



**PUBLIC COMMENTS OF THE ELECTRONIC FRONTIER FOUNDATION
REGARDING PROPOSED PRIVACY REQUIREMENTS FOR THE
UNMANNED AIRCRAFT SYSTEM TEST SITE PROGRAM**

Docket No: FAA-2013-0061

78 Fed. Reg. 12259

Submitted on April 23, 2013 to the Federal Aviation Administration

The Electronic Frontier Foundation (EFF) welcomes the FAA's interest in privacy in unmanned aircraft systems and is grateful for the agency's invitation to comment.

EFF is a non-profit organization that has worked for more than 20 years to protect civil liberties, privacy, consumer interests, and innovation in new technologies. EFF actively encourages and challenges the executive and judiciary to support privacy and safeguard individual rights as emerging technologies become more prevalent in society. Our organization has, for the last few years, been extensively involved in privacy and civil liberties issues raised by unmanned aircraft, commonly referred to as drones.¹ This work has included consulting with state and federal legislators on legislation that would place appropriate limits on law enforcement's abilities to use drones for surveillance; commenting on government and private use of drones on EFF's website, in the press, and in other public fora; and obtaining, reporting on and making accessible to the public drone authorization records received from the FAA pursuant to the Freedom of Information Act.²

With more than 21,000 contributing members and over 179,000 mailing-list subscribers, EFF is a leading voice in the global and national effort to ensure that fundamental liberties are respected in the digital environment.

I. SUMMARY

Unmanned aircraft systems—often called UAS, UAV or drones—are quickly becoming integrated into our society. This is due in equal parts to legislative and executive branch efforts

¹ For links to EFF's drone-related blog posts, press releases, press quotes, and news analysis, as well as unmanned aircraft documents received through open government requests, *see generally* "Drone Flights in the U.S.," *EFF.org*, <https://www.eff.org/foia/faa-drone-authorizations>.

² *See* Jennifer Lynch, "Are Drones Watching You?" *EFF.org* (Jan. 10, 2012) <https://www.eff.org/deeplinks/2012/01/drones-are-watching-you>.

*EFF's Comments Regarding Proposed Privacy Requirements
for the FAA's UAS Test Site Program*

to speed up UAS integration into the National Airspace;³ federal, state and local law enforcement needs to expand surveillance capabilities while cutting costs; industry efforts to sell military-developed technology to the domestic market;⁴ and municipal, corporate, and private interests in using drones for purposes as varied as news-gathering, cinematography, fire-fighting, and crop management.⁵ The FAA has predicted that, in addition to the hundreds of drones currently used domestically by the military and law enforcement, there will be between 7,500 to 10,000 commercial drones flying in the US skies in just five years,⁶ while the federal Joint Planning and Development Office notes industry projections put the number of US drones at more than 15,000 by 2018.⁷

While UAS may be capable of providing benefits to society, they also present significant privacy and civil liberties risks. UAS are capable of highly advanced and near-constant surveillance through live-feed video cameras, thermal imaging, communications intercept capabilities, and backend software tools such as license plate recognition, GPS tracking, and facial recognition. They can amass large amounts of data on private citizens, which can then be linked to data collected by the government and private companies in other contexts.

The FAA has recognized these privacy concerns,⁸ and the Proposed Privacy Requirements for UAS test site operators are a good first step in addressing them. However, the Proposed Requirements do not go far enough. To ensure that the FAA creates rules that adequately protect privacy, both in the UAS test site program and as the agency expands UAS authorizations throughout the country in the coming years, EFF respectfully urges the FAA to address the concerns set forth below and to review and revise its Proposed Requirements and the data reporting requirements listed in Appendix B of the Other Transaction Agreement (OTR) to

³ See FAA Modernization and Reform Act of 2012, Pub. L. 112-95; Gary Martin & Viveca Novek, "Push to Step up Domestic Use of Drones," *SF Chronicle* (Nov. 27, 2012) <http://www.sfgate.com/nation/article/Push-to-step-up-domestic-use-of-drones-4064482.php>.

⁴ Martin & Novek, "Push to Step up Domestic Use of Drones," *SF Chronicle*; Jill Replogle, "The Drone Makers and their Friends in Washington," *KPBS* (April 11, 2013) <http://www.kpbs.org/news/2012/jul/05/drone-makers-friends-washington/>.

