29] These rights enable individuals to sue law enforcement agencies and private entities that have, for example, used their images unlawfully,[30] conducted surveillance of property without appropriate permissions,[31] flown a drone over private property,[32] or otherwise invaded privacy.[33]

In enacting these drone privacy laws, states have articulated the privacy risks drones pose. The Florida legislature explained, "[t]he prospect of constant monitoring, whether performed by a government entity or some private entity (perhaps a potential employer, insurance company, private detective, etc.), may have a chilling effect on associational and expressive freedoms enjoyed by the American populace."[34] Similarly in Oregon, the drone bill's sponsor stated, "[a]s drones become more ubiquitous in the future, we will need to ensure that our legal protections keep pace with the use of this

[26] Arkansas, California, Mississippi, Oregon, Tennessee, Texas, and Wisconsin.
[27] *See, e.g.,* Mississippi, SB 2022 (2015).
[28] *See, e.g.,* Wisconsin SB 196 (2014).
[29] Arkansas, California, Florida, Idaho, North Carolina, Oregon, Tennessee, Texas.
[30] *See, e.g.,* North Carolina, SB 744 (2014).
[31] *See, e.g.,* Arkansas, HB 1349 (2015).
[32] *See, e.g.,* Oregon, HB 2710 A (2013).
[33] *See, e.g.,* Idaho, SB 1134 (2013).
[34] Florida Senate, *Bill Analysis and Fiscal Statement, SB* 766 (Apr. 13, 2015), http://www.flsenate.gov/Session/Bill/2015/0766/Analyses/2015s0766.ap.PDF.

technology."[35] Other state legislatures have also expressed concerns about the privacy threats posed by drones.[36]

While the states have appropriately identified privacy as a core issue associated with drone use, their focus is narrow and many individuals are still left without appropriate protections. Nationwide drone registration is an essential requirement to ensure the effective enforcement of state laws. To ensure that the drone registry fosters "accountability and responsibility"[37] among drone operators, the drone registry must include provisions addressing privacy issues to ensure a comprehensive baseline set of protections that facilitate the safe integration of drones.

IV. Robust registration requirements are necessary to address the safety and privacy implications of drone deployment in the United States.

The FAA's drone registration proposal provides an opportunity for the agency to increase the safety and better protect the privacy of the public. The agency must implement a robust registration requirement that fully considers the safety and privacy risks of drones in the national airspace.

A. Drone registration information should be broadcast by drones while in operation.

The current drone registration framework the FAA is considering does not go far enough in many respects.[38] As the Washington Post Editorial Board recently commented,

---

[35] Lauren Gambino, KATU, *Ore. Senate passes Bill Regulating Police Drones* (Jun. 11, 2013, 6:47am), http://www.katu.com/politics/Ore-Senate-passes-bill-regulating-police-drones-210949811.html.

[36] *See, e.g.,* Alaska State House of Representatives, *Sponsor Statement: HB 255* (Mar. 11, 2014, 4:47pm), http://www.housemajority.org/2014/03/11/sponsor-statement-hb-255-2/ (describing privacy as "the number one topic of concern" related to drones).

[37] 80 Fed. Reg. 63,913.

[38] Editorial Board, *The Government's Plan to Register Drones Does Not Go Far Enough*, The Washington Post (Oct. 26, 2015), https://www.washingtonpost.com/opinions/the-governments-

> Yet this is just the bare minimum the government should be doing, and it has taken far too long to get even here. Drones should be required to carry transponders that are difficult to deactivate so that they can be seen as they enter restricted airspace and so that investigators can easily identify owners.[39]

The FAA is proposing that drone operators be required to register their drones so each drone can be associated with its owner. The FAA states that registration will "help make sure that operators know the rules and remain accountable to the public for flying their unmanned aircraft responsibly."[40]

Currently, one of the problems with holding drone operators accountable is that it is difficult to identify the drone or the operator of a drone. The registration scheme, as currently envisioned, does little to solve this problem. If drone identification simply requires the display of a small registration code, then the only drones that will be identifiable are those that are recovered after a crash. Moreover, the current registration plan does nothing to inform the public of the surveillance capabilities of the drone, which is also necessary to make drone operators accountable to the public.

The shortcomings of the registration plan could encourage dangerous self-help remedies such as shooting down drones by those who see no other recourse against a drone that trespasses on private property, poses a physical threat, or engages in tracking

---

plan-to-register-recreational-drones-doesnt-go-far-enough/2015/10/26/bd21aac8-79c5-11e5-a958-d889faf561dc_story.html; Gail Collins, *Dreading Those Drones*, N.Y. Times (Oct. 30, 2015), http://www.nytimes.com/2015/10/31/opinion/dreading-those-drones.html.

[39] The Washington Post Editorial Board, *supra* note 38.

