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

Agency Information Collection Activities: Requests for Comments; Clearance of a Renewed Approval of Information Collection: B4UFLY Smartphone App

[Docket No. FAA-2019-0159; OMB Control Number: 2120-0764]

May 13, 2019

By notice published March 14, 2019, the Federal Aviation Administration ("FAA") renewed data collection using the smartphone app, B4UFLY.[1] B4UFLY "provides situational awareness of flight restrictions—including locations of airports, restricted airspace, special use airspace, and temporary flight restrictions—based on a user's current or planned flight location."[2] "The data collected will assist the FAA with determining the best processes to authorize recreational UAS pilots and inform air traffic control personnel of a UAS pilot's intended flight in order to assess whether the UAS may disrupt or endanger manned air traffic."[3]

EPIC submits these comments to the FAA to: (1) urge the establishment of a remote identification requirement that would broadcast location, course, purpose, and operator identifying and contact information; (2) encourage the agency to publish clear explanations of

[1] *Agency Information Collection Activities: Requests for Comments; Clearance of a Renewed Approval of Information Collection: B4UFLY Smartphone App*, 84 Fed. Reg. 9411-12 (Mar.14, 2019), https://www.govinfo.gov/content/pkg/FR-2019-03-14/pdf/2019-04696.pdf.
[2] 84 Fed. Reg. 9411.
[3] 84 Fed. Reg. 9411-12.

the categories of data collected, as well as how that data is protected, used, and disseminated; and (3) emphasize that hobbyist drone operator information collected by the app must be protected.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy issues.[4] For well over a decade, EPIC has maintained expertise on privacy, safety, and security concerns related to drones and has prominently advocated for better regulation of the national airspace related to these threats.[5] 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.[6]

EPIC has repeatedly urged the FAA to require that drone registration include disclosure of surveillance capabilities and also to provide real-time, remote identification of drones aloft.[7] 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."[8] EPIC also testified to legislative

[4] EPIC, *About EPIC* (2018), https://epic.org/epic/about.html.
[5] 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/.
[6] 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.
[7] 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.
[8] 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.

bodies on the "unique threat to privacy" posed by drones[9] because "[t]he technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology."[10]

EPIC has also specifically recommended that drones broadcast location, course, and purpose.[11] 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.[12]

Like passive registration, the B4UFLY app does nothing to address the privacy risks posed by drones. According to the FAA, the mobile app provides information on drone flight restrictions and allows the FAA to collect information the agency hopes will inform how to communicate to air traffic control drone flights. This is not enough. The FAA should require drones to broadcast their location, course, speed, and registration number, and the B4UFLY app should allow the public to quickly and easily determine this information about nearby drones.

---

[9] *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.

[10] 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).

[11] 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.

[12] *Id.* at 11.

I. The FAA must require drones to broadcast identification, location, course, and purpose.

EPIC agrees "a key way to help people safely fly unmanned aircraft is to provide situational awareness by letting them know where they should and should not fly and where there might be conflicts."[13] However, the B4UFLY app does not go far enough to make the airspace safe and address the privacy issues raised by drones. Furthermore, the B4UFLY app handles the issue of operator accountability in a roundabout way that completely depends on the operator to provide information to the FAA. Those who are least likely to comply with FAA regulations are most likely to ignore the B4UFLY app. The app also fails to inform air traffic controllers in real-time of drones near an airport that might pose a risk. Even if an air traffic controller were to visually spot a drone that posed a risk, there would be no way to hold that person accountable unless the drone operator was spotted and identified during the operation of the drone or the drone itself was captured. Importantly, the app fails to take advantage of one of the best ways to inform air traffic controllers and the public of nearby drones and hold drone operators accountable—requiring commercial drones to broadcast relevant location and course information, as occurs routinely with planes and vessels.

B4UFLY takes geolocation data from the operator's phone and displays a map based off that location data to allow the operator to plan a flight path that avoids restricted areas.[14] This tool may be useful to prevent drones from entering restricted airspace due to an operator's mistake, but it does nothing to hold drone operators accountable or inform air traffic controllers

[13] Fed. Aviation Admin., *B4UFLY General Questions & Answers*, https://www.faa.gov/uas/recreational_fliers/where_can_i_fly/b4ufly/media/UAS_B4UFLY_QandA.pdf.
[14] U.S. Dep't of Transp., *Privacy Impact Assessment for Federal Aviation Administration (FAA) Office of Information and Technology (AIT) B4UFLY*, 2-3 (Feb. 13, 2019), https://www.transportation.gov/sites/dot.gov/files/docs/resources/individuals/privacy/331276/privacy-faa-b4fufly-pia-approved-021319.pdf [hereinafter B4UFLY PIA].

in real-time of drone operating near their airport. A better system would require all drones to be outfitted with broadcast ID technology that can be recognized and charted by the B4UFLY app or similar app.

