WASHINGTON
LEGISLATIVE OFFICE

April 23, 2013

Michael Huerta, Administrator
Federal Aviation Administration
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Room W12-140
West Building Ground Floor
Washington, DC 20590-0001

Re: Comment on "Unmanned Aircraft System Test Site Program" NPRM Docket No: FAA-2013-0061

Dear Administrator Huerta:

On behalf of the American Civil Liberties Union ("ACLU"), America's oldest and largest civil liberties organization, and its more than half a million members, countless additional supporters and activists, and 53 affiliates across the country, we write to express our position regarding the privacy policies required by the Federal Aviation Administration's (FAA) proposed rule and made necessary by the FAA Modernization and Reform Act of 2012 (FMRA). Introduction of unmanned aircraft systems (UAS) by the FAA into the National Airspace System (NAS) creates unavoidable privacy concerns that the FAA must address head on. We applaud the FAA for considering the privacy problems raised by UAS and initiating this rulemaking to ensure that the test site selection process does not result in privacy violations.

The FMRA sets up a number of required way stations on the road to broader introduction of UAS into the NAS. The FAA has satisfied the first requirement of the FMRA by streamlining the process by which state and local government entities obtain FAA Certificates of Waiver or Authorization (COAs), which are necessary to operate UAS in the NAS.[1] Now, the FAA is seeking to implement the first project required by the FMRA—the establishment of six test sites, each for five years, for UAS research.[2] These test sites are "defined geographic area[s] where research and development are conducted."[3]

AMERICAN CIVIL LIBERTIES UNION
WASHINGTON
LEGISLATIVE OFFICE
915 15th STREET, NW, 6TH FL
WASHINGTON, DC 20005
T/202.544.1681
F/202.546.0738
WWW.ACLU.ORG

LAURA W. MURPHY
DIRECTOR

NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500

[1] *FAA Makes Progress with UAS Integration*, Federal Aviation Administration (May 14, 2012, 3:09 PM), http://www.faa.gov/news/updates/?newsId=68004.
[2] "Not later than 180 days after the date of enactment of this Act, the Administrator shall establish a program to integrate unmanned aircraft systems into the national airspace system at 6 test ranges. The program shall terminate 5 years after the date of enactment of this Act." FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 332(c)(1), 126 Stat 11 (2012).
[3] *Id.* at § 331(7).

The FAA published a notice of proposed rulemaking (NPRM) in the Federal Register on February 22, 2013 regarding the development of privacy policies to which test site operators must adhere.[4] The ACLU believes that these policies are a step in the right direction. However, in order to more fully address the privacy concerns that accompany the use of UAS at the test sites, the FAA should:

- Require strict adherence to the Fair Information Practice Principles (FIPPs). While we commend the FAA for identifying FIPPs as the appropriate framework for handing information collected by UAS, we believe it is critical that the FAA strengthen the language employed in the rule to ensure FIPPs are followed rather than merely considered.

- Develop a required minimum privacy policy based on FIPPs for adoption at the test sites. This would serve as a floor, and site operators should enact stricter privacy guidelines where appropriate to their specific geographic area and test plan.

- Ensure that appropriate oversight is in place to monitor compliance with the final rule, including independent audits and community involvement.

- Consider whether the proposed test site operators have experience with ethics and privacy issues, and ensure that the privacy impacts on urban areas are included.

I. Background

The introduction of UAS into the NAS represents a monumental change in both the use of America's skies and the potential exposure of Americans to aerial surveillance. While this rulemaking may only impact the privacy implications of the test site selection process, it sets the tone for the FAA's approach to UAS going forward.

Recent technological innovations make UAS uniquely capable of blanket surveillance of large areas with unprecedented ease and efficiency. Advances in imaging sensor technology have made real-time surveillance of entire cities from a small fleet of Unmanned Aerial Vehicles (UAVs) possible. For example, DARPA has developed a system of surveillance known as ARGUS-IS, or Autonomous Real-time Ground Ubiquitous Surveillance-Imaging System, that produces up to 65 video streams simultaneously, allowing for unprecedented citywide aerial surveillance, even in the dark.[5] This technology is capable of watching tens of square miles simultaneously.[6]

---

[4] Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 12259-01 (Feb. 22, 2013) (to be codified at 14 C.F.R. pt. 91), *available at* http://www.gpo.gov/fdsys/pkg/FR-2013-02-22/pdf/2013-03897.pdf [hereinafter Test Site Program NPRM].