⁵ Sara Sorcher, "What Drones Can Do for You," *National Journal* (April 11, 2013) <http://www.nationaljournal.com/magazine/what-drones-can-do-for-you-20130411>.

⁶ FAA Aerospace Forecast Fiscal Years 2012-2032: Unmanned Aircraft Systems, available at http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2012-2032/media/Unmanned%20Aircraft%20Systems.pdf; FAA Aerospace Forecast Fiscal Years 2012-2032: Unmanned Aircraft Systems, available at http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2013-2033/media/Unmanned_Aircraft_Systems.pdf. The FAA notes that the Teal Group, an aerospace and defense industry analyst organization, has predicted that worldwide UAS spending in the next ten years will reach \$89.1 billion. *Id.*

⁷ *Operating Unmanned Aircraft Systems in 2018 and Beyond: NextGen Challenges and Opportunities*, Joint Planning & Development Office (Jan. 4, 2011) <http://www.jpdo.gov/newsarticle.asp?id=146>.

⁸ Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 12259 (Proposed Feb. 22, 2013) (to be codified at 14 C.F.R. pt. 91) <https://federalregister.gov/a/2013-03897>.

incorporate the suggestions proposed by EFF, ACLU, the Electronic Privacy Information Center (EPIC), the Center for Democracy & Technology (CDT), and other privacy advocates.

Specifically, EFF recommends that the FAA:

- (1) Develop and provide a model privacy policy for test site operators;
- (2) Add additional types of privacy-specific data to its data collection and reporting requirements;
- (3) Require test site operators to conduct privacy-specific tests;
- (4) Incorporate privacy protections developed through the FAA's test site program throughout the FAA's unmanned aircraft authorization process; and
- (5) Make drone flight data available and easily accessible to the public.

II. Unmanned Aircraft's Impact on Americans' Privacy and Civil Liberties

Up until a few years ago, most Americans didn't know much about drones or unmanned aircraft. However, the U.S. military has been using modern drones in its various wars and conflicts around the world for nearly 20 years,⁹ using the Predator drone for the first time in Bosnia in 1995, and the Global Hawk drone in Afghanistan in 2001.¹⁰ In the Iraq and Afghanistan wars, the US military has used several different types of drones to conduct surveillance for every major mission in the war. In Libya, President Obama authorized the use of armed Predator drones, even though the United States was not technically at war with the country.¹¹ And in Yemen, the CIA used drones carrying Hellfire missiles to kill three American citizens, including the cleric Anwar al-Awlaki and his 16-year-old son.¹² By the end of 2011, almost one in three U.S. warplanes was a drone, according to the Congressional Research Service.¹³ In 2005, that number was only 5%.¹⁴

⁹ The U.S. military has been researching and employing various forms of unmanned aerial vehicles since 1912. See Jeremiah Gertler, *U.S. Unmanned Aerial Systems*, 1, Congressional Research Service, (Jan. 3, 2012) available at <http://www.fas.org/sgp/crs/natsec/R42136.pdf>.

¹⁰ Eric Scmitt, "In the Skies Over Iraq, Silent Observers Become Futuristic Weapons," *NY Times* (April 18, 2003) <http://www.nytimes.com/2003/04/18/world/nation-war-military-aircraft-skies-over-iraq-silent-observers-become-futuristic.html>; Gerry Gilmore, "Joint STARS, Global Hawk Afghanistan-Bound, Official Says," *American Forces Press Service* (Nov. 2, 2001) <http://www.defense.gov/news/newsarticle.aspx?id=44494>.

¹¹ "Obama Approves Use of Predator Drones in Libya," *Fox News* (Apr. 21, 2011) <http://www.foxnews.com/politics/2011/04/21/obama-approves-use-predator-drones-libya/>.

¹² Mark Mazzetti, et al. "Two-Year Manhunt Led to Killing of Awlaki in Yemen," *NY Times* (Sept. 30, 2011) <http://www.nytimes.com/2011/10/01/world/middleeast/anwar-al-awlaki-is-killed-in-yemen.html>.

¹³ Gertler, *U.S. Unmanned Aerial Systems* at 9.

