COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to

THE FEDERAL AVIATION ADMINISTRATION of the

DEPARTMENT OF TRANSPORTATION

[Docket No. FAA—2012—0252]

Request for Comments on Unmanned Aircraft System Test Sites

May 8, 2012

By notice published on March 9, 2012, 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 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 the mandates, the FAA requests comments to "help develop refined UAS test site requirements, designation standards, and oversight activities."[3]

EPIC recommends that the FAA identify testing sites and develop evaluation criteria with consideration for the privacy and civil liberties threats arising from drone deployment. The FAA states that drone test sites will "assist in the effort to safely and

[1] Request for comments, Unmanned Aircraft System Test Sites, 77 Fed. Reg. 14319 (proposed Mar. 9, 2012).
[2] *Id*. at 14319-20.
[3] *Id*. at 14320.

efficiently integrate" drones into the national airspace.[4] To "efficiently integrate" drones into the national airspace, and because drones possess unparalleled surveillance capabilities, the FAA should assess and prevent privacy risks *before* drones are further deployed.

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 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.

EPIC recommends that the FAA support privacy by mandating transparency and accountability in drone operations, preventing unlawful access to drone surveillance information, and limiting the exposed population whenever possible.

EPIC's FAA Petition

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

[4] *Id*. at 14319.

[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).

privacy safeguards against expansive surveillance systems.[6] 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.[7] 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. The agency has so far failed to respond to EPIC's petition.

EPIC's petition to the FAA noted that many federal agencies and law enforcement units are now acquiring drones for deployment in US airspace.[8] 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.[9]

---

[6] *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.

[7] 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.

[8] *Id*. at 1-2.

[9] *Id*. at 2-3 (internal citations omitted).

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.[10]

EPIC's petition specifically requested a rulemaking on drone surveillance, and indicated that such a rulemaking should consider, among other things, data use and retention, property rights, use limitations, and enforcement.[11]

By May 14, 2012, the FAA is required to simplify the process by which government entities operate drones in the national airspace.[12] Despite this imminent deadline, and the fact that more than two months have passed since the petition was officially filed with the FAA, EPIC has not received a substantive response from the Agency.

EPIC's Recommendations on Drone Test Sites

The FAA requests comments on a variety of issues concerning drone test sites. EPIC's recommendations, detailed below, correspond to the section letters referenced in the Federal Register notice.

(A) Local governments should manage drone test ranges to aid in accountability and transparency.

The FAA asks, "should the management of these new test ranges be held by local governments or should a private entity schedule and manage the airspace?"[13] EPIC strongly recommends that local governments, in conjunction with the FAA, manage the

[10] *Id*. at 3.
[11] *Id*. at 1, 5.
[12] FAA Modernization and Reform Act of 2012, Pub. L. 112-95 §324(c)(1) (2012), *available at* https://www.gpo.gov/fdsys/pkg/BILLS-112hr658enr/pdf/BILLS-112hr658.pdf.
[13] 77 Fed. Reg. 14320.

drone test sites to aid in accountability and transparency. Giving the FAA oversight of drone test sites will provide accountability and oversight on testing activities through the Freedom of Information Act ("FOIA").[14] Additionally, in the event that the FAA collects and maintains records of individuals' images captured by the test drones, the Privacy Act of 1974 will permit those individual with access to the records.[15]

The FOIA can provide members of the public with access to drone testing results and research.[16] This information will provide further insight into the surveillance and data collection, retention, and dissemination capabilities of drones. Oversight of FAA activity is imperative in ensuring that the privacy threats posed by drones are properly addressed. Private entities would have no accountability under the FOIA or Privacy Act of 1974, and therefore they should not manage drone testing airspace.

(B) Drone network security should be evaluated.

To the extent that drone surveillance is lawfully permissible, only individuals with lawful access to drone hardware and software should operate drones. The FAA has outlined certain test site focal areas "to ensure that research is accomplished in each of the areas identified as a major obstacle" to drone integration.[17] One of those areas is drone system safety and data gathering, and the FAA asks if there are other focal areas that should be considered.[18] EPIC recommends that drone network security be considered as a test site focal area.

