

April 9, 2019

The Honorable David Price, Chairman  
The Honorable Mario Diaz-Balart, Ranking Member  
U.S. House Committee on Appropriations  
Subcommittee on Transportation, and Housing and Urban Development, and Related Agencies  
H-307 The Capitol  
Washington, D.C. 20515

Dear Chairman Price and Ranking Member Diaz-Balart:

In advance of the upcoming budget hearing for the Department of Transportation,<sup>1</sup> we write to inform you of EPIC's ongoing work to establish transparency and oversight for the use of unmanned aircraft in the United States. The Federal Aviation Administration (FAA) must: 1) issue regulations on drone privacy, and 2) mandate the remote identification of drones.

EPIC is a public-interest research center established in 1994 to focus public attention on emerging privacy and civil liberties issues. EPIC has taken a particular interest in the unique privacy problems of Unmanned Aerial Vehicles (UAVs or "drones"), and has sued the FAA for its failure to establish privacy safeguards to protect Americans.<sup>2</sup> EPIC sued the FAA for the agency's failure to establish drone privacy safeguards.<sup>3</sup> EPIC has also filed suit to enforce the transparency obligations of the Drone Advisory Committee, a body created by the FAA to study and make recommendations on U.S. drone policy.<sup>4</sup>

EPIC has also pursued several open government matters regarding the FAA's decision making process, which appears intended to purposefully avoid the development of meaningful privacy safeguards.<sup>5</sup>

---

<sup>1</sup> *Department of Transportation Budget Request for Fiscal Year 2020*, 116<sup>th</sup> Cong. (2019), H. Comm. on Appropriations, Subcomm. on Trans., and Housing and Urban Development, and Related Agencies, <https://appropriations.house.gov/legislation/hearings/department-of-transportation-budget-request-for-fiscal-year-2020> (Apr. 10, 2019).

<sup>2</sup> *EPIC v. FAA*, No. 15-1075 (D.C. Cir. May 10, 2016); See also *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, EPIC, <https://epic.org/privacy/drones/>; See also EPIC, *EPIC v. FAA, Challenging the FAA's Failure to Establish Drone Privacy Rules*, <https://epic.org/privacy/litigation/apa/faa/drones/>

<sup>3</sup> *EPIC v. FAA*, <https://epic.org/privacy/litigation/apa/faa/drones/>.

<sup>4</sup> *EPIC v. Drone Advisory Committee*, <https://epic.org/privacy/litigation/faca/epic-v-drone-advisory-committee/>.

<sup>5</sup> *EPIC FOIA: Drone Industry Cozied Up to Public Officials* (Dec. 21, 2016), EPIC, <https://epic.org/2016/12/epic-foia-drone-industry-cozie.html>; *EPIC v. Department of Transportation - Drone Registration Task Force*, EPIC, <http://epic.org/foia/dot/drones/taskforce/>.

## *Aerial Drones: A Unique Privacy Threat*

Drones pose a unique threat to privacy. The technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology. Small, unmanned drones are already inexpensive; the surveillance capabilities of drones are rapidly advancing; and cheap storage is readily available to maintain repositories of surveillance data. A Pew Research Center survey found that a majority of Americans object to drones flying near private homes.<sup>6</sup> However, in recent years individual drone use has soared, and the FAA predicts that 7 million drones will be sold by 2020.<sup>7</sup> As drone use increases so do the risks to privacy and safety.

Drones are now regularly equipped with high definition cameras that increase the ability of a user to conduct domestic surveillance.<sup>8</sup> The DJI Inspire 2 is a high-end, commercially available hobbyist drone about the size of a small desktop printer and weighs less than eight pounds, yet it can transmit high definition video to an operator over four miles away and can live-stream that video.<sup>9</sup> Even lower-end hobbyist drones costing less than \$100 can stream live video. The Hubsan X4 H502E DESIRE, a drone that can fit in the palm of your hand, utilizes a front facing high definition camera with 720P resolution that can stream live video up to 200 meters away.<sup>10</sup> Drones can be used to view individuals inside their homes and can facilitate the harassment and stalking of unsuspecting victims.<sup>11</sup> Drones can also be modified with tools that can enable them to gather personal information using infrared cameras, heat sensors, GPS, automated license plate readers, and facial recognition devices.<sup>12</sup>

Drones also pose risks to security and cybersecurity. Close calls between drones and traditional aircraft have risen significantly as their use becomes more widespread.<sup>13</sup> Furthermore, the very features that make drones easy to operate also make them susceptible to cyberattacks.<sup>14</sup>

---

<sup>6</sup> 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/>.

<sup>7</sup> *FAA Aerospace Forecast: Fiscal Years 2016-2036*, FAA, 2016, [https://www.faa.gov/data\\_research/aviation/aerospace\\_forecasts/media/FY2016-36\\_FAA\\_Aerospace\\_Forecast.pdf](https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2016-36_FAA_Aerospace_Forecast.pdf).

