KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

P +1-202-637-9800
F +1-202-637-0968
E info@cdt.org

COMMENTS TO THE FEDERAL AVIATION ADMINISTRATION ON UNMANNED AIRCRAFT SYSTEM TEST SITE PROGRAM

Docket No. FAA–2013–0061

April 23, 2013

On behalf of the Center for Democracy & Technology ("CDT"), a Washington DC-based public policy organization, we submit the following comments in response to the Request for Comments issued February 22, 2013 (78 Fed. Reg. 12259) entitled "Unmanned Aircraft System Test Site Program." We particularly applaud the Federal Aviation Administration ("FAA") for considering privacy protections in Unmanned Aircraft System ("UAS") Test Site procurement and operation. As the licensing authority for aircraft and their pilots, regardless of manned or unmanned systems, FAA is uniquely capable of setting privacy-relevant policy for systems that operate in manned airspace.

CDT has been involved in the national public policy discussion around integration of UASs (commonly referred to as drones) into the National Airspace System ("NAS") since last year's passage of the FAA Modernization and Reform Act.[1] We have been monitoring privacy-relevant UAS legislation[2] and determining specific steps the FAA could take to better integrate UAS operations with social privacy norms and safety concerns by requiring they have radio-frequency "license plates."[3] With active work in consumer privacy, free expression, national security, and cybersecurity, CDT has a unique perspective that balances both individual privacy interests and business innovation.

Surveillance-capable UASs are quite different than manned aircraft and other types of surveillance activities for a number of reasons. First, platforms for UAS-based surveillance are increasingly inexpensive, with small systems costing a few hundred dollars, compared to many thousands of dollars per hour of operation for manned surveillance aircraft such as airplanes and helicopters. Because of their small size and lack of an on-board human pilot, UASs are capable of going many places manned aircraft cannot (such as between narrow buildings) and capable of operation in environments that humans cannot (such as

---

[1] Harley Geiger, *How Congress Should Tackle the Drone Privacy Problem*, CENTER FOR DEMOCRACY & TECHNOLOGY (March 27, 2012), https://www.cdt.org/blogs/harley-geiger/2703how-congress-should-tackle-drone-privacy-problem.

[2] G.S. Hans, *Drone Privacy Bills Attempt to Protect Americans from Governmental, Commercial Surveillance*, CENTER FOR DEMOCRACY & TECHNOLOGY (April 8, 2013), https://www.cdt.org/blogs/gs-hans/0804drone-privacy-bills-attempt-protect-americans-governmental-commercial-surveillance.

[3] Joseph Lorenzo Hall, *"License Plates" for Drones?*, CENTER FOR DEMOCRACY & TECHNOLOGY (March 8, 2013), https://www.cdt.org/blogs/joseph-lorenzo-hall/0803license-plates-drones.

during high-g tactical maneuvers, high altitudes and long times aloft). UASs, like manned surveillance aircraft, are capable of unique vantage points from which ground-based individuals may not expect surveillance systems to observe. Finally, the nexus of these considerations result in aerial surveillance platforms that may be very difficult – if not impossible – to visually identify, such that many types of UAS surveillance are possible with no notice to ground-based individuals.

I. Test Site and UAS Operator Privacy Policies

The RFC plans to require Site Operators to have "privacy policies governing all activities conducted under the [site operator agreement], including the operation and relevant activities of the UASs…". There are at least two components to this requirement: requiring the Test Site itself to have a privacy policy governing its own operations and requiring UAS operators authorized by the Site Operator to have their own privacy policy. We discuss each in turn.

A. Test Site Privacy Policies

While there is some inconsistency between the FAA press release announcing the comment opportunity and the RFC from the Federal Register,[4] the RFC makes it clear that privacy policies "should be informed by Fair Information Practice Principles." First, we believe, that this "should" should be a "must," such that for both Test Sites and authorized UAS Operators, privacy policies are grounded in Fair Information Practice Principles (FIPPs).[5] Incorporating each of the FIPPs into the site operators' privacy policies is a necessary measure to protect individual privacy. The FIPPs are delineated as they should apply to UAS privacy policies as follows:

- **Transparency:** The privacy policies should be transparent about data collection capabilities and the use, dissemination, and maintenance of PII (personally identifiable information).
- **Individual Participation:** To the extent practicable, test site operators should seek consent of individuals whose PII is collected.
- **Purpose Specification:** The privacy policy should specify for what purposes, if any, PII collected via test site operations will be used.
- **Data Minimization:** PII collected at test sites should be only retained for the specified purposes. PII collected at test sites should be permanently deleted within ninety days of collection or within thirty days of the end of the test period, whichever comes first, except where the specified purpose is for journalistic use, in which case the data need only be minimized as the Test Site or UAS Operator specifies in its privacy policy.

