epic.org

ELECTRONIC PRIVACY INFORMATION CENTER

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

April 23, 2013

By notice published on February 22, 2013, the Federal Aviation Administration ("FAA") of the Department of Transportation ("DOT) has requested comments on unmanned aircraft systems ("UAS") test sites.[1] Pursuant to Congressional mandates under the FAA Modernization and Reform Act of 2012 ("FMRA") and the National Defense Authorization Act ("NDAA"), the FAA must "identify six test ranges/sites to integrate unmanned aircraft systems ("UAS") into the National Airspace Systems ("NAS")."[2] To carry out these Congressional mandates, the FAA has requested comments in order to "develop a body of data and operational experiences to inform the integration and the safe operation of [drones] in the National Airspace System."[3]

[1] Request for comments, Unmanned Aircraft System Test Sites, 78 Fed. Reg. 12259 (proposed Feb. 22, 2013), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-22/pdf/2013-03897.pdf [hereinafter "RFC/SIR"].
[2] FAA Modernization and Reform Act, Pub. L. 112-95 (2012) [hereinafter "FMRA"].
[3] RFC/SIR, *supra* n. 1 at 12259.

These comments are submitted by the Electronic Privacy Information Center ("EPIC"). EPIC is a public interest research center in Washington, D.C., established in 1994 to focus public attention on emerging civil liberties issues and to protect privacy, the First Amendment, and constitutional values. EPIC has a particular interest in preserving privacy safeguards against expansive surveillance systems.[4]

The use of drones implicates significant Fourth Amendment interests and well established common law privacy rights.[5] With special capabilities and enhanced equipment, drones are able to conduct detailed surveillance, obtaining high-resolution picture and video, peering inside high-level windows, and through solid barriers, such as fences, trees, and even walls.

In *U.S. v. Jones*, the Supreme Court upheld Fourth Amendment privacy rights implicated by pervasive government surveillance. In *Jones*, the Supreme Court held that attachment of a GPS tracking device to a vehicle, and subsequent use of the device to monitor the vehicle's movements along public streets, constituted a search within the

[4] *See, e.g.*, EPIC: Unmanned Aerial Vehicles (UAVs) and Drones, http://epic.org/privacy/drones/; EPIC: Video Surveillance, http://epic.org/privacy/surveillance/; EPIC Statement on CCTV, D.C. Council Bill 17-438 (Mar. 11, 2008), *available at* http://epic.org/privacy/surveillance/epic_dc17-438_031108.pdf; Comments of the Electronic Privacy Information Center on the Expansion of CCTV Pilot Program (June 29, 2006), *available at* http://epic.org/privacy/surveillance/cctvcom062906.pdf; Brief of *Amicus Curiae* Electronic Privacy Information Center (EPIC), *Federal Aviation Administration, et al., v. Stanmore Cawthon Cooper* (2011)(No. 10-1024), *available at* http://epic.org/amicus/cooper/Cooper-EPIC-Brief.pdf.

[5] Many state governments have enacted legislation to protect individuals from the type of persistent surveillance that drones would facilitate. Sometimes called "Peeping Tom" laws, each state prohibits the intrusion upon a person's seclusion. *See Elements of an Intrusion Claim, Citizen Media Law Project*, http://www.citmedialaw.org/legal-guide/elements-intrusion-claim (last visited Feb. 21, 2012). *See also, e.g.* Cal. Civ. Code § 1708.8 (West 2011); Neb. Rev. Stat. § 20-203 (2011). Unlike trespass laws, intrusion does not require a physical trespass. *Id.* This is important since the United States has established that a person has no property rights in the airspace over their property. *See U.S. v. Causby*, 328 U.S. 256 (1946); *See also* 49 U.S.C. § 40103 (2011) ("The United States Government has exclusive sovereignty of airspace of the United States."). However, there is a possibility that certain drone operators may be guilty of common law trespass, particularly in regard to small-sized drones flying at low altitudes. *Id*. Many states have laws with even higher level of privacy protection, such as California's regulation on the use of telephoto lenses to photograph private property. Cal. Civ. Code § 1708 (West 2011).

Fourth Amendment's purview.[6] Therefore, law enforcement officials were required to obtain a warrant before performing the search. In a concurring opinion, Justice Sotomayor stated, "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations."[7] The same can be said for drone surveillance because, like GPS tracking, drone surveillance persistently monitors individual behavior and generates a comprehensive personal record.