[5] Autonomous Real-time Ground Ubiquitous Surveillance - Infrared (ARGUS-IR), DARPA.Mil, *available at* http://www.darpa.mil/Our_Work/I2O/Programs/Autonomous_Real-time_Ground_Ubiquitous_Surveillance_-_Infrared_%28ARGUS-IR%29.aspx (last visited Apr. 18, 2013).

[6] Doug Beizer, *BAE to Develop Surveillance System*, Wash. Post (Nov. 12, 2007), http://www.washingtonpost.com/wp-dyn/content/article/2007/11/11/AR2007111101348.html.

Besides powerful imaging equipment, the use of specialized software augments the surveillance abilities of UAVs. They can carry facial recognition and license plate scanning software.[7] Small UAVs can be programmed to maneuver through windows,[8] perch and stare,[9] and fly in swarms.[10] Using recently-developed "ubiquitous navigation" technologies, UAVs can accurately navigate inside of homes by incorporating atmospheric pressure sensors, radios, and other weak location indicators, which can provide a more accurate location when used in concert.[11] They can also be outfitted with robotic arms to carry objects into or remove objects from various places.[12]

While Americans have long been subject to other forms of aerial surveillance, use of UAS for surveillance purposes leads to a difference in degree that becomes a difference in kind. Americans have never before faced the threat of being watched with unrelenting scrutiny by a system with such low operational costs. In recent testimony to the Senate Judiciary Committee, Benjamin Miller, Unmanned Aircraft Program Manager for the Mesa County Sheriff's Office, estimated that "unmanned aircraft can complete 30 percent of the missions of manned aviation for 2 percent of the cost."[13] Those differentials will only grow as technology advances.

Given this combination of advanced capabilities and low operational costs, Americans are concerned about the implications of placing UAS above their homes and places of work and worship. In a recent poll conducted by Monmouth University, nearly two-thirds of Americans surveyed expressed at least some concern about the use of UAS with high-tech surveillance cameras by U.S. law enforcement.[14] UAS manufacturers are also concerned with the privacy implications of UAS. In creating a code of conduct for the UAS industry,[15] the AUVSI told the L.A. Times, "We want everybody to know that this technology will be handled safely and with

---

[7] Leslie Harris, *UAVs: Will Our Civil Liberties Be Drones Out?*, ABC News (June 7, 2012), http://abcnews.go.com/Technology/unmanned-aerial-vehicles-civil-liberties-droned/story?id=16511914#.ULjaVIU1WhI.

[8] GRASP Lab, Univ. of Pa., *Aggressive Maneuvers for Autonomous Quadrotor Flight*, YouTube (May 21, 2010), http://www.youtube.com/watch?v=MvRTALJp8DM.

[9] *Id*.

[10] GRASP Lab, Univ. of Pa., *A Swarm of Nano Quadrotors*, YouTube (Jan. 31, 2012), https://www.youtube.com/watch?v=YQIMGV5vtd4.

[11] Christopher Mims, *A New Microchip Knows Just Where You Are, Indoors and Out*, MIT Tech. Rev. (Apr. 9, 2012), http://www.technologyreview.com/news/427451/a-new-microchip-knows-just-where-you-are-indoors-and-out/.

[12] GRASP Lab, Univ. of Pa., Construction with Quadrotor Teams, YouTube (Jan. 13, 2001), https://www.youtube.com/watch?v=W18Z3UnnS_0.

[13] *The Future of Drones in America: Law Enforcement and Privacy Consideration Before the S. Judiciary Comm.*, 2013 WL 1153562 **(**statement of Benjamin Miller, Unmanned Aircraft Program Manager, Mesa County Sheriff's Office)**,** *available at* http://www.judiciary.senate.gov/hearings/testimony.cfm?id=d27f2c4073b40a8e678e4a9f6f36acec&wit_id=d27f2c4073b40a8e678e4 a9f6f36acec-0-6.

[14] *U.S. Supports Some Domestic Drone Use*, Monmouth Univ. Polling Inst. (June 12, 2012), https://www.monmouth.edu/assets/0/84/159/2147483694/3b904214-b247-4c28-a5a7-cf3ee1f0261c.pdf.

