



Steven D. Benjamin
President

President

Steven D. Benjamin Richmond, VA

President-Elect

Jerry J. Cox Mount Vernon, KY

First Vice President

Theodore Simon Philadelphia, PA

Second Vice President

E. G. Morris Austin, TX

Treasurer

John Wesley Hall Little Rock, AR

Secretary

Barry J. Pollack Washington, DC

Immediate Past President

Lisa Monet Wayne Denver, CO

Parliamentarian

Vicki H. Young San Francisco, CA

Directors

Chris Adams Charleston, SC
Brian H. Bieber Coral Gables, FL
Andrew S. Birrell Minneapolis, MN
Alexander Bunin Houston, TX
Ellen C. Brotman Philadelphia, PA
William H. Buckman Moorestown, NJ
Ramon De La Cabada Miami, FL
Jean-Jacques Cabou Phoenix, AZ
Jay Clark Cincinnati, OH
Josh A. Cohen San Francisco, CA
Anthony Cotton Waukesha, WI
Aric M. Cramer St. George, UT
Candace C. Crouse Cincinnati, OH
Paul DeWolfe Baltimore, MD
Drew Findling Atlanta, GA
Richard K. Gilbert Washington, DC
Nina J. Ginsberg Alexandria, VA
Elissa Heinrichs Newtown, PA
Michael Heiskell Fort Worth, TX
Bonnie Hoffman Leesburg, VA
Richard S. Jaffe Birmingham, AL
Ashish S. Joshi Ann Arbor, MI
Nellie L. King West Palm Beach, FL
Benjamin R. Labranche Baton Rouge, LA
Tracy Miner Boston, MA
Tyrone Moncriffe Houston, TX
Norman R. Mueller Denver, CO
George H. Newman Philadelphia, PA
Timothy P. O'Toole Washington, DC
Maria H. Sandoval San Juan, PR
Melinda Sarafa New York, NY
David Smith Alexandria, VA
Jeffrey E. Thoma Fairfield, CA
Geneva Vanderhorst Washington, DC
Christopher A. Wellborn Rock Hill, SC
Steven M. Wells Anchorage, AK
Christie N. Williams Dallas, TX
William P. Wolf Chicago, IL

Executive Director

Norman L. Reimer Washington, DC

April 23, 2013

Docket Operations, M – 30
U.S. Department of Transportation
1200 New Jersey Avenue, SE
Room W12-140, West Building Ground Floor
Washington, DC 20590-0001

Re: Federal Aviation Administration: “Unmanned Aircraft System Test Site Program,” Docket No. FAA-2013-0061

The National Association of Criminal Defense Lawyers (NACDL) respectfully submits the following comments to the Federal Aviation Administration (FAA) in response to the Request for Comments on the FAA’s proposed approach for addressing the privacy questions raised by the operation of unmanned aircraft systems within the test site program. In February 2012, NACDL joined dozens of civil liberties groups in a petition organized by the Electronic Privacy Information Center urging the FAA to “conduct a rulemaking to address the threat to privacy and civil liberties that will result from the deployment of aerial drones within the United States.”¹ NACDL applauds the FAA for taking the first step in requesting comments on the privacy implications raised within the test site program, and we look forward to ongoing conversations about the privacy and civil liberties impact of this new technology as the Administration moves forward with its mandate to integrate unmanned aircraft systems into the National Airspace System.

NACDL is a nonprofit organization committed to ensuring justice and due process for all persons accused of crime, fostering the integrity, independence and expertise of the criminal defense profession, and promoting the proper and fair administration of criminal justice. Such a policy respects cherished civil rights and liberties that are fundamental to our democracy. Citizens have a right to expect privacy in their homes, vehicles, and communications, and a right not to be deprived of their liberty or property without due process of law. To further these guiding principles, NACDL’s Fourth Amendment Committee, which is comprised of leading Fourth Amendment experts from across the country, issued a white paper entitled *Electronic Surveillance & Government Access to Third Party*

¹ Available at <http://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=23746&libID=23715>.