The privacy concerns arising from the use of drones in domestic airspace is underscored when the technical specifications of the devices are examined. Recent documents obtained by EPIC under the Freedom of Information Act demonstrate that the U.S. Bureau of Customs and Border Protection ("CBP") acquisitioned Predator B model drones with technology to intercept electronic communications and identify human targets.[8] EPIC responded by petitioning the Agency, joined by thirty organizations and over one thousand individuals.[9] The petition requested that CBP suspend their border drone program pending the establishment of concrete privacy regulations.[10]

Accordingly, EPIC recommends that the FAA (1) clarify the roles of NASA and the Department of Defense, (2) mandate compliance with Fair Information Practices, (3) list all drone operators in an easily accessible, public database, (4) require drone

---

[6] *United States v. Jones*, 132 S. Ct. 945 (2012).
[7] *Id*. at 955.
[8] *See* Declan McCullagh, *DHS Built Domestic Surveillance Tech into Predator Drones*, CNET (Mar. 2, 2013), http://news.cnet.com/8301-13578_3-57572207-38/dhs-built-domestic-surveillance-tech-into-predator-drones/.
[9] *See* Ernie Smith, *Drone Privacy Concerns Have Some Associations on Defensive*, Associations Now (Apr. 1, 2013), http://associationsnow.com/2013/04/drone-privacy-concerns-have-some-associations-on-defensive/.
[10] Petition from EPIC, *et al.*, to David V. Aguilar, Deputy Commissioner, U.S. Customs and Border Protection (May 22, 2013), *available at* http://epic.org/drones_petition/.

operators to disclose data collection and minimization practices, and (5) establish a process of independent auditing for drone operators.

EPIC Has Led Drone Privacy Efforts to the FAA

On February 24, 2012, EPIC, joined by over 100 organizations, experts, and members of the public, submitted a petition to the FAA requesting a notice and comment rulemaking under the Administrative Procedure Act on the privacy impact of drones in the United States.[11] EPIC's Petition noted that many federal agencies and law enforcement units are acquiring drones for deployment in US airspace.[12] The Petition further noted that drones have the technical capabilities to greatly increase surveillance of individuals in the United States:

> Gigapixel cameras used to outfit drones are among the highest definition cameras available, and can 'provide real-time video streams at a rate of 10 frames a second.' On some drones, operators can track up to 65 different targets across a distance of 65 square miles. Drones may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers. In the near future these cameras may include facial recognition technology that would make it possible to remotely identify individuals in parks, schools, and at political gatherings.[13]

Finally, EPIC's Petition observed that drones are designed with certain innate qualities that allow them to undertake constant surveillance to a degree that former methods of aerial surveillance were unable to achieve.[14] The Petition pointed out that the FAA Modernization and Reform Act of 2012 (signed on February 14, 2012) provides an opportunity for the Agency to address the privacy questions raised by drone usage.[15]

---

[11] Petition from EPIC, *et al*., to Michael P. Huerta, Acting Administrator, United States Federal Aviation Administration (Feb. 24, 2012), *available at* http://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf [hereinafter "FAA Petition"].
[12] *Id*. at 1-2.
[13] *Id*. at 2-3 (internal citations omitted).
[14] *Id*. at 3.
[15] *Id*.

On February 14, 2013 the Agency responded to EPIC's petition and consented to making privacy a necessary part of the integration of drones into the U.S. national airspace:

> While the expanded use of [drones] presents great opportunities, it also presents significant challenges as [drones] are inherently different from manned aircraft. The FAA is working to ensure the safe and efficient integration of [drones] into the [National Air Space]. In addition to safety and efficiency considerations, the FAA recognizes that increasing the use of [drones] raises privacy concerns. The agency intends to address these issues through engagement and collaboration with the public, and we urge your organization to participate in this effort.[16]

EPIC now responds to the FAA's request for input on privacy requirements and recommendations for drone operators in conjunction with the Unmanned Aircraft System Test Site Program.

The FAA's Role in Implementing Individual Privacy Protections

The FAA is mandated to "promote safe flight of civil aircraft."[17] The FAA Modernization and Reform Act requires the FAA to, within a certain amount of time, "develop a comprehensive plan" to implement government and commercial drones into civil commerce.[18] The plan must "define the acceptable standards for operation" for civil drone use.[19] In addition, the FAA is required to "provide guidance on a public entity's responsibility when operating an unmanned aircraft."[20] Before May 14, 2012, the FAA must "simplify the process" through which government entities operate drones in the national airspace.[21]

[16] Letter from Kathryn B. Thomson, Chief Counsel, FAA to Marc Rotenberg, President, EPIC (Feb. 14, 2013), *available at* http://epic.org/privacy/drones/DOT-UAS-Privacy-Issues-Letter.pdf.
[17] 49 U.S.C. § 44701(a).
[18] FMRA, *supra* n. 2 at § 322(a)(1).
[19] *Id*. at § 322 (a)(2)(B)(i).
[20] *Id*. at § 324(a)(4).
[21] *Id*. at § 324(c)(1).