[4] The press release announcing this comment opportunity stated that Site Operators "*must* ensure that its privacy policies are informed by Fair Information Practice Principles" (emphasis added) when the RFC states a "should" (78 Fed. Reg. 12260). *See* Press Release, Federal Aviation Administration, FAA Announces Request for Proposals For Unmanned Aircraft Systems Research and Test Sites (February 14, 2013), *available at* http://www.faa.gov/news/press_releases/news_story.cfm?newsId=14313 (last visited April 9, 2013).

[5] U.S. DEPARTMENT OF HOMELAND SECURITY, MEMORANDUM NUMBER 2008-01, PRIVACY POLICY GUIDANCE MEMORANDUM: THE FAIR INFORMATION PRACTICE PRINCIPLES: FRAMEWORK FOR PRIVACY POLICY AT THE DEPARTMENT OF HOMELAND SECURITY, (December 29, 2008), *available at* http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

- **Use Limitation:** PII collected and retained by test site operators should only be used for the specified purposes.
- **Data Quality and Integrity:** To the extent possible, test site operators should ensure that the data collected and retained is accurate.
- **Security:** Test site operators should take steps to protect data from unauthorized access or disclosure.
- **Accountability and Auditing:** Test site operators should communicate their commitments under the privacy policies to other entities, including UAS operators, and conduct audits to ensure their compliance with privacy policies.

With regards to data collection, both test site operators and UAS operators should apply different standards to PII versus aggregated information. Personally identifiable information, such as photographs of an individual, biometric readings, or video records, should be deleted or effectively anonymized within thirty days under general data minimization principles (apart from journalistic uses, as described above). Aggregated information, which should not include any PII but instead should anonymize any data pertaining an individual, need not be deleted within the same period as PII, but should be used for limited purposes.

B. UAS Privacy Policies (Data Collection Statements)

UAS operators as a condition of licensing should file Data Collection Statements (DCS) with the FAA for UAS operations that involve remote sensing and signals surveillance from the UAS platform.[6] The final contract between FAA and Site Operators should provide more clear guidance about the elements that a licensed drone's DCS must disclose, including:

- The purpose for which the UAS will be used and the circumstances under which its use will be authorized and by whom,
- The specific kinds information the UAS will be capable of collecting, including whether that information is personally identifiable or not,
- The length of time for which the information will be retained (in a manner that preserves identifying data),
- Methods used to minimize or aggregate data and delete old data,
- Parties with which information will be shared,
- The possible impact on individuals' privacy,
- The specific steps the operator will take to mitigate the impact on individuals' privacy, including protections against unauthorized disclosure,
- The individual responsible for safe and appropriate use of the UAS, and
- An individual point of contact for citizen complaints.

After a UAS operator has submitted its DCS to the FAA, the FAA will need to ensure oversight of the operator to ensure that it remains in compliance with the DCS. In addition to making each DCS publicly available, the FAA should execute audits of operators and their

[6] Each DCS will need to be current, and licensing should prohibit activities not detailed in the DCS.

UASs to determine that the actual use of each UAS comports with the statements in its DCS, with penalties ranging from fines to revocation of the operator's license.

Once a UAS has been deployed, its operation will also need to be subject to public oversight in order to ensure the DCS accurately reflects the actual operative use of the UAS. The creation of a public facing registry that includes each DCS will help individuals to monitor specific UASs and their operations, and to determine whether the actual operations comport with the specifics of the filed DCS. In addition, introducing mandatory limitations on the use of data collected by UASs, such as creating opt-outs for the use of data collected by UASs for controversial purposes (e.g. marketing) and limitations on identifying individuals without court orders, will also give individuals more confidence that data collected by UASs will not be used for unwanted purposes without oversight.