[15] Association for Unmanned Vehicle Systems International, *Association Unmanned Aircraft System Operations Industry "Code of Conduct"*, AUVSI.org, *available at* https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedFiles/AUVSI%20UAS%20Operations%20Code%20of%20Conduct%20-%20Final.pdf (last visited Apr. 19, 2013).

the utmost respect to individuals' privacy … Ultimately, public confidence is needed in fielding these systems."[16]

Responding to widespread concern over UAS, Congress and state legislatures have begun to consider legislation to regulate UAS privacy, showing the concern of the American people over the privacy risks of UAS. On April 11, 2013, Idaho became the first state to pass comprehensive UAS regulation.[17] By our latest count, UAS legislation is active in 29 states[18] and the House of Representatives, where two UAS privacy bills were recently introduced.[19]

The wide outpouring of concern over the introduction of UAS into America's skies necessitates a comprehensive and forward-looking approach to privacy in every step of the integration process. Without meaningful and effective regulation, the availability and low cost of UAS threatens to turn America into a surveillance state. In the past, law enforcement agencies have been eager to make full use of new surveillance technologies, such as networks of surveillance cameras,[20] hidden GPS tracking devices, and automated license plate readers.[21] While UAS can certainly be used in beneficial ways that do not violate privacy, comprehensive privacy oversight by the FAA at this preliminary stage is necessary to ensure that notions of privacy govern the way surveillance technology is used, and not the other way around.

II. The FAA Should Require Strict Compliance with FIPPs in Test Site Selection

The FAA's NPRM contains the following text related to the privacy precautions to be taken by test site operators:

> (1) The Site Operator must ensure that there are privacy policies governing all activities conducted under the OTA, including the operation and relevant activities of the UASs authorized by the Site Operator. Such privacy policies must be available publically, and the Site Operator must have a mechanism to receive and consider comments on its privacy policies. In addition, these policies should

---

[16] W.J. Hennigan, *Drone trade group adopts guidelines for flying in U.S. airspace*, LATimes.com (July 5, 2012), http://articles.latimes.com/2012/jul/05/business/la-fi-drone-privacy-20120705.

[17] S. Bill No. 1134, 62nd Leg., 1st Sess. (Idaho 2013) (enacted), *available at* http://www.legislature.idaho.gov/legislation/2013/S1134E2.pdf.

[18] Allie Bohm, *Status of Domestic Drone Legislation in the States*, ACLU Free Future Blog, http://www.aclu.org/blog/technology-and-liberty/status-domestic-drone-legislation-states (last updated Apr. 18, 2013).

[19] Preserving American Privacy Act, H.R. 637, 113th Cong. (2013), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-113hr637ih/pdf/BILLS-113hr637ih.pdf; Drone Aircraft Privacy and Transparency Act of 2013, H.R. 1262, 113th Cong. (2013), http://markey.house.gov/sites/markey.house.gov/files/documents/3.19.13_DroneAircraftPrivacyTransparencyAct2013.pdf.

[20] *See, e.g.*, Suzanne Ito, *Surveillance Cameras in Chicago: Extensive, Pervasive and Unregulated*, ACLU, http://www.aclu.org/blog/free-speech-national-security/surveillance-cameras-chicago-extensive-pervasive-and-unregulated.

[21] *See, e.g.*, Julia Angwin & Jennifer Valentino-DeVries, *New Tracking Frontier: Your License Plates*, Wall St. J. (Sept. 29, 2012), *available at* http://online.wsj.com/article/SB10000872396390443995604578004723603576296.html.

> be informed by Fair Information Practice Principles. The privacy policies should be updated as necessary to remain operationally current and effective. The Site Operator must ensure the requirements of this paragraph are applied to all operations conducted under the OTA.[22]

The proposed requirement is promising, but not meaningful enough to provide adequate privacy protection to those who live within the range of the test sites. In this context, privacy policies must be read to mean detailed guidance on the handling of personal information, including controls over how the information is collected, what can be done with it, how it is kept secure, and when it must be destroyed. Too often "privacy policy" has been shorthand for telling consumers about the privacy rights that they don't have.

The proposed rule's language is not strong enough to ensure that Operators' privacy policies strictly comply with the FIPPs. Requiring only that the policies "should be informed" by FIPPs is too weak to ensure effective privacy protection. The final rule should require operators to apply each principle of FIPPs directly, and the FAA should give detailed guidance on the permissive application of FIPPs in this context.

Furthermore, the NPRM does not specify which version of the FIPPs a Site Operator must look to when drafting a privacy policy. Several versions of the FIPPs are in active use.[23] We believe that the FIPPs promulgated by the White House as part of its National Strategy for Trusted Identities in Cyberspace report[24] are well suited for the Test Site selection process. Alternatively, the FIPPS used by DHS in conducting Privacy Impact Assessments are similar and also suitable. Both of these versions provide a robust articulation of the data privacy principals that form privacy best practices.

