Comments of the National Association of Criminal Defense Lawyers
On the Interim Study re Unmanned Aerial Vehicles
To the Oklahoma House of Representatives
September 24, 2013

The National Association of Criminal Defense Lawyers (NACDL) respectfully submits the following comments to the Oklahoma House of Representatives in response to the Interim Study to address the privacy questions raised by the operation of unmanned aircraft systems, also known as drones, in Oklahoma. NACDL has an Oklahoma State affiliate, the Oklahoma Criminal Defense Lawyers Association.[1] NACDL applauds the House of Representatives for taking the first step in studying the privacy implications raised by the use of domestic surveillance drones, and we look forward to ongoing conversations about the privacy and civil liberties impact of this new technology as you move forward with the study.

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 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 drones.[3] Finally, NACDL maintains the Domestic Drone Information Center, a one-stop-shop for all things drones, including pending state legislation, scholarship, events of interest, and case law.[4]

The increasing number of bills introduced in states across the country addressing the use of domestic surveillance drones signal that not only are states concerned with intrusive government surveillance of their citizens without a warrant, but that domestic drone use is becoming more prevalent as the technology advances, signaling a sudden need for legislation. There are major Fourth Amendment and privacy implications that come with the use of drones in the United States, and the threats to privacy and civil liberties need to be properly addressed in any new drone legislation. Many outdated statutes are applied today in the digital age that undercut Fourth Amendment rights, and new regulations need to address the concerns surrounding these rapidly advancing surveillance tools.

Traditionally, the Constitution is the floor of our rights, not the ceiling, and the states can always provide more protection than what the federal Constitution mandates. NACDL believes

---

[1] http://www.ocdlaoklahoma.com/

[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] *Available at* http://www.nacdl.org/domesticdrones.

that states should provide for the best privacy protections they can before these unmanned aircrafts take flight. Privacy protections must be applied to private use of unmanned aircraft as well as law enforcement use. These comments outline a few of NACDL's recommendations. NACDL's complete model drone legislation is attached to the end of these comments.

Prohibited Use Without a Warrant and Suppression of Evidence

If drones are used by a person or entity of the government or funded in any way by the government, a warrant should be required for any surveillance of a person within a state, county, or municipality. A warrant should also be required for the surveillance of personal or business property located within the state to gather evidence or other information pertaining to criminal conduct or conduct in violation of a statute or regulation, except in certain special circumstances. This prevents unwanted government intrusion into privacy, and protects Fourth Amendment and state privacy rights.

Even though the Supreme Court has already approved the use of manned aircraft to conduct surveillance in certain circumstances, Oklahoma 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 already 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. 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 without a warrant constituted a search under the Fourth Amendment. 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.

Traditionally, an exception to the warrant requirement exists for evidence that is found in "plain view." The plain view doctrine becomes muddled, however, when drones are used because drones have high-tech capabilities, that are not in the "general public use," to conduct surveillance on areas in plain view and not in plain view, such as the inside of a home. The technology is evolving so rapidly that it is currently difficult to discern exactly what kind of private data may be collected by the government and private entities using domestic surveillance drones.

Additionally, any evidence obtained in violation of drone legislation should be inadmissible in a criminal trial. It is important that a suppression remedy be included in state drone legislation, otherwise the only recourse an individual could have is civil, which does not benefit a defendant facing criminal charges. A warrant requirement may be toothless without such a suppression remedy.

Limit Exigent Circumstances

Reasonable exceptions to a warrant requirement for the use of a surveillance drone could include exigent circumstances or the assessment of an environmental or weather related catastrophe. Exigent circumstances exist when law enforcement possesses reasonable suspicion that absent swift preventative action there is an imminent danger to life or imminent risk of threat or bodily harm. This should further be limited for use only until the danger and risk that prompted the use of the drone are no longer imminent.

The Third Party Problem

Current law does not adequately protect citizens' privacy rights. NACDL's 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 by and accessible to a third party such as the bank or telephone company. 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. This is known as the "third-party doctrine."

Today, third party records include copies of email messages, geolocation information, cell-site location information, and the websites 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."

As all states can do, some states have provided greater protection than what the federal Constitution affords to third party records. Such protections may be found in legislation, court cases, or even state constitutions. NACDL encourages the House of Representatives to consider including such protections in future drone legislation. Law enforcement should 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.

Conclusion

NACDL commends the House of Representatives for undertaking an interim study on privacy questions raised with regard to the operation of unmanned aircraft systems in Oklahoma. We encourage you to consider the above suggestions. Given the rapid development of drone technology and technologies that can be utilized by drones, it is imperative that privacy protections be in place before the drones take flight.

113TH CONGRESS
1ST SESSION

BILL NUMBER

[Purpose]: To protect individual privacy against unwarranted governmental intrusion through the use of unmanned aerial systems commonly called drones, and for other purposes.

IN THE [CHAMBER] OF THE UNITED STATES

DATE
Xx introduced the following bill; which was read twice and referred to the Committee on the Judiciary

---

A BILL

To protect individual privacy against unwarranted governmental intrusion through the use of unmanned aerial systems commonly called drones, and for other purposes.

Be it enacted by the Senate and House of Representatives of the United States of America in Congress assembled,

SECTION 1. SHORT TITLE.

This Act may be cited as the "[Insert Short Title"]

SECTION 2. DEFINITIONS.