Similar apps exist today for vessels and planes. For example, a popular vessel tracking app for the iPhone and the Android is MarineTraffic, which provides "near real-time positions of ships and yachts worldwide."[15] And FlightTracker tracks flights "all over the world."[16] Both apps are widely available to the general public. For boat captains, inexpensive apps that provide real-time location information about the location, course, and identification of other vessels reduce the risk of collision and promote public safety.[17]

EPIC has repeatedly called for remote, broadcast ID for drone deployment in the United States.[18] 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 (i.e. drone registration number), similar to the Automated Identification System ("AIS") for commercial vessels.[19] The B4UFLY app could not only be a way to inform drone operators where they cannot fly but also be the tool in which the public and air traffic controllers

[15] Marine Traffic – Ship Tracking, Apple App Store Preview, Maltenoz Limited, https://itunes.apple.com/us/app/marinetraffic-ship-tracking/id563910324?mt=8

[16] The Flight Tracker, Apple App Store Preview, Flist Holding B.V., https://itunes.apple.com/us/app/the-flight-tracker/id533365777

[17] *See, e.g.*, Global Marine Insurance Agency, *AIS Improving Boating Safety*, (Nov. 1, 2018), https://www.globalmarineinsurance.com/ais-improving-boating-safety/

[18] 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), 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), https://epic.org/apa/comments/EPIC-Coalition-Comments-FAA-Drone-ID-Mar2019.pdf.

[19] *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.

can identify nearby drones and hold drone operators accountable for actions that undermine privacy or safety.

II. The FAA should clarify the data practices surrounding B4UFLY data collection.

The FAA should explain which categories of records are collected, how the data is used, how it is disclosed, how long it is retained, and what safeguards exist to protect the data and to ensure the data cannot be traced to specific drone operators if breached. To that end, the FAA should make public all privacy assessments or analysis conducted with respect to the B4UFLY program.

The currently available Privacy Impact Assessment ("PIA") for the B4UFLY app provides apparently conflicting explanations of what data is collected by the FAA. This sows confusion. At first, the PIA implies that there is no collection by the FAA of location information:

> Upon launching B4UFLY for the first time, Users are requested to permit the B4UFLY application to turn on their mobile device's geolocation capability for the purposes of populating the B4UFLY map with information specific to their location. The geolocation and Global Positioning System (GPS) information is stored locally on the User's devices and is not transmitted to the FAA. Users are not required to turn on their geolocation, but by not doing so; Users will not receive the most accurate flight information.[20]

Later in the assessment, however, the PIA plainly states, "Users must consent to the use of geolocation data for the purposes of populating the B4UFLY map with information specific to their location. *This geolocation data transmitted to FAA* is not associated with the individual who submits it."[21]

[20] B4UFLY PIA, *supra* note 14, 3.
[21] *Id.* at 4 (emphasis added).

A few sections after, the PIA states the only information maintained is "the number of downloads of the B4UFLY application."[22] The FAA should explain its data practices with regard to the B4UFLY application. This is especially important because nearly any click within the app grays out the screen and prompts a message saying, "Please turn on your GPS," and does not allow you to do anything else in the app besides click "OK."

The FAA should clarify the confusion and seemingly contradictory information provided by the PIA and publish all other related documents. The government should not collect information without clear explanations of what records are collected, how long they will be retained, how they will be used, to whom they will be disclosed, and what safeguards are in place.

To the extent personal information is collected, it should be protected. Operators of commercial drones should make known their identity when they operate a drone in the National Airspace. However, the personal data of drone hobbyists operating a drone on private land need not be disclosed to the public.[23] The FAA should adopt safeguards to protect B4UFLY hobbyist user information from improper release and use by both the public and other government agencies. Furthermore, the FAA should limit the information collected from B4UFLY app users.

[22] *Id.* at 5.
[23] Although EPIC supports drone registration and advocates for drones to broadcast certain information, EPIC has also urged the FAA to provide privacy protections for the personal information of hobbyist registrants. 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, 2016), https://epic.org/privacy/drones/EPIC-FAA-Drone-Reg-Comments.pdf.

Conclusion

While the B4UFLY app provides useful guidance to drone operators, it does nothing to promote accountability or protect the privacy or safety of bystanders. As such, the FAA should promulgate a rule requiring remote broadcast of identifying information, including the location, course, and purpose. Further, the FAA needs to clarify what data is collected by the agency through the app and the data practices that apply to the collection. Lastly, to the extent that the app does collect information about non-commercial operators, it should actively protect that information.

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