III. The FAA Should Promulgate a Baseline Privacy Policy for Test Site Operators

In order to regulate privacy in a uniform and comprehensive manner, the FAA should promulgate a baseline privacy policy (BPP) that would apply to all selected Operators. The BPP should serve as a regulatory floor, ensuring the continued adherence to minimum privacy standards throughout the test site process. Operators should be encouraged, and in some cases required, to go beyond the BPP in creating adequate privacy protections for their specific mission. For instance, an Operator in an urban location would require additional precautions on account of the increased population density and resultant increased risk of privacy invasion. A robust BPP should ensure that every test site recognize and mitigate unwarranted intrusions upon privacy while giving Operators leeway to develop additional privacy policies that address the unique privacy challenges they face.

---

[22] Test Site Program NPRM, *supra* note 4.

[23] For a history of Fair Information Principles and catalog of variants, see Robert Gellman, Fair Information Practices: A Basic History (Nov. 12, 2012), *available at* http://bobgellman.com/rg-docs/rg-FIPShistory.pdf.

[24] White House, National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy: Enhancing Online Choice, Efficiency, Security, and Privacy, App. A (Apr. 2011), *available at* http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

To prevent unwarranted privacy harms, the BPP should ensure that each test carried out follows a strict data collection policy. In brief, the BPP should directly reference the eight FIPPs:

- **Transparency:** The Operator should create and make publicly available a data collection policy that explains the data that is being collected. Following their tests, they should prepare a public report on the type of data collected and catalog any privacy incidents that occurred during the test. In addition, the FAA should explore whether technological solutions exist that would allow the public to track the location of UAS during flights.

- **Individual Participation:** The Operator should consult with the community living within the test area through community meetings and online consultations. Residents in the test area who object should be given an opportunity to opt their property out of the test area.[25] They should be given access to any personally identifiable information (PII) collected and provided a means to correct or redress use of PII gathered by the use of UAS.

- **Purpose Specification:** UAS should be flown only pursuant to specific, articulated purposes. The Operator should inform the affected communities of the purpose of the test sites and UAS missions. They should specifically inform the affected residents of the purposes to which any collected PII is intended to be used.

- **Data Minimization:** The Operator should only store data that is clearly needed for test purposes, and should not store data for longer than is necessary. The FAA should set concrete standards for the duration of data retention and ensure that PII is deleted after that time.

- **Use Limitation:** Use of captured data should not exceed the authorization of the FAA or the testing purpose of the Operator. Data should not be shared with parties beyond the Operator and the FAA, or as otherwise authorized by the FAA to ensure compliance with the BPP. In addition, the FAA should make clear that PII collected by the test operators and shared with the agency is governed by the Privacy Act.

- **Data Quality and Integrity:** The Operator should ensure that any PII collected is "accurate, relevant, timely, and complete."[26] This type of PII would include individuals or property identified by the UAS. The Operator has a duty to ensure that the information collected has not been altered or destroyed in an unauthorized manner and that affected residents have the ability to correct inaccuracies in the PII aggregated by the use of UAS.

---

[25] Exclusion zones should be feasible given the advanced navigation capabilities of UASs.

[26] White House, National Strategy for Trusted Identities in Cyberspace: Enhancing Online Choice, Efficiency, Security, and Privacy: Enhancing Online Choice, Efficiency, Security, and Privacy, App. A (Apr. 2011), *available at* http://www.nist.gov/nstic/NSTIC-FIPPs.pdf.

- **Security:** Data collection statements and test plans should detail the security used for communication between ground stations and UAS. All communications should be encrypted when audiovisual content is being transmitted.

- **Accountability and Auditing:** All employees should be familiar with the privacy policy and the Site Operator should ensure that employee and contractor behavior is in line with the policy. The Site Operator should audit employee performance on a randomized basis to ensure that the privacy policy is being strictly followed. The FAA also has significant oversight responsibilities which we have articulated in more detail below.

For the purposes of the above principles, the FAA should define PII as "information that is reasonably likely "to enable identification of an individual; or information about an individual's property that is not in plain view."[27]

IV. The FAA Should Provide Meaningful Privacy Oversight of Test Site Operators

The NPRM relies on self-regulation and does not contain any mechanism for privacy oversight. It requires compliance with "[f]ederal, state, and other laws regarding the protection of an individual's right to privacy"[28] and relies on law enforcement agencies to ensure such laws are not being violated by Site Operators. However, the NPRM does not indicate any method for monitoring compliance with the Operators' privacy policies. This omission does not comport with the severity of the privacy risks inherent in broad tests related to introducing UAS into the NAS. The FAA must provide continuous oversight of Test Site Operators to ensure they remain in compliance with the BPP and/or their own privacy policies.