Finally, as discussed above in the test site context, data minimization is one of the most important FIPPs in the UAS context and deserves particular attention from the FAA. Ensuring that PII collected is deleted within ninety days or within 30 days of the conclusion of the test site program (and exempting journalistic purposes) and that aggregated information is removed after a longer limited period (preferably 120 days) will help to protect individuals from possible privacy invasions. Because UASs are able to collect both PII and non-PII without individual knowledge or consent, ensuring that such data is appropriately limited in scope and retention will help to reduce the likelihood of privacy invasions that could result from lengthy retention. Both UAS operators and test site operators should be subject to the same application of FIPPs, in order to both ensure consistent application and protect individual privacy. However as we describe in the previous section, UAS operator-specific privacy policies (or Data Collection Statements) will need to be operationalized to reflect the general characteristics of UAS operational capabilities.

C. Baseline Privacy Policies/Data Collection Statements

In order to assist test site operators and UAS operators in crafting their privacy policies and DCS submissions, the FAA should issue model baseline DCSs and privacy policies to operators of both UASs and test sites to provide guidance. By doing so, the FAA can help ensure from the outset of the test site program that operators include measures to protect individual privacy.

II. Sanctions and Prohibitions

The FAA should rescind site operator licenses when UAS operators at a given site have been found to engage in serious privacy-invasive behavior, such as voyeurism, stalking, and operating outside the parameters of a data collection statement (e.g., sharing UAS surveillance data with third party commercial entities in violation of statements made in a data collection statement). The FAA should also consider levying fines against operators that fail to comport with their DCSs and privacy policies, potentially at a level akin to traffic violations.

There should also be appropriate prohibitions on where UASs can operate even within a test site. Certain settings, such as the home, curtilage,[7] health care facilities, and places of worship, should receive stronger protections due to the unique and highly personal and private activities

[7] The immediate area around a property where individuals have a reasonable expectation of privacy.

that take place in such venues. In addition to the federal constitutional protections that attach to activities conducted in the home, locations such as health care facilities and places of worship are deserving of strong privacy protections. The FAA should recognize these determinations and prohibit the use of UASs to monitor or conduct surveillance of such areas. Violation of this prohibition should result in the revocation of an operator license, and potentially a test site license depending on the instance.

III. UAS Licensing, Registry, and Identification Signaling

The unmanned nature of UAS allow them to be physically small and operate in conditions that humans could not easily tolerate, such as remaining aloft for days at a time. UASs at altitude will be very difficult to visually identify by ground-based observers, and those observers will have a difficult time assessing the class of given UAS aircraft as well as its functional capabilities.

There exists an important public interest in individuals on the ground being able to answer questions such as: "What UASs are operating near me and what are each of their surveillance capabilities?", "If a UAS is operating in an inappropriate manner, how do I contact the owner/operator?" To fulfill this need, there are two crucial considerations: a UAS registry and a UAS identification signal.

A. UAS Licensing and Registration

Similar to licensing and registration of larger aircraft, the FAA will need to license UAS aircraft that operate above 400 feet (as well as the operators of such aircraft), when they operate in regulated manned airspace. Much like the FAA Aircraft Registry[8] — in which records relevant to ownership and airworthiness are registered — the FAA will need to set up a similar UAS Registry. The UAS Registry will need to be somewhat different from the Aircraft Registry, in order to provide information that is relatively enhanced for UAS compared to larger aircraft:

- Name and address of the UAS owner: Each UAS should publicly identify as being owned by an individual or incorporated entity with contact information.
- UAS classification: Only approved classes of UAS aircraft should be operated and the UAS class identifier should allow a public citizen to learn about features of the class, such as airframe type, weight, dimensions, locomotive mechanics and power (e.g., fixed-wing w/ propeller, quadracopter, etc.) and maximum duration aloft.
- Data Collection Statement: The Data Collection Statement (DCS, see above) required of all UAS operating above 400 feet should be directly available as part of the registration record (as opposed to, e.g., a hyperlink provided by the owner/operator to resources maintained outside of the Registry).
- ATCRBS Mode S Code ("hex code"): Each licensed UAS should be issued an Air Traffic Control Radar Beacon System (ATCRBS) Mode S Code — currently a fixed 24-bit

[8] *See* FEDERAL AVIATION ADMINISTRATION, *FAA-Registry – Aircraft – N-Number Inquiry,* http://registry.faa.gov/aircraftinquiry/.

address[9] — that becomes part of the UAS registration record and would be used by the UAS to identify itself during interrogation by secondary surveillance radar (SSR).