*EFF's Comments Regarding Proposed Privacy Requirements
for the FAA's UAS Test Site Program*

Now drones are also being used domestically for non-military purposes, raising significant privacy concerns. For example, U.S. Customs and Border Protection (CBP) currently has 10 drones and a contract with General Atomics to purchase at least 14 more within the next few years.¹⁵ It uses these drones inside the United States to patrol borders, and also uses them to aid state and local police for routine law enforcement purposes, such as rousting out cattle rustlers in North Dakota.¹⁶ As EFF has learned through its Freedom of Information Act (FOIA) litigation seeking access to the FAA's drone records,¹⁷ state and local police are also using drones for routine law enforcement activities from catching drug dealers to finding missing persons.¹⁸ Some within law enforcement have even proposed using drones to record traffic violations.¹⁹

As the FAA has recognized, UAS are “inherently different from manned aircraft.”²⁰ This is due to three major factors, including drone design, cost, and surveillance capabilities. Drones have no human pilot on board, are remotely operated, and can be programmed to fly a specific predetermined route and detect and accommodate for flight variables. Some drones are capable of staying in the air for 16-24 hours at a time²¹ and can be refueled from the air, fueled by the sun, or recharged by lasers from the ground.²² Without a pilot on board, there is little need for

¹⁴ *Id.*

¹⁵ Trevor Timm, “Homeland Security Wants to More Than Double Its Predator Drone Fleet Inside the US, Despite Safety and Privacy Concerns,” *EFF.org* (Nov. 20, 2012) <https://www.eff.org/deeplinks/2012/11/homeland-security-wants-more-double-its-predator-drone-fleet-inside-us-despite>.

¹⁶ Brian Bennett, “Police employ Predator Drone Spy Planes on Home Front,” *LA Times* (Dec. 11, 2011) <http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211>. The *Times* quoted local police as saying they “have used two unarmed Predators based at Grand Forks Air Force Base to fly at least two dozen surveillance flights since June.”

¹⁷ EFF filed two FOIA requests for records related to the UAS Certificates of Authorization (COAs)—the licenses issued to public entities and universities wishing to fly drones—and has been litigating these requests for over a year. See “Who Is Flying Unmanned Aircraft in the U.S.?” *EFF.org* (Jan. 10, 2012) <https://www.eff.org/press/releases/who-flying-unmanned-aircraft-us>; “EFF Demands Answers About Predator Drone Flights in the U.S.” *EFF.org* (Oct. 31, 2012) <https://www.eff.org/press/releases/eff-demands-answers-about-predator-drone-flights-us>.

¹⁸ Jennifer Lynch, “Newly Released Drone Records Reveal Extensive Military Flights in US,” *EFF.org* (Dec. 5, 2012) <https://www.eff.org/deeplinks/2012/12/newly-released-drone-records-reveal-extensive-military-flights-us>; Jennifer Lynch, “These Drones are Made for Watchin’,” *EFF.org* (Aug. 16, 2012) <https://www.eff.org/deeplinks/2012/08/these-drones-are-made-watchin>

¹⁹ Peter Finn, “Domestic use of aerial drones by law enforcement likely to prompt privacy debate,” *Wash. Post* (Jan. 23, 2011) <http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html>.

²⁰ Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 12259.

²¹ “A160 Hummingbird: Boeing’s Variable-Rotor VTUAV,” *Defense Industry Daily* (July 4, 2012) <http://www.defenseindustrydaily.com/a160-hummingbird-boeings-variable-rotor-vtuav-03989/>.

²² “Unstaffed Drone Refuelling Test ‘Successful,’” *BBC News* (Oct. 8, 2012) <http://www.bbc.co.uk/news/technology-19871063>; David Ferris, “This Solar-Powered Drone Will Watch You All Day,” (Aug. 16, 2012) *Forbes* <http://www.forbes.com/sites/davidferris/2012/08/16/this-solar-powered-drone-will->

these drones to land. Other drones may not stay in the air as long but, due to their small size and maneuverability,²³ can fly and land in areas where no manned plane or helicopter ever could.