[40] U.S. Department of Transportation, *U.S. Transportation Secretary Anthony Foxx Announces Unmanned Aircraft Registration Requirement* (Oct. 19, 2015) https://www.transportation.gov/briefing-room/us-transportation-secretary-anthony-foxx-announces-unmanned-aircraft-registration.

and surveillance that is tortious and unlawful.[41] 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.

B. The FAA should implement a drone registration requirement that provides transparency around each drone's capabilities, data collection, and data storage.

Drone registration should include not only the identity of the operator, but also a description of the technical and surveillance capabilities of the drone, including the collection and storage capabilities. As with the drone registration number, drones should broadcast their 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.[42] Drones can also be equipped to enable facial recognition, scan license plates, and identify nearby cell phones and other mobile devices.[43] 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.

---

[41] *See* Jacob Gersham, *Judge Dismisses Case Against "Drone Slayer" Who Shot Down Drone From Back Porch*, WSJ (Oct. 28, 2015), http://blogs.wsj.com/law/2015/10/28/judge-dismisses-case-against-drone-slayer-who-shot-down-drone-from-back-porch/.
[42] Richard M. Thompson II, Cong. Research Serv., R43965, *Domestic Drones and Privacy: A Primer 3* (2015).
[43] *Id.*

C. The FAA should establish registration requirement for all drones.

The size of the drone is not strictly indicative of the privacy risks posed by the drone. In fact, smaller drones can more easily conduct surreptitious surveillance on unsuspecting individuals. As the surveillance technology improves and becomes more compact, micro drones will pose even greater threats to privacy.

The FAA should impose the registration requirement on all drones with the capability to collect images, audio, or transmissions, in public spaces. This rule, for example, would require all drones capable of recording individuals in public to register. Similarly, drones that do not have video recording capabilities but that are capable of monitoring nearby mobile devices would also have to register. The drone registration database of commercial operators should be publicly accessible, but the database of hobbyist drone operators should only be accessible for limited purposes related to protecting the safety and privacy of the public.

V. The FAA must implement privacy protections for hobbyist registrants.

The FAA's proposal to extend the current Aircraft Registration System to include recreational drone owners poses serious privacy risks that must be addressed prior to implementation. The FAA should adopt safeguards to protect registrants' information from improper release and use by both the public and other government agencies. Furthermore, the FAA should limit the information collected from drone registrants.

A. The FAA should restrict the release and use of the personal information it collects from hobbyist drone registrants.

Currently, the FAA requires all applicants to provide, at minimum, their aircraft model information, full legal name, physical address, and legal documents such as proof

of ownership and lien and collateral documents.[44] The FAA makes these registration records available and searchable by the public.[45] Releasing individual registrants' personal information to the public impacts the registrants' right to privacy. Drone registration information should be treated the same as the driver records collected by state departments of motor vehicles.

In the past, the personal information of registered drivers in many states was easily accessible at the local Department of Motor Vehicles ("DMV"): anyone could request and obtain the information for a small fee by presenting a license plate number.[46] As a result of this lax privacy protection, individuals were subject to threats of stalking, kidnapping, and violence.[47] Congress addressed this issue by establishing safeguards in the Driver's Privacy Protection Act ("DPPA"), which generally prohibits the release and use of registered drivers' personal information except for limited purposes.[48] Given the fast-growing market for drones,[49] a publicly accessible database of operators would implicate privacy and safety concerns comparable to those that inspired the DPPA.

Privacy concerns are greater for hobbyists than for commercial operators. Unlike commercial operators, hobbyists are more likely to register their drone with private home

---

[44] *See* 14 C.F.R. § 47.31 (2010); AC Form 8050-1.
[45] Privacy Act of 1974: Systems of Records, 65 Fed. Reg. 79, 19476, 19518 (Apr. 11, 2000). Members of the public can search the registry database online, at http://registry.faa.gov/aircraftinquiry/.
[46] 140 Cong. Rec. H2522 (daily ed. Apr. 20, 1994) (statement of Rep. Moran).
[47] 139 Cong. Rec. S15,761 (daily ed. Nov. 16, 1993) (statement of Sen. Boxer, a sponsor of the Act).
[48] 18 U.S.C. § 2721(a).
[49] The Consumer Electronics Association projects 2015 sales to approach 700,000 units. *New Tech to Drive CE Industry Growth in 2015, Projects CEA's Midyear Sales and Forecasts Report*, The Consumer Electronics Association (July 15, 2015) https://www.ce.org/News/News-Releases/Press-Releases/2015-Press-Releases/New-Tech-to-Drive-CE-Industry-Growth-in-2015,-Proj.aspx.

addresses, implicating the same concerns that drivers face when registering with the DMV. Also, many hobbyist drones are being marketed to children. So, for example, someone who has identified a drone flown by a minor could easily search the FAA database for the physical address linked to that child.