[14] The Freedom of Information Act, Pub. L. 89-554, 5 U.S.C. § 552 (2012).
[15] The Privacy Act of 1974, Pub. L. 93-579, 5 U.S.C. § 552a (2012).
[16] 5 U.S.C. § 552 (a)(2).
[17] 77 Fed. Reg. 14320.
[18] *Id*.

"Drone hacking," or the process of remotely intercepting and compromising drone operations, poses a threat to the security of lawful drone operations. The six test sites should examine the risk of interception of drone surveillance feeds. Specifically, test site operations should explore: (1) the ability to circumvent encryption codes within drone surveillance software and (2) the ability to manipulate hardware to gain access to drone surveillance data.

As news reports detail, drone hacking can expose troves of sensitive data.[19] EPIC's petition notes unique drone surveillance equipment that is capable of gathering hours of footage over hundred mile ranges. Thus, the FAA must address the privacy threats that arise from compromised drone surveillance.

(G) The FAA should utilize requirements contained in 14 CFR 91.305 that limit flight testing to "sparsely populated areas."

The FAA asks, "[s]hould the FAA apply [the legal requirements in 14 CFR 91.305 and FAA Order 8130.34B] to those seeking a UAS test site designation?"[20] EPIC strongly advocates that both of these requirements apply to drone test site designation. FAA Regulation 14 CFR 91.305 and FAA Order 8130.34B both limit drone flight testing to sparsely populated areas. To protect individual privacy during drone testing, it is important that testing occurs in sparsely populated areas. Adhering to these requirements

---

[19] *See* August Cole, Yochi J. Dreazen, and Siobhan Gorman, *Insurgents Hack U.S. Drones*, WALL STREET JOURNAL, Dec. 17, 2009, http://online.wsj.com/article/SB126102247889095011.html. *See also* Noah Shachtman, *Computer Virus Hits U.S. Drone Fleet*, WIRED, Oct. 7, 2011, http://www.wired.com/dangerroom/2011/10/virus-hits-drone-fleet/; Jim Miklaszewski, *US Military: Concern but no panic over drone virus,* MSNBC.COM, Oct. 8, 2011, http://www.msnbc.msn.com/id/44830227/ns/us_news-security/t/us-military-concern-no-panic-over-drone-virus/.

[20] 77 Fed. Reg. 14321.

would protect large numbers of people from unwarranted surveillance during drone testing.

Even in sparsely populated areas, however, it is important that residents and other interested parties who will be affected by the drone test sites are notified of the surveillance technology that will be tested and used. Individuals in these areas should be given advance notice of what drones will be tested, in what areas, at what times, and what surveillance equipment these drones will carry. Though notice is an insufficient privacy safeguard, a proactive approach that provides affected members of the population with relevant information will provide a necessary level of transparency in drone test operations.

Conclusion

In the early stages of a program it is important to adequately evaluate and consider the potential impact the program will have on privacy and civil liberties. The FAA should use the opportunity of this test phase to develop new safeguards that can be implemented to protect the privacy and civil liberties of individuals in the United States from pervasive drone surveillance.

Drone aircraft deployment poses immense privacy threats. To minimize these threats, the FAA should take affirmative steps during the mandatory drone testing. Specifically, EPIC urges the FAA to:

1. Task local governments, in conjunction with the FAA, with the management of drone test ranges. This will aid in accountability and transparency throughout the drone integration process;

2. To the extent that drone surveillance is lawfully permissible, test drone network security, which will inform the FAA on the best methods to prevent drone software from being compromised;
3. Limit flight testing to sparsely populated areas and provide notice to the individuals in those areas of all scheduled tests. Limiting drone testing in this fashion can minimize privacy threats caused by drones.

Respectfully submitted,

Marc Rotenberg
EPIC Executive Director

Khaliah Barnes
EPIC Open Government Fellow

Amie Stepanovich
EPIC Associate Litigation Counsel