Records in February 2012.² This report was followed by the recent release of model legislation for local, state, and federal governments interested in protecting citizens' from unwarranted law enforcement use of unmanned aircraft (also known as "drones").³

While the FAA traditionally views its mandate as being outside the context of the protection of constitutional rights, the Supreme Court has held otherwise. In relevant cases on law enforcement use of manned aircraft, like helicopters and airplanes, the Court relied heavily on then existing FAA regulations regarding the appropriate flying level of these aircraft to determine the defendants' expectation of privacy.⁴

Thankfully, the Constitution is the floor of our rights, not the ceiling, and the government can always provide more protection than what the Constitution mandates. NACDL believes that it is first the responsibility of the FAA to undergo proposed rulemaking and comment periods to provide for the best privacy protections it can before these unmanned aircrafts take flight. The inclusion of the privacy protections in the required Other Transaction Agreement (OTA) is a good first step, but it is by no means sufficient to protect citizens' Fourth Amendment rights. Additionally, requiring that Fair Information Practice Principles (FIPPs) inform the privacy policies of the Site Operators and requiring their operation in accordance with existing Federal, state, and other laws are helpful mandates, but woefully inadequate to keep people safe from unreasonable and unwarranted searches and seizures. These comments will address two specific FIPPs—use limitation and data minimization—in addition to explaining why these privacy principles must be applied to private use of unmanned aircraft as well as law enforcement use.

Use Limitation

Any use of surveillance drones at soon to be determined test sites, must only collect data for the purpose specified in the notice—"to develop a body of data and operational experiences to inform integration and the safe operation of these aircraft in the National Airspace System." Test sites should not be used for official government surveillance, and no data obtained from a surveillance drone used at a test site should be shared with law enforcement for the purpose of investigating or prosecuting a crime. NACDL believes that, with limited and specific exceptions, the Government of the United States, whether Federal, state or local, should not be permitted to use an unmanned aircraft for surveillance of a person, or personal or business property within the United States to gather evidence or other information pertaining to criminal

² Available at http://www.nacdl.org/reports/thirdpartyrecords/thirdpartyrecords_pdf/.

³ Available at <http://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=26568&libID=26537>.

⁴ See *California v. Ciraolo*, 476 U.S. 207 (1986) (holding that because the airplane flew at an altitude of 1000 feet, as permitted by FAA regulations, when law enforcement officers observed marijuana growing in the defendant's backyard, the defendant's backyard was in "public view" and the defendant had no reasonable expectation of privacy in his backyard from this altitude); *Dow Chemical Co., v. United States*, 476 U.S. 227 (1986) (holding that "open areas of an industrial plant complex are not analogous to the 'curtilage' of a dwelling for purposes of aerial surveillance"; therefore, the use of an airplane to conduct surveillance of an industrial plant was not a search under the Fourth Amendment); *Florida v. Riley*, 488 U.S. 445 (1989) (holding that because officers were well within navigable airspace under FAA regulations, law enforcement's use of a helicopter to view marijuana plants through a crack in the defendant's greenhouse roof was not a search under the Fourth Amendment).

conduct, or conduct in violation of a statute or regulation, without first securing a warrant based on probable cause. Test site surveillance should be off limits to law enforcement entities, and, moving forward, the rule for law enforcement use of unmanned aircraft must be prohibition of such use except with a warrant.⁵

Even though the Supreme Court has already approved the use of manned aircraft to conduct surveillance in certain circumstances, the FAA can and should protect citizens Fourth Amendment rights against unwarranted use of unmanned aircraft. This will not take away existing law enforcement tools to conduct surveillance. Yes, manned aircraft are more expensive than unmanned aircraft, and yes, law enforcement has limited resources, but this lack of resources acts as an extra check on law enforcement's ability to conduct mass surveillance and collect massive amounts of data that are irrelevant to the investigation of an existing crime. Law enforcement has the tools it needs to adequately protect citizens and to investigate and prosecute crimes.

Unmanned aircrafts may be outfitted with surveillance equipment to include high resolution cameras, thermal heat imaging devices, and geolocation tracking devices. The Supreme Court is already skeptical about law enforcement's use of these technologies, which permit law enforcement to know what is taking place within a person's home without ever stepping foot into that home, or to create a picture of what a person's day to day life may look like, aside from gathering evidence of crime. In *Kyllo v. United States*, the Supreme Court held that the use of a thermal heat imaging device to detect a marijuana grow house constituted a search under the Fourth Amendment.⁶ The Court reasoned that the police used a device not in "general public use" to gather information about the inside of a home that they otherwise could not detect. Then, eleven years later in *United States v. Jones*, a unanimous Court held that the attachment of a GPS device to a defendant's car was a trespass and therefore constituted a search under the Fourth Amendment.⁷ Most important to the analysis of what the Court might decide about law enforcement use of drones, however, are the concurring opinions of Justice Sotomayor and Justice Alito, which discuss long-term monitoring of a suspect's movements. Under the "mosaic theory," which is a collection of numerous pieces of data which create a large mosaic picture, constitutional concerns may exist, especially in light of the technology that is available to be utilized by drones, like facial recognition, continuous video recording, etc.