- N-number — While the hex code is a permanent identifier for a given UAS, there will need to be a more human-readable short code to identify UAS aircraft. A "U-number" — short for "UAS number — would serve that purpose and could use the same general structure of the N-number (e.g., a "U" followed by 5 alphanumeric characters). If a UAS were to crash on public or private property, the owner may be identified by physical insignia bearing this U-number.

The FAA UAS Registry should be searchable in the same manners as the FAA Aircraft Registry, although it might also be useful to provide real-time (or close to real-time) search capabilities based on an input location.

B. UAS Identification Signaling

With a UAS Registry that provides more information on surveillance capabilities and data collection practices, an individual on the ground could theoretically know a number of important details about UAS operations in their vicinity. However, in order to practically know specifically which individual UAS aircraft are currently operating and their capabilities, each UAS will need to publicly file flight plans before each flight and/or affirmatively broadcast a signal that identifies the UAS during flight. It is easy to imagine an UAS deviating from a filed flight plan, and there already exists requirements for broadcasting an identification signal that could be easily translated from larger aircraft to UAS.

In addition to a somewhat static FAA UAS Registry, UAS aircraft should be required to carry a transponder that can broadcast certain information (identification number, location, altitude and velocity) using automatic dependent surveillance-broadcast (ADS-B Out). ADS-B Out data broadcasting will be required of most aircraft operating in US airspace by 2020 via rules set in the FAA's Next Generation Air Transportation System (NextGen) effort.[10] ADS-B seems well suited for UAS operations as well.

We consider the traffic broadcast element of ADS-B Out to be of particular use for tracking UAS operations.[11] If UAS aircraft are required to broadcast an ADS-B Out signal that transmits the UAS hex code identification number, current location, altitude and velocity, this would complete the missing link between the enhanced UAS Registry and direct knowledge of UAS capabilities, ownership, etc. by ground-based observers. There exist now relatively cheap ADS-B receivers — $800 for the Garmin GDL 39[12] and $899 for the ForeFlight Stratus 2[13] — that interface with popular consumer electronics like the Apple iPad. Such

[9] The given limit of almost 17 million hex codes may need to be revisited if current and projected allocations anticipate saturation of the address space in the short and medium term.

[10] Such transponder equipment requirements are explained in 14 C.F.R. pt. 91.130 (Class C airspace), 14 C.F.R. pt. 91.131 (Class B airspace), 14 C.F.R. pt. 91.135 (Class A airspace).

[11] While one of the primary uses for ADS-B in larger aircraft is to increase precision and efficiency of air-traffic control (ATC) collision avoidance operations, it is unclear if there will be an ATC-like entity directing UAS traffic. However, such signals could be quite useful for automated, programmatic collision avoidance.

[12] GARMIN, Product Overview: GDL 39, https://buy.garmin.com/shop/shop.do?pID=93601&ra=true (last visited April 22, 2013).

[13] ForeFlight, Product Overview: Stratus 2, *available at:* http://www.foreflight.com/stratus (last visited April 22, 2013).

tools would allow anyone with this equipment to receive real-time UAS flight information, and differentiate specific UASs based on their hex code. We also expect organizations to provide UAS mapping and flight plan archive services, possibly reducing the equipment for public tracking of UAS operations to a simple Internet-connected device. Moreover, these services can integrate the above-mentioned FAA UAS Registry such that real-time UAS flight data can be combined with elements of the UAS license registration, such as information from the UAS' data collection statement and/or information about the sensor capabilities for each UAS currently aloft.