Cost is one of the largest delineators between manned and unmanned aircraft. Where a single helicopter might cost a police department \$500,000-\$3 million to purchase and several hundred dollars an hour to fly, a drone can be purchased and maintained for hundreds of thousands less.²⁴

Drone surveillance capabilities have expanded exponentially in the last few years as the military has increasingly relied on drones in all aspects of the wars overseas, pushing the technology forward. Drones can carry various types of equipment including live-feed video cameras, infrared cameras, heat sensors, chemical and biological sensors, and radar.²⁵ Some newer drones, flying at altitudes above 20,000 feet, can carry super high resolution “gigapixel” cameras²⁶ that can monitor all activity within an entire city, tracking multiple people and vehicles at one time.²⁷ Drones can eavesdrop on electronic transmissions,²⁸ can crack Wi-Fi networks and can intercept text messages and cell phone conversations²⁹—without the knowledge or help of either the communications provider or the customer. Drones, by virtue of

watch-you-all-day/; Mark Brown, “Lockheed Uses Ground-Based Laser to Recharge Drone Midflight,” *Wired UK* (July 12, 2012) <http://www.wired.co.uk/news/archive/2012-07/12/lockheed-lasers>.

²³ Jennifer Lynch, “Newly Released Drone Records Reveal Extensive Military Flights in US,” *EFF.org* (Dec. 5, 2012) <https://www.eff.org/deeplinks/2012/12/newly-released-drone-records-reveal-extensive-military-flights-us>.

²⁴ See, e.g., March 2, 2012 Email from Aviel Sanchez at Miami-Dade Police Department to EFF noting that “One [of Miami-Dade’s drones] was purchased through a Department of Justice (DOJ) grant at the cost of approximately \$100k, and the other is leased from the Honeywell Corporation at the cost of one dollar.” https://www.eff.org/sites/default/files/filenode/MDPD_Email_re_Drone_Program.pdf. Hobbyists can purchase drones at retail outlets for as little as \$300. See, e.g., <http://www.brookstone.com/parrot-ar-drone-2-quadricopter>. These can then be outfitted with a Go Pro camera costing only \$300 more: Matthew Wald, “Drone Cameras May Be High Worry, but They’re Not High Tech,” *NY Times Bits Blog* (March 21, 2013) <http://bits.blogs.nytimes.com/2013/03/21/drone-cameras-may-be-high-worry-but-theyre-not-high-tech/>.

²⁵ Brian Bennett, “Police employ Predator Drone Spy Planes on Home Front.”

²⁶ Andrew Munchbach, “US Army's A160 Hummingbird drone-copter to don 1.8 gigapixel camera,” *Engadget* (Dec. 27, 2011) <http://www.engadget.com/2011/12/27/us-armys-a160-hummingbird-drone-copter-to-don-1-8-gigapixel-cam/>.

²⁷ Paul Szoldra, “Drone Spying Capabilities Are About To Take Another Huge Leap,” *Business Insider* (Jan. 29, 2013) <http://www.businessinsider.com/darpa-argus-mega-camera-most-detailed-surveillance-camera-in-world-2013-1>.

²⁸ Greg Miller, “CIA Flew Stealth Drones into Pakistan to Monitor Bin Laden House” *Wash. Post* (May 17, 2011) http://www.washingtonpost.com/world/national-security/cia-flew-stealth-drones-into-pakistan-to-monitor-bin-laden-house/2011/05/13/AF5dW55G_story.html.

²⁹ Andy Greenberg, “Flying Drone Can Crack Wi-Fi Networks, Snoop On Cell Phones,” *Forbes* (July 28, 2011) <http://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/>.

their design, their size, how high or low they can fly,³⁰ and their surveillance capabilities can operate undetected in urban and rural environments, allowing the government, and, in the future, commercial entities, to spy on Americans without their knowledge.

Americans and their legislators have become increasingly concerned about UAS flights and have pushed back on unregulated drone use. Legislation restricting drone use has been introduced in Congress and in more than 30 states,³¹ and Congress members have repeatedly called on the FAA, Department of Homeland Security and other federal agencies to address the privacy issues implicated by UAS.³²

The FAA is in a unique position to protect Americans' privacy interests from UAS surveillance. All applications to fly drones must go through the agency for approval, and the agency already has a system in place and an office dedicated to reviewing and approving Certificate of Authorization (COA) applications. The FAA could and should incorporate privacy reporting requirements into this process and could use the test site program as a model.