Data Minimization

The FAA and test site operators should only collect data that is directly relevant and necessary to accomplish the specified purpose outlined in the notice—"to develop a body of data

⁵ The Fourth Amendment Committee agreed on limited exceptions to this warrant requirement, including exigent circumstances to include instances when a law enforcement agency possesses reasonable suspicion that absent swift preventative action, there is an imminent danger to life or bodily harm; or during an environmental or weather related catastrophe to preserve public safety, protect property, and conduct surveillance for the assessment and evaluation of environmental or weather related damage, erosion, flood or contamination during a lawfully declared state of emergency.

⁶ *Kyllo v. United States*, 533 U.S. 27 (2001).

⁷ *United States v. Jones*, 132 S. Ct. 945 (2012).

and operational experiences to inform integration and the safe operation of these aircraft in the National Airspace System,” and only retain that data for as long as is necessary to fulfill this specified purpose. This minimization requirement must be placed on drone operators as well as the government in order to protect citizens’ Fourth Amendment and privacy rights, both at the test sites and moving forward to into general use.

Current law does not adequately protect citizens’ privacy rights. The FAA has a responsibility to regulate beyond FIPPs and existing privacy laws. The Fourth Amendment Committee’s report on law enforcement access to third party records demonstrates the many ways law enforcement can dodge Fourth Amendment warrant requirements by reaching out to private entities to gather information that law enforcement would otherwise need a warrant to secure. Third party records are records that are created and stored by private companies in the ordinary course of business. Banking information and telephone call information are two traditional examples of third party records. In *Miller v. United States* and *Smith v. Maryland*, the Supreme Court held that individuals have no reasonable expectation of privacy in such records due to the fact that they are maintained and accessible to a third party such as the bank or telephone company.⁸ By revealing one’s affairs to another, reasoned the Court, a person “assume[s] the risk” that the company would reveal that information to the government.⁹ This is known as the “third-party doctrine.”

Today, third party records include copies of all email messages, geolocation information, cell-site location information, and every website one visits and the search terms used to find those sites, which are often created without the user’s knowledge and can reveal highly personal and private information. Surveillance drones used by private entities have the potential to generate such personal and private information, and a person’s privacy interests in such information must not be automatically waived without his or her consent and shared with the government. It is this premise, “that an individual has no reasonable expectation of privacy in information voluntarily disclosed to third parties,” that Justice Sotomayor took issue with in the *Jones* case. She opined that “[t]his approach is ill suited to the digital age, in which people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks.”¹⁰

The FAA must be aware of existing jurisprudence and regulate at least in accordance with the constitutionally mandated floor; however, NACDL urges the FAA to provide greater privacy protections than are currently mandated by statute and case law. Again, with regard to test sites, test site surveillance should be off limits to law enforcement entities. Moving forward to more general use, law enforcement must be required to obtain a warrant for data collected and held by a third-party. Drone technology is evolving so rapidly, it is difficult to discern exactly what kind of private data may be collected by the government and private entities. The government should not be given an end run around the Fourth Amendment simply because the technology is developing faster than the law.

⁸ *United States v. Miller*, 425 U.S. 435 (1976), *Smith v. Maryland*, 442 U.S. 735 (1979).

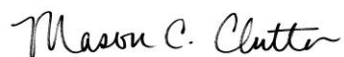
⁹ *Smith*, 442 U.S. at 744.

¹⁰ *Jones*, 132 S. Ct. at 957.

Conclusion

NACDL commends the FAA for issuing the Request for Comments on privacy questions raised with regard to the operation of unmanned aircraft systems within the test site program. We encourage you to implement the above suggestions pertaining to data minimization and use limitations, while recognizing that implementation of FIPPs and existing privacy law, while a good first step, is inadequate to protect privacy and civil liberties. We agree with the FAA that “the privacy policies should be updated as necessary to remain operationally current and effective,” and believe that our recommendations are a step in that direction. Given the rapid development of drone technology and technologies that can be utilized by drones, it is imperative that the FAA observe this commitment to update the privacy policies during the test site program and in the future when drones are in general use in the National Airspace System.

Respectfully Submitted,



National Association of Criminal Defense Lawyers
Mason C. Clutter
National Security and Privacy Counsel
1660 L Street NW, 12th Floor
Washington, DC 20036