There are, undoubtedly, additional protections that can only be implemented through legislation. For example, it may be outside of the FAA's congressional authority to institute a warrant requirement as a prerequisite for law enforcement drone surveillance operations. However, as the administrative agency with the statutory authority to issue drone operation licenses and maintain order in the national airspace, the FAA is the most appropriate agency to oversee comprehensive privacy rules and regulations for drone operators. The FAA is uniquely positioned to ensure that transparency, accountability, and other privacy-protective principles of data collection are built in to the drone authorization process.

The FAA's RFC/SIR on Drone Test Ranges and Privacy

The FAA requested comment on the development of a test site program for the integration of drones in to the National Airspace. The FAA's Request for Comment / Screening Information Request ("RFC/SIR") solicits public feedback concurrently with the application process for test site designation.[22] In regard to the test site applicants, the FAA indicates,

> Once the FAA has conducted and completed its considerations of the submissions, and the Administrator has issued an Order designating each successful applicant as a test site operator, each operator will be required to enter into an Other Transaction Agreement ("OTA") with the FAA. Each OTA will set out the legally binding terms and conditions under which the entity will operate the UAS Test Site.[23]

In the RFC/SIR, the FAA announced that the OTA will, in part, include "privacy requirements applicable to all operations at a test site."[24] The FAA has proposed four

[22] RFC/SIR, *supra* n. 1.
[23] *Id*. at 12260.
[24] *Id*.

privacy requirements for test site designees.[25] EPIC provides the following comments in response to the RFC/SIR and the draft privacy requirements.

(A) The Roles of NASA, and the Department of Defense Must Be Clarified

By way of the FAA Modernization and Reform Act, Public Law 112-95 ("FMRA"), Congress directed the FAA to "consult with the National Aeronautics and Space Administration and the Department of Defense," in determining the location of six test ranges for the development of drones.[26] Accordingly, the FAA has indicated that they are working "in coordination with the National Aeronautics and Space Administration ("NASA") and the Department of Defense ("DoD")."[27]

The roles of NASA and the DoD in the test site and operation process have never been publically clarified. In the interest of transparency, the FAA should take this opportunity to clearly elaborate on how these agencies intend to interact in the development of the six planned test sites.

(B) Test Site Operators Should Be Required to Comply with Fair Information Practices

Drone technology provides a new platform for persistent mass surveillance. Additionally, when compared to traditional aerial vehicles, drones drive down the cost of surveillance and make it cheaper and easier for government and corporate entities to collect information on individuals. EPIC has previously described the types of technology that drones are designed to carry:

> Gigapixel cameras used to outfit drones are among the highest definition cameras available, and can "provide real-time video streams at a rate of 10 frames a second." On some drones, operators can track up to 65 different targets across a distance of 65 square miles. Drones may also carry

[25] *Id*.
[26] FMRA, *supra* n. 2 at § 332(c)(3)(C).
[27] RFC/SIR, *supra* n. 1.

> infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers. In the near future these cameras may include facial recognition technology that would make it possible to remotely identify individuals in parks, schools, and at political gatherings.[28]

The FAA has proposed that all Site Operators enact, through public notice and comment, a privacy policy to "govern[] all activities conducted under the OTA." The FAA requests, "these policies should be informed by Fair Information Practice[s]." The FAA falls short from mandating the full integration of the Fair Information Practices ("FIPs").

The FIPs outline rights and responsibilities that provide the basis for privacy laws. Not only have FIPs played a significant role in framing privacy laws in the United States,[29] but they have also contributed to development of privacy laws around the world and to the development of important international guidelines for privacy protection.[30] The FIPs provide the basis for the Safe Harbor arrangements between the United States and Europe.[31] Recently, President Obama's Consumer Privacy Bill of Rights incorporated the FIPs into a technology-neutral framework for consumer privacy protection.[32]

As a starting point for Site Operator privacy policies, the FAA needs to affirmatively require the implementation of the FIPs into Site Operator Privacy Policies. By merely recommending that FIPs be used, the FAA fails to establish necessary baseline privacy standards. For example, Site Operators may choose to rely on the FIPs or may