And while the agency has not had the opportunity to address privacy concerns with other aircraft systems in the past, this should not stop it from doing so now and in the future. The FAA can draw on the experience of agencies both within and outside the Department of Transportation, including the National Highway Traffic Safety Administration's (NHTSA) recent efforts to address privacy and electronic data recorders in cars,³³ the Department of Homeland Security's Privacy Office, which works with each of its components "to ensure that privacy considerations are addressed when planning or updating any program, system or

³⁰ John Whitehead, "Roaches, Mosquitoes and Birds: The Coming Micro-Drone Revolution," *Huffington Post* (April 17, 2013) http://www.huffingtonpost.com/john-w-whitehead/micro-drones_b_3084965.html. Compare DARPA's Nano Hummingbird drone, which can fly in and out of buildings with the Zephyr or Solar Eagle drones, which are designed to fly in the stratosphere. See Jason Paur, "Video: Hummingbird Drone Does Loop-de-Loop," *Wired Danger Room* (Feb. 18, 2011); John Villasenor, "High-Altitude Surveillance Drones: Coming to a Sky Near You," *Scientific American Blog* (Feb. 24, 2012) <http://blogs.scientificamerican.com/guest-blog/2012/02/24/high-altitude-surveillance-drones-coming-to-a-sky-near-you/>.

³¹ See "Markey Drone Privacy Legislation to Prevent Flying Robots from Becoming Spying Robots" (March 19, 2013) <http://markey.house.gov/press-release/markey-drone-privacy-legislation-prevent-flying-robots-becoming-spying-robots>; Allie Bohm, "Drone Legislation: What's Being Proposed in the States?," *ACLU* (March 6, 2013) <http://www.aclu.org/blog/technology-and-liberty-national-security/drone-legislation-whats-being-proposed-states>.

³² "McCaul Hearing Exposes Vulnerability of Drones in US Airspace," (July 19, 2012) <http://mccaul.house.gov/press-releases/mccaul-hearing-exposes-vulnerability-of-drones-in-us-airspace/>; "Leahy: Judiciary Committee Will Hold Two Hearings On Drones" (March 13, 2013) <http://www.leahy.senate.gov/press/leahy-judiciary-committee-will-hold-two-hearings-on-drones>.

³³ See "Mandatory Black Boxes in Cars Raise Privacy Questions," *EFF.org* (Feb. 11, 2013) <https://www.eff.org/press/releases/mandatory-black-boxes-cars-raise-privacy-questions>.

initiative,³⁴ and Department of Justice's Office of Privacy and Civil Liberties, which does the same for Department of Justice components.³⁵

III. Incorporating Privacy Protections into the UAS Test Site Process and Beyond

The FAA has recognized that drone flights raise privacy issues and has taken a small first step in addressing those issues by proposing the Privacy Requirements for UAS test site operators. However, these Proposed Requirements do not go far enough. EFF recommends the agency incorporate the following five measures to further protect privacy.

First, the Proposed Requirements themselves are too vague and limited to provide much privacy protection. The FAA should, at a minimum, flesh out actual privacy rules and provide a model policy for test site operators to follow. These rules could be based in part on the Fair Information Practices (FIPs), as the FAA has proposed, but should also highlight the most important practices within the FIPs and should demonstrate how test site operators can craft FIPs-based and Constitutionally-compliant rules specific for UAS.

Second, the FAA should add additional types of data to its data collection and reporting requirements laid out in Appendix B to the Other Transaction Agreement (OTA).³⁶ Currently these reporting requirements are focused on design and flight capabilities of the unmanned aircraft and the training and capabilities of the pilot and crew. However, they should be expanded to include data surveillance capabilities of the specific drones operating at the test sites and on the actual data collected by the drone.

Third, the FAA should require drone operators at test sites to conduct specific tests related to surveillance and privacy. Test site operators could design the sites—perhaps by creating fake houses or businesses—to allow drone operators to test how accurate their surveillance systems are and test how much data those systems collect. This is especially important for surveillance capabilities that exceed the understanding of most members of the public, such as hyperspectral imaging, synthetic aperture radar (SAR), and forward-looking infrared (FLIR).³⁷

³⁴ DHS, *About the Privacy Office*, <http://www.dhs.gov/about-privacy-office>.

³⁵ Department of Justice, Office of Privacy & Civil Liberties, *Mission*, <http://www.justice.gov/opcl/>.

³⁶ See “Other Transaction Agreement (OTA) Memorandum of Agreement Between Federal Aviation Administration and (To Be Determined - TBD)” (hereinafter “Draft OTA”) (Feb. 14, 2013) *available at* <https://faaco.faa.gov/index.cfm/attachment/download/29581>.