In this Act---

(a) the term "unmanned aircraft" means any aircraft that is operated without the possibility of direct human intervention from within or on the aircraft (as defined in section 331 of the FAA Modernization and Reform Act of 2012 (49 U.S.C. 40101 note). and
(b) the term "law enforcement agency" means a person or entity authorized by law, or funded by the Government of the United States, to investigate or prosecute offenses against the United States.
(c) the term "unmanned aircraft system" means an unmanned aircraft and associated elements (including communication links and the components that control the unmanned aircraft) that are required for the pilot in command to operate safely and efficiently in the national airspace system.

(d) the term "anti-personnel device" means any projectile, chemical substance, electrical or directed-energy emission, whether visible or invisible, designed to harm, incapacitate, or otherwise negatively impact a human being.

SEC. 3. PROHIBITED USE OF UNMANNED AIRCRAFT SYSTEMS

Except as provided in section 4, a person or entity acting under the authority, or funded in whole or in part by, the Government of the United States shall not use an unmanned aircraft for surveillance of a person within the United States or for the surveillance of personal or business property located within the borders of the United States to gather evidence or other information pertaining to criminal conduct or conduct in violation of a statute or regulation except to the extent authorized in a warrant that satisfies the requirements of the Fourth Amendment to the Constitution of the United States.

SEC. 4. EXCEPTIONS

This Act does not prohibit any use of an unmanned aircraft for surveillance during the course of the following:

(a) PATROL OF NATIONAL BORDERS - The use of an unmanned aircraft to patrol within 25 miles of a national border for purposes of policing the border to prevent or deter illegal entry of any persons, illegal substances, or contraband.

(b) EXIGENT CIRCUMSTANCES - The use of an unmanned aircraft by a law enforcement agency is permitted when exigent circumstances exist. For the purposes of this paragraph, exigent circumstances exist when a law enforcement agency possesses reasonable suspicion that absent swift preventative action, there is an imminent danger to life or imminent risk of threat of bodily harm.

(c) DURING AN ENVIRONMENTAL OR WEATHER RELATED CATASTROPHE – The use of an unmanned aircraft by federal and state authorities 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.

SEC. 5. PROHIBITED SURVEILLANCE UNDER THIS ACT

This Act prohibits any use of an unmanned aircraft for the following:

(a) USE OF FORCE - No Federal agency may authorize the domestic use, including granting a permit for use, of an unmanned aircraft while armed with a lethal weapon or anti-personnel device.

(b) DOMESTIC USE IN PRIVATE SURVEILLANCE - No Federal agency may authorize the domestic use, including granting a permit for use, of an unmanned aircraft

to permit any private person to conduct surveillance upon any other private person without the express, informed consent of the private person or persons to be made subject to surveillance, or the owner or lessee of any real property on which that other private person is present.

(c) SURVEILLANCE OF THE EXERCISE OF 1ST AMMENDMENT RIGHTS - No Federal agency may authorize the domestic use, including granting a permit for use, of an unmanned aircraft for the purpose of the surveillance of persons engaged in the lawful exercise of First Amendment rights and or the Right of Freedom of Assembly.

SEC. 6. REMEDIES FOR VIOLATION.

Any aggrieved party may in a civil action obtain all appropriate relief to prevent or remedy a violation of this Act.

SEC. 7. PROHIBITIONS ON THE CONDUCT OF UNMANNED AIRCRAFT SURVEILLANCE AND THE USE OF ACQUIRED SURVEILLANCE AS EVIDENCE.

This Act prohibits the following:

(a) No evidence obtained or collected in violation of this Act may be admissible as evidence in a criminal prosecution during trial, at sentencing, before a grand jury, as rebuttal evidence, or during administrative hearings in any court of law in the United States.

(b) No imaging or other forms of observational data gathered by unmanned aircraft surveillance from or concerning the parties or places subjected to surveillance in violation of this Act may be preserved by law enforcement or government agencies for any purpose unless required by a Federal Court.

(c) No imaging or any other forms of data lawfully obtained under this Act for which there is not a reasonable and articulable suspicion that such images or data contain evidence of a crime, or are relevant to an ongoing investigation or trial, may be retained for more than 90 days, unless such retention is attendant to general agency guidelines regarding the retention of evidence in criminal cases. In such cases, the imaging or other data may not be distributed to agencies, entities, or individuals where such distribution is not necessary to meet general agency guidelines regarding the retention of evidence in criminal cases. A court order must be obtained before imaging or other forms of data may be retained lawfully for more than 90 days.

(d) No unmanned aircraft may conduct any type of surveillance that would violate Federal laws regarding the interception of aural communications, electronic communications and transmissions, personal location data, or the acquisition of video or still images of a person or conditions existing within a home or place without first obtaining all required warrants in compliance with the Federal or state statutes applying to such interceptions.

SEC. 8. DOCUMENTATION OF DRONE SURVEILLANCE

(a) All use of unmanned aircraft for surveillance shall be documented by the person or entity authorized to conduct the surveillance. All surveillance flights shall be documented as to:

(i) duration, flight path;
(ii) mission objectives, and
(iii) the names of places or persons authorized to be subject to surveillance.

(b) This flight information noted will be certified as accurate and complete by the supervising person authorized by a court to conduct the surveillance.

(c) This flight information must be retained for a period of five years.

(d) Persons seeking relief before a court of law or an administrative agency who have been a target of unmanned aircraft surveillance may obtain by proper motion to the court all information relating to them acquired in the course of such surveillance, excepting only the operational capabilities of the unmanned aircraft, unmanned aircraft system, and other operational information strictly related to the technical conduct and physical security of the surveillance operation.