The Supreme Court has recognized a legitimate privacy interest in avoiding the disclosure of an individual's name, address, and telephone number.[50] This interest remains intact even when the information is properly disclosed to the public under certain circumstances.[51] "[A] state intrusion is impermissible if it 'bears no direct relation to the constitutional justification for the intrusion.'"[52] Furthermore, limiting the use and disclosure of personal information submitted by aircraft registrants or vehicle licensees is consistent with their expectation of privacy.[53] It would not serve any legitimate purpose to make users' personal information available beyond the scope of a particular privacy or security threat. Therefore it is necessary to establish safeguards to protect the privacy of drone registrants.

The FAA should adopt, similar to the DPPA, a general prohibition against the disclosure of "personal information," including the name, address, and phone number of the registrant.[54] Permitted uses of the registry should be limited to serve the FAA's stated purposes of allowing "individuals and title search companies to determine the legal ownership of an aircraft" and to "provide aircraft owners and operators information about

[50] *Dep't of Defense v. Fed. Labor Relations Auth.,* 510 U.S. 487, 500 (1994).
[51] *Id.*; *Reporters Committee, U.S. Dep't of Justice v. Reporters Comm. For Freedom of Press*, 489 U.S. 749, 767, 770 (1989).
[52] Brief for EPIC as Amicus Curiae Supporting Petitioners at 4, *Reno v. Condon*, 528 U.S. 141 (2000) (No. 98-1464), https://epic.org/privacy/drivers/epic_dppa_brief.pdf (quoting *Wilson v. Layne*, 526 U.S. 603, 613 (1999)).
[53] *Id.* at 4, 7-8.
[54] *See* 18 U.S.C. § 2725(3).

potential mechanical defects or unsafe conditions of their aircraft in the form of airworthiness directives."[55]

The permitted uses of registry data should be narrowly defined to suit these purposes. For example, the FAA could provide drone registration information with consent from the operator.[56] Where consent has not been obtained, the FAA could provide information to identify the operator of a drone that has caused injury, or in connection with a legal proceeding.[57] But not all information collected by the FAA would need to be subject to these privacy protections. For example, the DPPA excludes "information on vehicular accidents, driving violations, and driver's status" from the definition of "personal information."[58] Similarly, the FAA could properly provide drone owners and operators information on their model's mechanical defects or aircraft conditions, while protecting individual registrants' personally identifiable information.

Government access to the registration records should also be limited and transparent. The FAA's proposal states that drone registration information "may assist the FAA and law enforcement agencies to respond to inappropriate behavior, to share safety information, respond to emergency situations, and populate data fields for studies that track trends and help shape future management decisions."[59] These broadly stated purposes should be clarified and access should be limited to circumstances directly related to aircraft identification and operation. Drone owners, especially hobbyist owners,

---

[55] Privacy Act of 1974: Systems of Records, *supra* note 44 at 19,518.
[56] *See* 18 U.S.C. § 2721(b)(13).
[57] *See id*. § 2721(b)(4).
[58] 18 U.S.C. § 2725 (3).
[59] Operation and Certification of Small Unmanned Aircraft Systems; Proposed Rule, 80 Fed. Reg. 9544, 9574 (proposed Feb. 23, 2015) (to be codified at 14 CFR Pts. 21, 43, 45, 47, 61, 91, 101, 107, 183).

should not have their personal information subject to indiscriminate access by law enforcement and government agencies for purposes unrelated to aircraft safety.

The FAA might also consider collecting aggregate data to assist research into drone flights and usage, but research data should *not* include personal information. There must be strict restrictions against the general disclosure of registrants' personal information to government agencies and private entities, except as necessary to promote the FAA's mission of establishing safety and privacy in drone operations.

B. The FAA should explicitly limit and focus its collection of registrants' data.

When collecting information from recreational drone registrants, the FAA should also limit the information it collects about individuals—only collecting what is strictly necessary and directly related to safe operations of drones and respect for individual privacy rights in the national airspace. The FAA should tailor the collection of registrant information to only what is necessary to maintain the Aircraft Registry. For example, the FAA should not collect "highly restricted personal information," including "an individual's photograph or image, social security number, medical or disability information."[60] Such information is unnecessary to the FAA's administration of its registry and maintenance of drone safety.

Conclusion

The FAA must move quickly to establish a nationwide drone registration system. As the agency has already acknowledged, the deployment of drones in the national airspace poses many safety and privacy risks. The agency must also ensure that the

[60] *See* 18 U.S.C. § 2725(4).

registration process requires operators to inform the public about the surveillance capabilities of the drones they use. Finally, the agency should establish safeguards for the drone registry to ensure a minimum privacy burden on hobbyist users.

Respectfully submitted,

Marc Rotenberg
EPIC President and Executive Director

Khaliah Barnes
EPIC Associate Director

Alan Butler
EPIC Senior Counsel

Caitriona Fitzgerald
EPIC State Policy Coordinator

Jeramie D. Scott
EPIC National Security Counsel

Sophia Jeewon Choi
EPIC Law Clerk

Katherine Kwong
EPIC Law Clerk