³⁷ Joe Pappalardo, “Hyperspectral Sensors: The Flying Eyes that See the Invisible,” *Popular Mechanics* (June 28, 2011) <http://www.popularmechanics.com/technology/military/planes-uavs/hyperspectral-sensors-the-flying-eyes-that-see-the-invisible>; “Synthetic Aperture Radar: “Round the Clock Reconnaissance” *Lockhead Martin*, <http://www.lockheedmartin.com/us/100years/stories/sar.html>.

Fourth, the FAA should not limit its reach to the test site program but should incorporate reporting requirements proposed here and by other privacy organizations into the current Certificate of Authorization application process so that all drone operators are required to consider, specifically address and mitigate the privacy risks inherent in drone use.

Finally, the FAA must establish a simple way for the public to access the wealth of data on drone flights that has been and will be collected by the agency, test site operators, and individual drone operators. For too long, the public has been kept in the dark about drone flights in the United States and abroad. The only way Americans and their legislators can properly assess privacy issues raised by drone flights is if the FAA—the agency with access to most drone data collected and produced in the United States—makes that data available to the public.

A. The FAA's Proposed Privacy Requirements are Vague and Limited

The FAA has proposed five Privacy Requirements that would apply to UAS Test Site Operators. These include:

1. the operator must have privacy policies that govern all activities at the site;
2. these privacy policies must be publicly available;
3. the site operator must set up a way to receive and consider comments on the privacy policies;
4. the Fair Information Practice Principles should inform the privacy policies; and
5. the privacy policies should be updated regularly

The Proposed Requirements also state that the site operator must comply with federal, state and local rules regarding individuals' privacy rights, that any future legislation relating to UAS operation will be incorporated into this requirement, and that the transmission of data from the site operator to the FAA must only include data listed in Appendix B of the Other Transaction Agreement (OTR).³⁸

However, other than these somewhat vague and limited privacy requirements, the FAA has not provided much information to site operators on how to protect privacy. The FAA could go much further. For example, at a minimum, the FAA should develop a draft privacy policy that could be used as a model by test site operators. The FAA could also require that all drone proponents operating at the test site produce and follow their own individual privacy policies. And the FAA could require that all entities applying for an authorization to fly a drone—even outside of the test site program—be required to do the same.

³⁸ *Draft OTA* at 24-31.

B. FIPs-Based Privacy Principles

The FAA has noted that test site operators' privacy policies must be informed by the Fair Information Practices (FIPs). Originally developed as eight principles by the Organization for Economic Co-operation and Development (OECD),³⁹ the FIPs were later incorporated into the Privacy Act of 1974, 5 U.S.C. § 552a, and have been adopted and promoted by many federal agencies, including the Department of Homeland Security,⁴⁰ the Federal Trade Commission,⁴¹ the Department of Health & Human Services and others.⁴²

C. Privacy Principles Necessary to Protect Against Excessive UAS Surveillance

Any program that protects civil liberties and privacy from unnecessary drone surveillance must include FIPs-based principles. However, the traditional formulation of the FIPs, especially if it relies on voluntary efforts instead of enforcement, may not provide enough privacy protections. Further, any drones flown by government entities or state actors must also comply with all constitutional limitations under the First, Fourth, Fifth and Fourteenth Amendments.⁴³ In light of this, EFF proposes the following principles to regulate drone surveillance, some of which may be implemented by the FAA alone, and some of which may require further legislative action.

Limit Data Collection—Data collected by UASs should be limited to the minimum necessary to achieve the government or drone proponent's stated purpose and targeted not to exceed Constitutional and other limitations in state and federal laws like the Electronic Communications Privacy Act and state paparazzi and wiretap laws.

Define Clear Rules on the Legal Process Required for Data Collection—Data collected by law enforcement should be subject to clear rules on when it may be collected and which specific legal process—such as a warrant—is required prior to collection. Collection and retention should be specifically disallowed without legal process unless the collection falls under a few very limited and defined exceptions. For example, clear rules should be defined to govern

³⁹ Organization for Economic Co-operation and Development, OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data (1980) available at http://www.oecd.org/document/18/0,3343,en_2649_34255_1815186_1_1_1_1,00.html.

⁴⁰ See Hugo Teufel III, Chief Privacy Officer, DHS, Mem. No. 2008-01, Privacy Policy Guidance Memorandum (Dec. 29, 2008), available at http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf

⁴¹ Fair Information Practice Principles, Fed. Trade Commission, <http://www.ftc.gov/reports/privacy3/fairinfo.shtm> (last modified June 25, 2007).