[28] FAA Petition, *supra* n. 11 (internal citations omitted).
[29] *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2012).
[30] OECD guidelines on the Protection of Privacy and Transborder Flows of Personal Data, *available at* http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,000.html.
[31] *See, e.g.*, U.S.-EU Safe Harbor Overview, Export.gov (Apr. 26, 2012), http://export.gov/safeharbor/eu/eg_main_018476.asp.
[32] Consumer Data Privacy in a Networked World, the White House (Feb. 2012), http://www.whitehouse.gov/sites/default/files/privacy-final.pdf.

promulgate policies that contain few, or no, actual privacy protections.[33] By contrast, if Operators are required to incorporate FIPs into their privacy policies, the FAA can ensure that basic privacy rights are preserved. At the same time, Site Operators will have the flexibility to consider the unique aspects of the test site and the submitted public comments to determine the best methods for implementation of the FIPs to suite their community's expectations and needs.

(C) Drone Operators Should be Listed in an Easily Accessible, Public Database

There is currently no publicly accessible repository for information on past or current drone operators in the United States. In response to a letter from Representative Ed Markey in 2012, the FAA released a list of 228 entities that have applied for authorization to operate a drone in the National Airspace, including entities that were denied or were issued authorizations that have since expired.[34] Prior to this release, the only information on the identity of U.S. drone operators issued from records released pursuant to a Freedom of Information Act lawsuit filed against the FAA.[35] Even the

[33] Wells Bennett, *the FAA Wants to Hear From You About Privacy and Domestic Drones* (Mar. 1, 2013), http://www.lawfareblog.com/2013/03/the-faa-wants-to-hear-from-you-about-privacy-and-domestic-drones/ ("Which bring us to (1), the operators' privacy policies. As written, the draft says little about what these will look like. I count three hard-and-fast obligations: a privacy policy must be available publicly; the operator must be capable of receiving comments on the policy; and the policy must govern all of the operators' activities. Perhaps more interestingly, the draft also recommends conformity with Fair Information Practice Principles—uniform guidelines for the protection of personal information—but pointedly does not go so far as to require that. Thus we might wonder: substantively, could an operator satisfy the FAA, by having a "privacy policy" wherein the operator committed to obey any applicable privacy laws, both current and future? Or must a policy do something that background privacy law does not do already? And may policies vary from one site operator to the next? It is too early to tell.")

[34] Letter from Michael P. Huerta, Acting Administrator, FAA to the Honorable Edward J. Markey, House of Representatives (Sept. 21, 2012), *available at* http://markey.house.gov/sites/markey.house.gov/files/documents/FAA%20drones%20response.pdf.

[35] *See, e.g.*, Jennifer Lynch, *Who is Flying Unmanned Aircraft in the U.S.*, EFF (Jan. 10, 2012), https://www.eff.org/press/releases/who-flying-unmanned-aircraft-us.

information in those records was questionably incomplete or inaccurate based on contradictory statement made by the FAA.[36]

By contrast, manned aircraft operators are maintained in a searchable database that is accessible by serial number, geographic location, or name on the FAA's official website.[37] Any individual that wants to know what aircraft are licensed within their territory, state, or county need only enter the information and pull up a list that can be searched in an Internet browser, printed, or downloaded into a spreadsheet. The website indicates that the information is "updated each federal working day at midnight."[38]

The test sites designated by the RFC/SIR are the first step toward large-scale use of drones into the NAS. The FMRA directs the FAA to safely and fully integrate civil and public drones into the NAS. By any estimate, the number of entities applying for authorization to pilot a drone domestically is expected to rise exponentially in the years following this integration, which is currently scheduled to happen by 2015.

Before drones flood the U.S. skies, the FAA should establish a database for aerial drones similar to its current database for manned aircraft in order to allow individuals to specifically search for drone operators. The database should be easy to find and search, and provide additional information about data collection practices, as described in the next section. The creation of this database would provide a baseline for transparency in drone operations and a measure of protection against errant drone operators.

---

[36] *See* Jennifer Lynch, Just How Many Drone Licenses Has the FAA Really Issued, Electronic Frontier Foundation (Feb. 21, 2013), https://www.eff.org/deeplinks/2013/02/just---how---many---drone---licenses---has---faa---really---issued (providing details on contradictory statements made by the Federal Aviation Administration regarding the issuance of drone licenses).

[37] *See, e.g.*, FAA Registry – State / County Inquiry Results (District of Columbia), Federal Aviation Administration, http://registry.faa.gov/aircraftinquiry/StateCounty_Results.aspx?Statetxt=DC&Countytxt=DIST+OF+COLUMBIA&PageNo=1 (last visited Apr. 16, 2013).