The FAA should provide mechanisms to allow for citizen involvement. The FAA should require site operators to keep accurate, detailed, frequent, and accessible records, thereby creating the opportunity for effective citizen participation. Providing a mechanism for citizens to bring privacy policy violations to the attention of the FAA will lead to an increase in reporting that will deter violations of privacy policies.

Additionally, the FAA should conduct its own audits of test sites with particular attention to compliance with the BPP and the test site operators own privacy commitments. In the case of breaches of the BPP, the FAA should reserve greater authority to suspend test site operations than is currently reflected in the NPRM. A significant violation of a privacy policy should be sufficient grounds for termination of the operator's COA.

V. The FAA Should Consider the Privacy Record of Applicants and Select Site Operators Studying Privacy Aspects of UAS Integration

The FAA should take the privacy track record of Test Site Operators into account when selecting an Operator. The application should require a summary of any privacy incidents that

[27] Preserving American Privacy Act, *supra* note 19.
[28] Test Site Program NPRM, *supra* note 4.

Operator has been involved in. The FAA should also conduct its own due diligence to determine whether an applicant would present a privacy risk, based on past performance. Previous privacy violations by an applicant should serve as sufficient grounds for rejecting an application.

Just as previous privacy violations should stand as an impediment to test site applicants, would-be test sites that demonstrate an understanding of and willingness to pursue privacy testing warrant favorable consideration. This is not to suggest that a site's ability to address privacy should be the only factor considered. Rather, the FAA should ensure that one or more of the selected sites is well versed in privacy issues. Sites that have an active UAS research program with a focus on ethics and privacy will be particularly well-positioned to address the privacy concerns that accompany the introduction of UAS into the NAS.

For example, the University of North Dakota formed the Unmanned Aircraft Systems Research Compliance Committee in October 2012.[29] This Committee provides oversight for all UAS research activity within the University. "The committee will consider the ethical consequences of the proposed research and will apply community standards in determining whether a research project may be approved."[30] The existence of such a committee demonstrates a commitment to understanding the ethical and privacy concerns that surround the introduction of UAS into the NAS. The ACLU does not favor any particular site or applicant, but to the extent that a test site applicant is able to demonstrate similar or greater appreciation for the privacy issues at play, the FAA should consider that favorably.

In addition to an applicant's privacy track record and stated privacy policies, the test site's surrounding population density should inform the FAA's selection decisions. Congress has instructed the FAA to "consider geographic and climate diversity"[31] in selecting the test sites. The FAA should construe this mandate to include diversity in population density. Importantly, the risk of undue invasion of privacy by UAS increases with population density. Test sites that operate in primarily rural locations will face starkly different privacy problems than those that operate in large cities. The FAA should ensure that one or more of the test sites selected are located in or near a densely populated urban area.

VI. Conclusion

The FAA's forthcoming privacy regulations for test sites have the potential to make significant headway in the ongoing effort to secure the privacy interests of Americans against the increased risks of intrusion presented by UAS. These regulations, if crafted appropriately, will serve as the framework both for future regulations by the FAA and congressional legislative efforts. To ensure that the rule maximizes the ability of test site operators to explore the safety and privacy implications of UAS, the FAA should make adherence to the FIPPs mandatory. To facilitate compliance, the FAA should promulgate a baseline privacy protection (BPP) and take steps to ensure that test site operators adhere to the regulatory floor. Such steps may include an

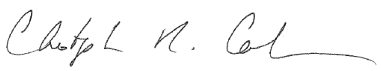
---

[29] *Unmanned Aircraft Systems Research Compliance Committee*, Univ. of N.D., http://und.edu/research/resources/uas-research-compliance-committee.cfm (last visited Apr. 19, 2013).
[30] *Id.*
[31] FAA Modernization and Reform Act of 2012, *supra* note 2, at § 332(c)(3)(A).

FAA oversight regime requiring test site operators to keep detailed records and make them accessible when necessary to comply with the BPP.

FAA regulation will not supplant the need for congressional action to augment the currently scant privacy protections surrounding UAS, especially with respect to protecting privacy against government intrusion. However, through this rulemaking, the FAA has taken positive steps towards creating a privacy oversight regime for UAS testing, and we applaud its proactive approach to ensuring that UAS are integrated in the NAS in a responsible and privacy-protective manner.

Sincerely,



Christopher R. Calabrese
Legislative Counsel
Washington Legislative Office

Ben Wizner
Director, Speech Privacy and Technology Project

Scott Bulua
Technology Law and Policy Clinic
New York University School of Law

Stephen Elkind
Technology Law and Policy Clinic
New York University School of Law