The FAA's current ADS-B rules apply to aircraft in class A, B, and C airspaces, but we certainly expect UAS operations in class D, E and G airspace and see no reason to exempt UASs operating in these other airspace classes from having to broadcast ADS-B Out data. Certainly, the traditional exemptions for model aircraft operation and the current unregulated airspace below 400 feet should still allow relatively simple UAS operations without such equipment requirements; however, if the UAS has sufficient power and recording capability, it should also be able to generate an ADS-B Out signal. We anticipate that some UAS aircraft intended to be used above 400 feet may not be capable of equipping and powering ADS-B Out equipment on their airframes, due to particularly small size, low weight, or low power ("nanodrones"). However, we believe the FAA should require in these instances that ADS-B Out information be broadcast from the operator's ground station location, relaying information sent to the ground station by the UAS via ADS-B Out transmission. This would only require a GPS receiver to be equipped and powered on the airframe and the typical command and control signaling infrastructure used to control the UAS. Small autonomous UAS that are not directly navigable by a ground operator — e.g., they may be preprogrammed — should not be allowed to co-occupy manned airspace classes, or should be required to broadcast ADS-B Out, especially for sense and avoid signaling.

The safety considerations alone are a compelling argument for requiring UAS to broadcast ADS-B Out. Any UAS platform that occupies regulated manned airspace runs the risk of interfering with or potentially colliding with manned aircraft. Manned aircraft capable of receiving ADS-B flight information will need to use this data to plan flights and incorporate into sense and avoid signaling systems. Given the possible density of aircraft around popular events or emergencies, providing data via ADS-B Out seems to be a basic, necessary but not sufficient element of regulating a safe diversified dense airspace.

IV. Test Site Selection

The FAA should choose at least one test site in a state with strong privacy protective UAS laws and regulations. One such state, Idaho, creates limitations on UAS use similar to those proposed above.[14] By doing so, UAS operators will be required to consider relevant state laws that protect individual privacy, and will be aware of the most stringent state regulations that they must comply with in a future, broader scale UAS program. The FAA should also choose an applicant that has an established UAS research program with active engagement with UAS privacy and ethical issues. (e.g., the University of North Dakota has a UAS-specific institutional

[14] Laura Zuckerman, *Idaho Restricts Drone Use by Police Agencies Amid Privacy Concerns*, REUTERS (April 11, 2013), *available at* http://www.reuters.com/article/2013/04/12/us-usa-drones-idaho-idUSBRE93B03S20130412.

review board[15]). An applicant that has had significant experience with exploring UAS issues would be well suited to examining the use of UASs in the field and applying ethical, technological, and privacy research in a field study. Finally, the FAA should be sure to select at least one test site near an urban area, in order to avoid a bias towards privacy issues relevant for rural UAS operations.

V. Privacy-Specific Testing Activities

While the NPRM does not specify in detail the activities that UASs operating on a test site will be required to perform, we would like to see UAS platforms operating at test sites perform a standard suite of privacy tests. Appendix B of the Other Transactions Agreement incorporated into the UAS Test Site SIR lists mandatory reporting data the FAA requires to better understand the safety and operational environment for UAS, but none of this mandatory data is directly relevant to privacy issues.

We would suggest that the FAA develop and require test sites to implement a standard battery of privacy-relevant tests that each UAS operating within a test site should have to perform in order to collect data that the FAA can use to make decisions about privacy issues. For example, certain types of sensors such as forward-looking infrared (FLIR), hyperspectral imaging and synthetic aperture radar (SAR) are capable of data collection that is far beyond the intuition or expectations of the public. Establishing mock testing environments — such as a fake home — to see what kinds of surveillance packages, under specific settings and environmental conditions, may be capable of invasive data collection would help inform future regulatory efforts by the FAA, other agencies, and Congress.

VI. Conclusion

We thank the FAA for engaging with privacy issues involved with incorporating UAS into the NAS, and seeking public comment. We also urge the FAA to consider the comments of other public interest organizations, including the Electronic Frontier Foundation, the American Civil Liberties Union, and the Electronic Privacy Information Center, in designing the implementation of the UAS program. We are available to provide further input as needed.

Respectfully submitted,

/s/

Justin Brookman
Joseph Lorenzo Hall
G.S. Hans
Center for Democracy & Technology
jbrookman@cdt.org
jhall@cdt.org
ghans@cdt.org

[15] In October 2012, the University of North Dakota set up the first research compliance committee, a kind of review board to address the social issues raised by drones, like security of private data." *See* Matthew Wald, *Just Don't Call It a Drone*, N.Y. TIMES (Feb. 1, 2013) at ED10, *available at* http://www.nytimes.com/2013/02/03/education/edlife/universities-offer-degrees-in-unmanned-aircraft-systems.html.