[38] *Id*.

(D) Drone Operators Should be Required to Disclose Data Collection and Minimization Practices

As described above, drones provide the capacity for increased domestic surveillance by both government and corporate entities. Drone manufacturers freely advertise the different types of advanced surveillance equipment that may be built into their vehicles.[39] However, once installed it is impossible for an individual to identify by sight exactly how a specific drone has been equipped.

Drone operators should disclose the limits of their operational license and surveillance capabilities.[40] In order to ensure transparency and accountability in drone operations, the FAA should require drone operators to provide statements describing the full suite of surveillance equipment carried by a drone, the geographical area where the drone will be operated, and the purposes for which the drone will be deployed.[41] This information should be reported with the greatest possible amount of detail to provide the best notice to the public.[42]

(E) Drone Operators Should be Subject to Independent Auditing to Ensure Compliance with Representations

Drones present a unique threat to privacy. Drones are designed to undertake constant, persistent surveillance to a degree that former methods of surveillance were unable to achieve. Drone manufacturers have recently announced new designs that would

[39] *See, e.g.*, UAS RQ-11B Raven, Aerovironment, http://www.avinc.com/uas/small_uas/raven/ (last visited Apr. 16, 2013); Gray Eagle UAS, General Atomics Aeronautical, http://www.ga-asi.com/products/aircraft/gray_eagle.php (last visited Apr. 16, 2013).

[40] Notably, the collection of this data by the FAA may also be necessary to preserve certain safety standards. For example, the FAA may use geographic limits to control aircraft population in areas within the National Airspace. Similarly, the equipment built in to a drone will assist the FAA in determining the drone's weight and airworthiness.

[41] A similar requirement has been set forth in a bill introduced by Representative Ed Markey. Drone Aircraft Privacy and Transparency Act of 2013, H.R. 1262 (2013), *available at* http://beta.congress.gov/113/bills/hr1262/113hr1262ih.pdf.

[42] In the future the FAA may believe that drone operators should turn over additional information in order to fulfill their safety function, such as flight plans. To the greatest extent possible, this additional information should be added to the public database.

allow drones to operate for more than 48 consecutive hours,[43] and other technology could extend the flight time of future drones out into weeks and months.[44] Also, "by virtue of their design, size, and how high they can fly, [drones] can operate undetected in urban and rural environments."

These innate qualities of drones may make it difficult for individuals to police violations of law or policy by drone operators. Though drone use in the United States is still limited, reports have demonstrated that there is already widespread disregard of the FAA's operating rules.[45]

In order to ensure that drone operators comply with the terms of their authorizations and with the disclosed data collection and minimization practices, the FAA should implement a system of regular, independent audits for drone operators. Operators found to be in violation of an FAA-approved authorization should face the revocation on the authorization as well as monetary fines. Audits are a crucial oversight tool for ensuring that behaviour comports with the law and licensing requirements.

Conclusion

It is important to build privacy rules and norms into the proliferation of new surveillance technology. The FAA should use this opportunity in the test site process to implement meaningful regulations in order to preserve individual rights and civil liberties.

---

[43] Mark Brown, *Lockheed Uses Ground-Based Laser to Recharge Drone Mid-Flight*, Wired (July 12, 2012), http://www.wired.co.uk/news/archive/2012-07/12/lockheed-lasers.
[44] Steven Aftergood, *Secret Drone Technology Barred by 'Political Conditions'*, Secrecy News (Mar. 22, 2012) http://www.fas.org/blog/secrecy/2012/03/sandia_drone.html.
[45] *See, e.g.* Chris Francescani, *Damn the Regulations! Drones Plying US Skies Without Waiting for FAA Rules*, NBC News (Mar. 4, 2013), http://openchannel.nbcnews.com/_news/2013/03/04/17181948-damn-the-regulations-drones-plying-us-skies-without-waiting-for-faa-rules?lite.

Deployment of drone aircraft poses immense privacy threats. To minimize these threats, the FAA should take affirmative steps to mandate specific safeguards. Specifically, EPIC urges the FAA to:

1. Clarify the roles of NASA and the Department of Defense;
2. Mandate compliance with Fair Information Practices;
3. List all drone operators in an easily accessible, public database;
4. Require drone operators to disclose data collection and minimization practices; and
5. Establish a process of independent auditing for drone operators

Respectfully submitted,

Marc Rotenberg
EPIC Executive Director

Amie Stepanovich
Director, EPIC Domestic Surveillance Project

Khaliah Barnes,
Director, EPIC Administrative Law Project