⁴² See Robert Gellman, "FAIR INFORMATION PRACTICES: A Basic History," (Nov. 12, 2012) available at <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf>

⁴³ As a government-sponsored program, where the goal is for private and public entity drone and test site operators to work with the FAA to develop standards to "support the FAA's development of the regulatory body needed for UAS," *Draft OTA* at 5, it is arguable that even non-government entities could be considered state actors subject to constitutional limitations.

when law enforcement agencies may use drones to surveil people walking around in spaces traditionally considered to be public.

Limit the Amount and Type of Data Stored—Rules should be set to limit the amount of data stored, and drone operators should be required to employ techniques to avoid over-collection of data, such as scrubbing the images of faces from video footage if those faces are not central to an investigation.

Limit the Combination of Data—Drone operators should not combine data collected for one purpose—such as data gathered for a commercial database—with data collected by the UAS. This increases the potential for tracking and surveillance and should be avoided or limited to specific individual investigations.

Limit Data Retention—Data retention periods should be clearly defined and should be limited to no longer than necessary to achieve the goals of the program. Data that is deemed to be “safe” from a privacy perspective today could become highly identifying tomorrow. For example, a data set that includes crowd images could become much more identifying as technology improves. Similarly, data that was separate and siloed or unjoinable today might be easily joinable tomorrow. For this reason retention should be limited, and there should be clear and simple methods for a person to request removal of his or her data from the system.

Define Clear Rules for Use and Sharing—Data collected for one purpose should not be used for another purpose. For example, a drone used to conduct environmental monitoring may, as a byproduct of that monitoring, also collect data on people living in the area. That data should not automatically be used or shared with another agency to use in a criminal context.

Enact Robust Security Procedures to Avoid Data Compromise—Data compromise is a risk in any system. Using traditional security procedures, such as basic access controls that require strong passwords and exclude unauthorized users, as well as encrypting data transmitted throughout the system, is paramount.

Mandate Notice Procedures—Because of the real risk with drones that data on people will be collected without their knowledge, rules should define clear notice requirements to alert people to the fact that their data has been collected. The notice provision should also make clear how long the data will be stored and how to request its removal from the database.

Define and Standardize Audit Trails and Accountability Throughout the System—All transactions, including data collection, access to and searches of the system, and data transmission, should be logged and recorded in a way that assures accountability. Privacy and security impact assessments, including independent certification of device design and accuracy, should be conducted regularly.

Ensure Independent Oversight—every entity that uses a drone to conduct surveillance or collect data must be subject to meaningful oversight from an independent entity, and individuals

whose data has been collected by a drone and later compromised should have a strong and meaningful private right of action.

IV. Thinking Beyond Privacy Policies

Requiring UAS test site operators to maintain privacy policies is an important first step, but it doesn't go far enough. As researchers have noted, most people do not read privacy policies, and, even though many Americans think that having a privacy policy means a company will protect individuals' privacy interests, many companies treat privacy policies as a means to enable data collection rather than restrict it.⁴⁴ The FAA can better protect privacy by incorporating it into the standards it will be working with the test site operators to develop.

The FAA and Congress have said that the goal of test sites is to create a program that will investigate ways to safely integrate UAS into the National Airspace (NAS).⁴⁵ As part of this goal, the FAA, in conjunction with the test site operators, plans to develop a "body of standards for the [UAS] platform, operators, and flight operations" and will ask site operators to "perform research and development activities to test and evaluate such standards and submit data and resulting reports to the FAA."⁴⁶ This body of standards and the research and development activities necessary to develop those standards must address privacy.

The test sites should be viewed as incubators for data collection practices that can be rolled out throughout the drone industry. As such, test site operators should be tasked with collecting privacy-related data in addition to other data they are will be required to collect and produce to the FAA. Currently the data the FAA plans to require⁴⁷—like the data the agency currently requires COA applicants to submit—is generally limited to the design and flight capabilities of the aircraft and the training and capabilities of the pilot and crew. However, this could be expanded, both through the reporting requirements currently proposed in the OTA and by broadening those requirements.