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

<sup>9</sup> DJI, *Inspire 2*, <http://www.dji.com/inspire-2/info#specs>.

<sup>10</sup> Hubsan, *X4 H502E DESIRE*, <https://www.hubsanus.com/shop/h502e.html>.

<sup>11</sup> Petition for Rulemaking Submitted by EPIC, *supra* note 8.

<sup>12</sup> *Id.*; Ciara Bracken-Roche et al., Surveillance Studies Centre, *Surveillance Drones: Privacy Implications of the Spread of Unmanned Aerial Vehicles (UAVs) in Canada* 46, Apr. 30, 2014,

[http://www.sscqueens.org/sites/default/files/Surveillance\\_Drones\\_Report.pdf](http://www.sscqueens.org/sites/default/files/Surveillance_Drones_Report.pdf); Mary Papenfuss, *Utah Couple Arrested Over 'Peeping Tom' Drone*, Huffington Post, Feb. 17, 2017,

[http://www.huffingtonpost.com/entry/peeping-tom-drone\\_us\\_58a6847fe4b045cd34c03e56](http://www.huffingtonpost.com/entry/peeping-tom-drone_us_58a6847fe4b045cd34c03e56).

<sup>13</sup> Alan Levin, *Drone-Plane Near misses, Other Incidents Surge 46% in U.S.*, Bloomberg, Feb. 23, 2017, <https://www.bloomberg.com/news/articles/2017-02-23/drone-plane-near-misses-other-incidents-surged-46-in-u-s>; Steve Miletich, *Pilot of Drone That Struck Woman at Pride Parade Gets 30 Days in Jail*, The Seattle Times, Feb. 24, 2017, <http://www.seattletimes.com/seattle-news/crime/pilot-of-drone-that-struck-woman-at-pride-parade-sentenced-to-30-days-in-jail/>.

<sup>14</sup> Dom Galeon, *As Drones Become Tools of War, Companies Turn to Hacking Them*, Futurism (Feb. 20, 2018), <https://futurism.com/drone-hack-technology>; Kacey Deamer, *How Can Drones Be Hacked? Let Us*

Hackers have the ability to exploit weaknesses in drone software to take over operation of a drone and access the camera and microphones.<sup>15</sup>

The privacy risks of drones, as well as the safety and security vulnerabilities, underscore the need for the FAA to develop drone privacy regulations. *We urge the Committee to question why the FAA has not yet taken steps to issue regulations on drone privacy despite prior Congressional directives to do so.*

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

The FAA has failed to take the action mandated by Congress. The FAA Modernization Act required the FAA to create a Comprehensive Plan to integrate drones into the National Airspace and subsequently conduct a notice and comment rulemaking. In the Plan, the FAA identified privacy as an important issue to address, acknowledging that “as demand for [drones] increases, concerns regarding how [drones] will impact existing aviation grow stronger, especially in terms of safety, privacy, frequency crowding, and airspace congestion.”<sup>16</sup>

Under the FAA Modernization Act, Congress required the FAA to implement the recommendations of the Comprehensive Plan via a public rulemaking within 46 months of the enactment of the Act. The FAA identified privacy as an important issue directly related to domestic drones, yet the agency has failed to address privacy in the agency’s only public rulemaking on drones in the National Airspace.<sup>17</sup> Indeed it has been over 60 months and the FAA has failed to implement the rulemaking that addresses the issues identified in the Comprehensive Plan, including privacy, as required by Congress.<sup>18</sup>

#### *The FAA Has Failed to Conduct the Required Drone Privacy Report*

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

Without adequate safeguards, expanded use of UAS and their integration into the national airspace raise a host of concerns with respect to the privacy of individuals.

---

*Count the Ways*, Live Science, Jun. 10, 2016, <http://www.livescience.com/55046-how-can-drones-be-hacked.html>.

<sup>15</sup> Wang Wei, *You Can Hijack Nearly Any Drone Mid-Flight Using This Tiny Gadget*, The Hacker News, Oct. 27, 2016, <http://thehackernews.com/2016/10/how-to-hack-drone.html>.

<sup>16</sup> Joint Planning and Dev. Office, Fed. Aviation Admin., *Unmanned Aircraft Systems (UAS) Comprehensive Plan: A Report on the Nation’s UAS Path Forward* 4 (2013), [https://www.faa.gov/about/office\\_org/headquarters\\_offices/agi/reports/media/UAS\\_Comprehensive\\_Plan.pdf](https://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf).

<sup>17</sup> Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42,063 (June 28, 2016) (codified at 14 C.F.R. pts. 21, 43, 61, 91, 101, 107, 119, 133, and 183).

<sup>18</sup> FAA Modernization and Reform Act of 2012, Pub. L. 112-95 § 332, 126 Stat. 73-75.