A. Expanding the Data Reporting Requirements in Appendix B to the Draft Other Transaction Agreement

OTA Appendix B, Section 2.15 requires the site operator to record and provide to the FAA data on many aspects of an unmanned aircraft system, including its "Payload Type." UAS payloads include surveillance equipment such as video cameras, thermal imaging, radar systems that can penetrate foliage, communications intercept capabilities, and even weapons. And many

⁴⁴ See, e.g., Aleecia M. McDonald and Lorrie Faith Cranor, "The Cost of Reading Privacy Policies," *I/S: A Journal of Law and Policy for the Information Society*, 2008 Privacy Year in Review, *available at* <http://www.aleecia.com/authors-drafts/readingPolicyCost-AV.pdf>.

⁴⁵ *Draft OTA* at 5; FAA Modernization and Reform Act of 2012.

⁴⁶ *Id.*

⁴⁷ See *Draft OTA*, Appendix B.

drones are designed to have their payloads swapped out to accommodate the specific needs of the drone operator at the time. Currently COA applicants are required to report payload data to the FAA. However, as we've seen in records received in response to our FOIA litigation, these reports can vary widely.⁴⁸

The payload data that test site operators and UAS operators should be required to provide to the FAA needs to do three things: 1) it needs to be specific to the actual drone flown at the site; 2) it needs to discuss the capabilities of that model of drone as a whole; and 3) it needs to provide specific information on the data the payload is capable of collecting. For example, it should include more than just whether the payload incorporates a camera but must also include the type of camera, its accuracy, and how much footage it can store on the drone itself or can transmit back to the "base." To ensure this, EFF recommends that the FAA specify in Appendix B to the OTA exactly what payload data the site operator and the UAS operator should be required to provide.

B. Requiring Data Collection Statements

The FAA's test site data reporting requirements must be broader than this however. They also must include information on what types of data the specific UAS operating at the site is collecting and is capable of collecting. Senators Markey and Barton recently introduced drone legislation can serve as a model. This legislation, called the "Drone Aircraft Privacy and Transparency Act of 2013"⁴⁹ requires that all drone operators produce a "data collection statement." This statement is similar to and overlaps in parts with a FIPs-based privacy policy, but also includes several drone-specific categories.⁵⁰ For example, it would require an assessment of the UAS's impact on individuals' privacy. It would also include data on whether the UAS will collect information about individuals or groups of individuals, and if so the kinds of data that would be collected. Other data that should be collected include: the specific areas where the UAS will operate; what entity and which pilot will be flying the UAS and, if applicable, whether the flight will be on behalf of a different entity; how long the UAS will fly for each flight; and the purpose for each flight.

V. CONCLUSION

EFF respectfully urges the FAA to adopt EFF's recommendations along with the recommendations of other privacy advocates, including CDT, EPIC, and ACLU. Specifically, EFF recommends (1) the FAA develop and provide a model privacy policy to test site operators;

⁴⁸ See generally FAA COA documents released in response to EFF's FOIA request, *available at* <https://www.eff.org/foia/faa-drone-authorizations>.

⁴⁹ *Available at* <http://www.govtrack.us/congress/bills/113/hr1262/text>.

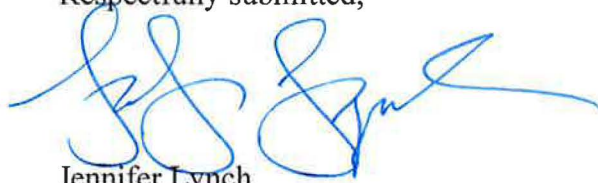
⁵⁰ The proposed data collection statement includes several FIPs-based reporting requirements, including reporting on how that data would be used and handled; who the data would be shared with; how the amount of data collected would be minimized; how long the data would be retained; and when and how the data would be destroyed.

*EFF's Comments Regarding Proposed Privacy Requirements
for the FAA's UAS Test Site Program*

(2) add additional types of privacy-specific data to its data collection and reporting requirements; (3) require test site operators to conduct privacy-related tests; 4) incorporate privacy protections developed through the FAA's test site program throughout the FAA's UAS application approval process; and (5) make drone flight data easily available to the public.

With the data collected and generated at the UAS test sites, the FAA—and the American public and its legislators—will learn much more about how drones operate, what data they are capable of collecting, and for how long that data can be stored. This will, in turn, allow each to make important decisions about how to place appropriate limitations on drone use.

Respectfully submitted,



Jennifer Lynch
Staff Attorney
Electronic Frontier Foundation

April 23, 2013