For this reason, the FAA is directed to conduct a study on the implications of UAS integration into national airspace on individual privacy.<sup>19</sup>

The report specifically required the FAA to study “how the FAA can address the impact of widespread use of UAS on individual privacy as it prepares to facilitate the integration of UAS into the national airspace.”<sup>20</sup> The report was to be submitted to Congress within 18 months of enactment of that appropriations bill and completed “well in advance of the FAA's schedule for developing final regulations on the integration of UAS into the national airspace.”<sup>21</sup> Nearly 63 months since the bill was enacted, the FAA has failed to produce the report. Furthermore, EPIC obtained documents through a Freedom of Information Act request that suggested that the FAA has no intention of complying with Congress’ directive to produce a report.<sup>22</sup>

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

### *Remote Identification of Drones*

The Federal Aviation Administration recently published an interim final rule that will require a visible registration number on the exterior of drones.<sup>23</sup> Previously, registration numbers could be hidden inside drones. While EPIC agrees external marking are preferable to hidden identifiers, EPIC said the rule did not go far enough. In comments to the FAA, EPIC wrote, “Because drones present substantial privacy and safety risks, EPIC recommends that the FAA require any drone operating in the national airspace system to broadcast location when aloft (latitude, longitude, and altitude), course, speed over ground, as well as owner identifying information and contact information[.]”<sup>24</sup> EPIC also suggested the agency require operators register and broadcast surveillance capabilities.

Currently, individuals cannot hold drone operators accountable because it is essentially impossible to identify the drone or the operator of a drone. The modified registration scheme proposed by the FAA still does little to solve this problem. Solutions exist.<sup>25</sup> To increase accountability of drone operators, the FAA Reauthorization Act of 2018 requires the FAA to

---

<sup>19</sup> See Explanatory Statement, Consolidated Appropriations Act of 2014, H.R. 3547, 113th Cong., Division L at 6 (Jan. 14, 2014), <https://www.congress.gov/congressional-record/2014/01/15/house-section/article/H475-2>

<sup>20</sup> *Id.*

<sup>21</sup> *Id.*

<sup>22</sup> <https://epic.org/privacy/litigation/apa/faa/drones/EPIC-16-07-20-FAA-FOIA-20160921-Production.pdf>.

<sup>23</sup> *External Marking Requirement for Small Unmanned Aircraft*, 84 Fed. Reg. 3669-3673 (Feb. 13, 2019), <https://www.federalregister.gov/documents/2019/02/13/2019-00765/external-marking-requirement-for-small-unmanned-aircraft>.

<sup>24</sup> Comments of EPIC et al. to the Federal Aviation Admin., *External Marking Requirement for Small Unmanned Aircraft* (Mar. 15, 2019), <https://epic.org/apa/comments/EPIC-Coalition-Comments-FAA-Drone-ID-Mar2019.pdf>.

<sup>25</sup> See, e.g., Isabella Lee, *FAA Issues Request for Information (RFI) from Industry Partners Interested in Developing Remote ID and Unmanned Traffic Management (UTM) Systems* (Jan. 24, 2019)

<https://uavcoach.com/remote-id-faa-rfi/> (“Remote ID development and testing has already begun in the private and commercial sector.”).

consider and develop remote identification for drones.<sup>26</sup> As the FAA Aviation Rulemaking Committee Working Group 1 pointed out, “placing a sticker or FAA registration number on the UAS will not provide remote ID and tracking, as it would be nearly impossible to read a registration number on a UAS that is more than a few feet away.”<sup>27</sup> Passive identification does not go far enough—the FAA must require active remote identification. The FAA should mandate remote identification and ensure also that drones routinely broadcast course, location, and other relevant operational information. Drones should simply not continue to fly above the laws that protect public safety.

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

### *Conclusion*

We ask that this letter be entered in the hearing record. EPIC looks forward to working with the Committee on these issues of vital importance to the American public.

Sincerely,

*/s/ Marc Rotenberg*  
Marc Rotenberg  
EPIC President

*/s/ Jeramie Scott*  
Jeramie Scott  
EPIC Senior Counsel

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

---

<sup>26</sup> See Federal Aviation Administration Reauthorization Act of 2018, Pub. L. No. 115-254, § 376(b)(2), (c)(3)(A) 132 Stat. 3186, 3305–06 (2018) (directing the FAA to develop a plan for the implementation of unmanned aircraft systems traffic management (UTM) services that, *inter alia*, permit the testing of remote identification and that assess the risks raised and mitigation means required to remotely identify drones).

<sup>27</sup> Aviation Rulemaking Comm., Fed. Aviation Admin., ARC Recommendations Final Report: Appendix B Working Group 1 Report 42 (2017),

[https://www.faa.gov/regulations\\_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf](https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf)