



UAS Privacy Considerations

Unmanned Aircraft Systems (UAS) are emerging technologies that have the potential to transform America by providing wide ranging economic, environmental, safety, and security benefits. A recent studyⁱ by the Association for Unmanned Vehicle Systems International conservatively estimates that 103,776 high paying jobs could be created and state tax revenue could exceed \$482 million by 2025. They believe that every year the integration of UAS into the aviation systemⁱⁱ is delayed, America will lose more than \$10 billion in potential economic impact.

UAS applications and benefits include assisting these civil government and commercial tasks: emergency deployment at accident scenes, search and rescue, barricade situations, structure or other fire emergencies, terror threats, firefighting, chemical and HAZMAT detection, crop dusting, agricultural development, monitoring of pollution, pipelines, wildlife, traffic, and floods, aerial news coverage, delivering medical supplies to remote areas, aerial photography, forensic photography, real-estate photography, filmmaking, communications, broadcasting, Arctic and volcanic research, damage assessment, cargo transportation, port, border, and event security, etc. In addition to these direct benefits, UAS implementation has the potential to spawn many new industries and provide an incredible array of manufacturing, operation, and other high paying job opportunities.

Along with these benefits come concerns about individual privacy. There is an existing body of federal, state and local law relating to privacy. The question is whether existing law is adequate, absent extensive judicial review, to alleviate the concerns of state legislators and citizens regarding privacy rights in light of this new technology. Because this technology can use a variety of sensors and some can potentially loiter for long periods of time without detection, there is a concern that government can use these systems to monitor individuals in a way that was not imagined in Supreme Court 4th Amendment rulings based on the presumption of privacyⁱⁱⁱ. Because state law interacts with Federal 4th Amendment rulings, states may choose to enact legislation addressing this issue. The challenge is to provide privacy protection while allowing the use of UAS to achieve UAS' many benefits, as described above.

Because of the complexity of this issue and the importance of privacy to citizens in every state, representatives of the Aerospace States Association (ASA)^{iv}, the Council of State Governments (CSG)^v, and the National Conference of State Legislatures (NCSL)^{vi}, have joined together to create considerations for states to evaluate in developing UAS legislation. As part of our impartial deliberative process, UAS privacy stakeholder associations including the ACLU, EPIC, and IACP Aviation Committee^{vii}, AUVSI – the industry trade association^{viii} – as well as academics^{ix} responded to our request to submit their suggestions for state privacy legislation to an independent law firm, Cadwalader, Wickersham & Taft LLP^x. These submissions can be seen at <http://aerostates.org/events/uas-privacy-submissions>. Our review also included the Congressional Research Service's report, "Integration of Drones into Domestic Airspace: Selected Legal Issues," from April 4, 2013, and a memorandum for the Secretary from the Office of Civil Rights and Civil Liberties, U.S. Department of Homeland Security, dated September 14, 2012. After deliberation, ASA, CSG, and NCSL provide the following considerations:

1. Warrants: States may consider requiring a warrant for government surveillance of an individual or their property where the individual is specifically targeted for surveillance in advance without their permission. All other observation activities should not require a warrant, to the extent allowed under Supreme Court rulings. Additionally, if there is not a specific person identified for surveillance in advance, it is generally not possible to obtain a warrant. Requiring one would eliminate UAS benefits, but can be addressed per recommendation number two, below.
2. Data Concerns: Some are worried about government use of data derived from warrantless observations. States may consider addressing this by prohibiting the repurposing of data collected from Government use of UAS in warrantless observation unless a warrant allows the repurposing.
3. States may consider prohibiting commercial UAS and model aircraft flights from tracking specific, identifiable individuals without their consent.
4. States can consider prohibiting weapons to be carried by any UAS in commercial airspace.
5. States may consider endorsing the International Association of Chiefs of Police Aviation Committee (IACP) "Recommended Guidelines for the use of Unmanned Aircraftⁱ." These guidelines define UAS and provide guidance for community engagement, system requirements, operational procedures, and image retention for UAS operations by law enforcement organizations.
6. States may consider emphasizing that the FAA regulates commercial UASⁱⁱ, and that they and model aircraft operations should be operated in a manner not to present a nuisance to people or property.

End Notes

ⁱ Economic Impact of Unmanned Aircraft Systems in the United States, March 2013, <http://www.auvsi.org/econreport>

ⁱⁱ The Federal Aviation Administration regulates all civil airspace, vehicles, and operators within the U.S. for safety and efficient airspace use through federal preemption. UAS safety regulations are being developed by the FAA. Until such regulations are in place, civil UAS operations must be specifically approved by the FAA. Government operations must comply with civil air traffic control directives. A lack of FAA permissive regulation and state prohibitions of UAS use delay integration of UAS into the aviation system and adversely affect America's global competitiveness in the development of this industry.

ⁱⁱⁱ The crucial inquiry for Fourth Amendment protection is whether a person has a reasonable expectation of privacy that society is prepared to recognize. Courts have found that individuals may have a Fourth Amendment right against the unreasonable search and seizure of the area surrounding a house, referred to as the "curtilage." The Supreme Court has found that aerial surveillance over private property does not violate the Fourth Amendment if conducted by an aircraft in legally navigable airspace.

However, UAV's can fly lower, often undetected, and this holding might not apply to UAVs and their unique capabilities, and arguably remains an open question.

^{iv} ASA is a bipartisan organization that represents the grassroots of American aerospace. It is a 501(c)(3) scientific and educational organization of lieutenant governors, governor-appointed delegates, and associate members from industry and academia. ASA was formed to promote a state-based perspective in federal aerospace policy development and to support education outreach and economic development opportunities.

^v Founded in 1933, The Council of State Governments is our nation's only organization serving all three branches of state government. CSG is a region-based forum that fosters the exchange of insights and ideas to help state officials shape public policy. This offers unparalleled regional, national and international opportunities to network, develop leaders, collaborate and create problem-solving partnerships.

^{vi} The National Conference of State Legislatures is a bipartisan organization that serves the legislators and staffs of the nation's 50 states, its commonwealths and territories. NCSL provides research, technical assistance and opportunities for policymakers to exchange ideas on the most pressing state issues. NCSL is an effective and respected advocate for the interests of state governments before Congress and federal agencies.

^{vii} In response to our request for information, papers were received from the Airborne Law Enforcement Association (including and referencing the guidelines from the International Association of Chiefs of Police Aviation Committee), the American Civil Liberties Union, the American Legislative Exchange Council, the Electronic Frontier Foundation, the Electronic Privacy Information Center and the National Association of Criminal Defense Lawyers.

^{viii} The Association for Unmanned Vehicle Systems International is the world's largest non-profit organization devoted exclusively to advancing the unmanned systems and robotics community. Serving more than 7,500 members from government organizations, industry and academia, AUVSI is committed to fostering, developing, and promoting unmanned systems and robotic technologies. AUVSI members support defense, civil and commercial sectors.

^{ix} Douglas Marshall of New Mexico State University and Paul Voss of Smith College responded to our requests.

^x Cadwalader, Wickersham & Taft LLP, established in 1792, is one of the world's leading international law firms, with offices in New York, Washington, D.C., Charlotte, Houston, London, Hong Kong, Beijing and Brussels. Cadwalader has provided pro bono legal services to ASA for over 20 years.

^{xi} http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf

^{xii} Code of Federal Regulations Title 14, as amended.



The Aerospace States Association

107 S. West Street, Suite 510, Alexandria, VA 22314
Tel: (202) 257-4872 E-mail: AerospaceStates@comcast.net

Alabama

Alaska

Arizona

Arkansas

California

Colorado

Connecticut

Delaware

Florida

Georgia

Guam

Hawaii

Idaho

Illinois

Indiana

Iowa

Kansas

Kentucky

Louisiana

Maine

Maryland

Massachusetts

Michigan

Minnesota

Mississippi

Missouri

Montana

Nebraska

Nevada

New Hampshire

New Jersey

New Mexico

New York

North Carolina

North Dakota

Ohio

Oklahoma

Oregon

Pennsylvania

Puerto Rico

Rhode Island

South Carolina

South Dakota

Tennessee

Texas

Utah

Vermont

Virginia

Washington

West Virginia

Wisconsin

Wyoming

May 3, 2013

Ms. Allie Bohm, American Civil Liberties Union

Dear Allie,

I am writing to invite you to join with the Aerospace States Association (ASA), the Council of State Governments (CSG), and the National Conference of State Legislatures (NCSL) in an important and timely dialogue on privacy issues related to incorporating Unmanned Aircraft Systems (UAS) into the national airspace.

I believe we all view privacy as a serious issue that our constituents are concerned about, yet we also see the long-term benefits in the use of unmanned aircraft for carrying out missions that are otherwise dirty, dull or dangerous. Commercial use could also create high paying jobs and environmental benefits that could transform our economy.

Many states have begun drafting legislation to address the privacy concerns related to UAS. We want to give thorough, thoughtful consideration to all sides of the issues in order to develop suggested legislation for consideration by the states.

Please be a part of this effort by reviewing the attached plan we've developed and **submitting your comments to Bob Davis by Email to bob.davis@cwt.com, fax to 202-862-2400 or mailed by post to Cadwalader, 700 6th Street, NW, Suite 300, Washington, DC 20001 by June 1.** Your submission should address civil, commercial and personal use of UAS and contain your views on the "assumption of privacy" in UAS use. Your submission should not exceed three pages. An independent law firm, Cadwalader, Wickersham & Taft LLP, and leaders of state government associations will review your submission and draft best practices and suggested legislation based on your comments, to be presented at a roundtable discussion in Washington, D.C. on August 14. You are invited to participate in the roundtable to personally discuss the results of our drafting effort.

Thank you for your leadership, and for taking the time to participate in this dialogue.

Sincerely,

Mead Treadwell
Lieutenant Governor, State of Alaska
Chair, Aerospace States Association



May 30, 2013

Bob Davis
Cadwalader
700 6th Street, NW, Suite 300
Washington, DC 20001

Dear Mr. Davis:

On behalf of the American Civil Liberties Union (ACLU), a non-partisan organization with more than a half million members, countless additional activists and supporters, and fifty-three affiliates nationwide, we appreciate the opportunity to comment on the privacy and civil liberties implications of domestic use of unmanned aircraft systems (UAS), also known as drones, and to recommend new protections for use of the technology.

Like any powerful surveillance tool, UAS have the potential to be used for good or ill. With implementation of good privacy ground rules, we can enjoy the benefits of this technology without bringing our country closer to a "surveillance society" in which every move is monitored, tracked, recorded, and scrutinized by the authorities.

UAS share some characteristics with manned aerial surveillance, such as planes and helicopters, but their threat to privacy is substantially greater in both scope and volume. Manned aircraft are expensive to purchase, operate, and maintain. They require trained pilots and ground crews and must land in order for pilots to rest. The expense both in dollars and in staffing has always imposed a natural limit on the government's aerial surveillance capacity. UAS's low cost and flexibility erode that natural limit. As technology improves, small, hovering devices will be able to explore hidden spaces, peer in windows, or even, potentially, enter homes, and large static blimps will enable continuous, long-term monitoring – all for much less than the cost of a helicopter or plane.

In our society, it is a core principle that the government does not collect information about individuals' innocent activities just in case they do something wrong. But UAS threaten to turn that principle on its head. What would be the effect on our society if everyone felt the keen eye of the government at all times? Psychologists have repeatedly found that people who are being observed tend to behave differently than when they are not being watched. This effect is so great that a recent study found that "merely hanging up posters of staring human eyes is enough to significantly change people's behavior."¹ There is a real danger that, if faced with the prospect of unregulated UAS, people will change how they behave in public – whether at a political rally or in their own backyards.

¹ Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," *Scientific American*, May 3, 2011, online at <http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person>; M. Ryan Calo, "People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship," 114 Penn St. L. Rev. 809, online at <http://www.pennstatelawreview.org/articles/114/114%20Penn%20St.%20L.%20Rev.%20809.pdf>.

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

UAS may also suffer from the problems we've seen with video surveillance – voyeurism,² racial profiling by operators,³ and automated law enforcement.⁴

The Supreme Court has not yet had occasion to consider whether the Fourth Amendment places limits on government use of UAS. However, it has allowed some warrantless aerial surveillance from *manned* aircraft. Most notably, in the 1986 decision *California v. Ciraolo*, the Court ruled that there was no intrusion into Ciraolo's privacy when police borrowed an airplane, flew it over his backyard and spotted marijuana plants growing there, because "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."⁵

Nonetheless, because of their potential for pervasive use and their capacity for revealing far more than the naked eye, there are good reasons to believe that UAS may implicate Fourth Amendment rights in ways that manned flights do not. In both *Dow Chemical Co. v. United States*⁶ and *Kyllo v. United States*,⁷ the Supreme Court suggested that using sophisticated technology not generally available to the public may be considered a search under the Fourth Amendment.

Further, the Supreme Court has suggested that the continuous use of a surveillance technology may heighten Fourth Amendment concerns. In *United States v. Knotts*, although the Court concluded that the use of the beeper in that case did not violate the Fourth Amendment, it held that if "such dragnet type law enforcement practices" as "twenty-four hour surveillance of any citizen of this country" ever arose, it would determine if different constitutional principles would be applicable.⁸ Similarly, in *United States v. Jones*, five justices agreed (in two concurrences) that when the government engages in prolonged location tracking, it conducts a search under the Fourth Amendment.⁹ While this decision may eventually play a role in regulating drone usage, the technology is moving far more rapidly than our jurisprudence, and it is critical that state legislatures act to protect their constituents' privacy.

State legislation should reflect the following key principles:

First, no one should be spied upon unless the government believes that person has committed a crime. Drone use over private property should occur only with a search warrant based on probable cause – the same standard used to search someone's house or business. It might be permissible to monitor individuals in public at a lower standard – perhaps reasonable suspicion – but the key is to prevent mass, suspicionless searches of

² "Did NYPD Cameras Invade A Couple's Privacy?" WCBS-TV report, Feb. 24, 2005, video no longer available online; Jim Dwyer, "Police Video Caught a Couple's Intimate Moment on a Manhattan Rooftop," *New York Times*, Dec. 22, 2005, online at <http://www.nytimes.com/2005/12/22/nyregion/22rooftop.html>.

³ Clive Norris and Gary Armstrong, "The Unforgiving Eye: CCTV Surveillance in Public Spaces," Centre for Criminology and Criminal Justice at Hull University, 1997.

⁴ Danielle Keats Citron, "Technological Due Process," 85 *Washington University Law Review* 1249 (2008), online at <http://lawreview.wustl.edu/inprint/85/6/Citron.pdf>.

⁵ 476 U.S. 207 (1986).

⁶ 476 U.S. 227 (1986).

⁷ 533 U.S. 27 (2001).

⁸ 460 U.S. 276, 283-84 (1983).

⁹ 132 S. Ct. at 964 (Alito, J., concurring in judgment), 955 (Sotomayor, J., concurring).

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

the general population, including for intelligence gathering. Exceptions to this rule should be limited to emergencies connected to life and safety or narrowly drawn administrative exceptions in order to prevent pretextual use of drones.

Additionally, while the Constitution may permit UAS surveillance of public spaces on less than a probable cause standard, the vast majority of the 96 different drone bills being considered in 43 states this legislative session¹⁰ require law enforcement to get a probable cause warrant before using a drone in an investigation, whether that investigation occurs in private or public space, a good indicator that a warrant requirement for drone use is both workable and palatable. Already, warrant requirements have been enacted in Florida,¹¹ Idaho,¹² Montana,¹³ and Tennessee.¹⁴

Second, images of identifiable individuals captured by law enforcement UAS should not be retained or shared unless they are of the target of the investigation that justified drone deployment, and there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.

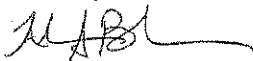
Third, while drone use should be permitted for reasonable non-law enforcement purposes where privacy will not be substantially affected, such as geological inspections or environmental surveys, information collected by drones for one purpose should not be used for another purpose such as general law enforcement or enforcing administrative laws.

Fourth, drones should not carry weapons.

Finally, oversight is crucial. Communities must play a central role in deciding whether to purchase drones, and the policies and procedures for the use of UAS should be explicit and written, and should be subject to public review and comment. Similarly, like any new technology, drone use must be monitored to make sure it's a wise investment that works.

Placing reasonable limitations on law enforcement is by no means a new idea – for example, authorities may take a thermal image of someone's home only when they get a warrant – and it is imperative that we implement a system of rules to ensure that we can take advantage of UAS technology without sacrificing our privacy. If you have any questions, would like to discuss the issue further, or would like to see ACLU's model state legislation, please don't hesitate to reach out to me at abohm@aclu.org or (212) 284-7335.

Sincerely,



Allison S. Bohm, Advocacy & Policy Strategist

¹⁰ "States with UAS Legislation" National Conference of State Legislatures, May 29, 2013. <http://www.ncsl.org/issues-research/justice/unmanned-aerial-vehicles.aspx>.

¹¹ S.B. 92 (Fla. 2013)

¹² S.B. 1134, 62nd Legislature (Idaho 2013)

¹³ S.B. 196, 63rd Legislature (Mont. 2013)

¹⁴ S.B. 796 (Tenn. 2013)

AMERICAN CIVIL LIBERTIES
UNION FOUNDATION
NATIONAL OFFICE
125 BROAD STREET, 18TH FL.
NEW YORK, NY 10004-2400
T/212.549.2500
WWW.ACLU.ORG

OFFICERS AND DIRECTORS
SUSAN N. HERMAN
PRESIDENT

ANTHONY D. ROMERO
EXECUTIVE DIRECTOR

MEMORANDUM

State of Alaska Department of Law

TO: Mead Treadwell
Lieutenant Governor
State of Alaska

DATE: May 20, 2013

FILE NO.: JU2011200514

FROM: Libby Bakalar *gmb*
Assistant Attorney General
Transportation Section

TEL. NO.: 907.465.3600 main
907.465.2520 fax

CC: Jim Cantor
Deputy Attorney General
Department of Law

SUBJECT: Legal issues related to
unmanned aircraft
systems

Margie Vantor
Chief Assistant Attorney General
Department of Law

Michaela Goertzen
Speechwriter
Office of the Lieutenant Governor

I. Introduction and background.

In your capacity as chair of the Aerospace States Association, you asked me to provide you with a brief description and analysis of the core legal issues related to the civilian use of Unmanned Aircraft Systems (UAS), also known as "drones." The context for your inquiry is the University of Alaska's pending application with the Federal Aviation Administration (FAA) to become one of a limited number of testing sites in the nation for UAS. Please note that this document is not legal opinion of the Office of the Attorney General, but rather simply a compendium of my research and a preliminary analysis.

UAS are unmanned aircraft designed to do tasks that are too difficult, dull, dangerous, or expensive for manned aviation, and are designed to carry a "system payload" such as a camera or sensor.¹ Traditionally, UAS have been used for military

¹ Association for Unmanned Vehicle Systems International ("AUVSI"), UAS Privacy Issues Document.

purposes, but they are being increasingly deployed in domestic civilian contexts such as law enforcement, disaster relief, fire-fighting, agriculture, energy, industry, wildlife tracking, and others.² Commercial use of UAS is currently prohibited, but that is expected to change by 2014.³ UAS can range in size from smaller than a cell phone to larger than a commercial jetliner.⁴ Research sponsored by the Association for Unmanned Vehicle Systems International (AUVSI), a non-profit trade association that supports the civilian use of UAS, concluded that the integration of UAS into the national airspace has the potential to create more than 100,000 new jobs and \$82 billion of economic impact by 2025.⁵

The legal issues surrounding the civilian use of UAS relate mainly to privacy and property interests, and are relatively untested in the courts because of the novelty of the technology involved and the regulatory vacuum in which that technology operates. Fortunately, there has been significant legal scholarship as well as congressional reporting⁶ in this area, all of which I rely upon heavily in this memorandum. I have also reviewed all the materials Charles Huettner emailed me after our April 5th teleconference. Some limited case law also exists on the privacy concerns raised by aerial surveillance and similar technologies. These cases telegraph how the Supreme Court might view the privacy implications of UAS. Following is the requested description, summary, and analysis of the issues that have arisen and been analyzed by legal scholars to date. I also discuss the Alaska-specific implications of these issues, which are not discussed in any of the law reviews, journals, or reports.

II. Core legal issues raised by the use of UAS/drones.

The FAA oversees all aircraft operations in the United States and makes and

² See Villasenor, John, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 Harv. J.L. & Pub. Pol'y 458, 459 (2013).

³ *Id.* at 471.

⁴ *Id.* at 465.

⁵ "The Economic Impact of Unmanned Aircraft Systems Integration in the United States," AUVSI, March, 2013.

⁶ See *Integration of Drones into Domestic Airspace: Selected Legal Issues*, Congressional Research Service, CRS Report for Congress (April 4, 2013).

enforces rules to implement and interpret laws passed by Congress governing aviation.⁷ Federal law enacted in February 2012 (The Federal Aviation Administration Modernization and Reform Act of 2012) requires the FAA to devise a comprehensive plan to integrate all civilian UAS into the national airspace system by September 30, 2015, appropriates billions of dollars in funding, and creates the six UAS test sites for which many states, including Alaska, are vying.⁸

The federal government is still struggling with the regulation of UAS, specifically, how to define these vehicles, how to clarify which—if any—existing regulations apply to them, how to craft future regulations to encompass vehicles not governed by existing regulations, and how to ensure that future regulations do not inadvertently regulate other industries such as model or hobby aircraft.⁹ The FAA will need to identify technology (e.g. cameras and radar) that will obviate the need for regulations requiring pilots to “see and avoid” other aircraft, address appropriate training for UAS operators, devise proper procedures for when a UAS loses contact with an operator or is hacked, coordinate with other countries and agencies in adopting regulations, and ensure that there is sufficient wireless spectrum to accommodate the communication needs of these vehicles.¹⁰ Presently, UAS operators engaged in both public aircraft operations and private operations are required to have special certifications from the FAA.¹¹

There is no legislation yet governing UAS in Alaska, although there is model legislation that AUVSI is compiling, and according to news reports, at least one other state—Florida—has begun to legislate UAS. Two bills were introduced in Alaska last session that touch upon UAS: HB 159, “An Act relating to the admissibility of evidence acquired through the use of an unmanned aerial vehicle; establishing a crime for certain uses of unmanned aerial vehicles; and restricting the use of unmanned aerial vehicles for collection of information or investigation by peace officers and other government agents;” and HCR 6, “Recognizing the Alaska Center for Unmanned Aircraft Systems

⁷ Villasenor, *supra* note 2, at 469.

⁸ P.L. No. 112-095 (Feb. 14, 2012).

⁹ See Kapnik, Benjamin, *Unmanned but Accelerating: Navigating the Regulatory and Privacy Challenges of Introducing Unmanned Aircraft into the National Airspace System*, 77 J. Air L. & Com. 439, 443 (2012).

¹⁰ *Id.* at 448-49.

¹¹ Villasenor, *supra* note 2, at 471.

Integration at the University of Alaska Fairbanks as a national leader in unmanned aircraft research and development; and relating to a Task Force on Unmanned Aircraft Systems.” Presumably, these bills could be revisited next session.

Any discussion of UAS legislation must also consider federal pre-emption and the interplay between state and federal law. Although aircraft safety, trade, and noise regulation is the established provenance of the federal government, states may still pass laws governing how aircraft are flown.¹² Both Alaska and federal law prohibit the reckless operation of aircraft, but Alaska could not enact privacy laws that would decrease or implicate in any way the safety of flight operations, such as laws governing aircraft speed or altitude.¹³ From a pre-emption standpoint, the safest area for state legislation is in the realm of privacy laws aimed at non-government actors that address trespass, invasion of privacy, stalking, and harassment, because state power to legislate in this area is well-established.¹⁴

In short, there is both a mandate and pressing need to legislate and regulate UAS at both the state and federal level. However, the precise parameters and scope of that legislation and regulation remain nebulous at best.

III. Constitutional rights.

A. The Fourth Amendment.

Probably the biggest legal issue surrounding UAS is the implications of these devices for individual privacy rights. The Fourth Amendment to the United States Constitution guarantees to the people the right to be free from unreasonable search and seizure by the government.¹⁵ The Alaska Constitution contains an analogous search and seizure provision, as well as an explicit clause guaranteeing to its citizens the right to privacy.¹⁶ Because the FAA is primarily a regulating agency whose mandate is to ensure

¹² Villasenor, *supra* note 2, at 513.

¹³ *Id.*

¹⁴ *Id.*

¹⁵ See U.S. Const. amdt. IV.

¹⁶ Alaska Const. art. I, §§ 14 and 22. Note that these provisions bind only government actors—not private citizens.

the efficient and safe operation of U.S. airspace, questions have arisen whether this agency is really the appropriate entity to ensure that government actors using UAS are not violating these basic constitutional principles or whether constitutional privacy compliance should be spearheaded at the state or federal level by some other agency. It is clear, however, that no government actor may commit such violations.

The crucial inquiry for Fourth Amendment and state constitutional privacy purposes is whether a person has a reasonable expectation of privacy that society is prepared to recognize. One scholar notes that “[w]here a [UAS] captures images that could have been obtained from civilian aircraft traveling in a legally authorized manner, privacy claims are limited. Consumers lack a reasonable expectation of privacy with respect to areas already exposed to civilian over-flights.”¹⁷ However, novel imaging technologies such as thermal and infrared imaging could raise concerns. Indeed, as noted by another scholar who has examined the issue, “[t]he privacy issues raised by the potential ubiquity of [UAS] go beyond the current Fourth Amendment jurisprudence.”¹⁸ Indeed, “[t]here is no precedent that squarely addresses privacy implications of governmental use of a technology that allows essentially permanent, multi-dimensional, multi-sensory surveillance of citizens twenty-four hours a day.”¹⁹

However, there has been some judicial guidance. *Katz v. U.S.*²⁰ was a landmark Fourth Amendment case in which the Supreme Court held for the first time that a Fourth Amendment violation could occur absent a physical intrusion—specifically, through a listening device the police had affixed to the outside of a public phone booth. This was the first “remote sensing” case, soon to be followed by a trilogy of key “aerial surveillance cases.”

The “remote sensing” cases fall into two categories: “open fields” and “curtilage.” Remote sensing in “open fields” does not implicate the Fourth Amendment because open

¹⁷ Geoffrey Christopher Rapp, *Unmanned Aerial Exposure: Civil Liability Concerns Arising from Domestic Law Enforcement Employment of Unmanned Aerial Systems*, 85 N.D.L. Rev. 623, 641 (2009).

¹⁸ Joseph J. Vacek, *Big Brother Will Soon Be Watching—Or Will He?*, 85 N.D. L. Rev. 673, 674 (2009).

¹⁹ *Id.* at 675.

²⁰ 389 U.S. 347 (1967).

fields are areas of public and private property that “do not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from government surveillance or interference.”²¹ However, “curtilage” is a legal “penumbra” surrounding a home where the Fourth Amendment may be implicated.²² Whether a given area constitutes “curtilage” depends on the proximity of the area to the home, whether the area is enclosed, the nature of the use to which the area is put, and the steps taken by the resident to protect the area from observation.²³ Although a person may have reasonable expectations of privacy in curtilage, remote sensing of curtilage “does not require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.”²⁴ The bottom line is that remote sensing will not implicate the Fourth Amendment “if it is done from a public vantage point where law enforcement officers can make open observations.”²⁵

The Supreme Court’s “aerial surveillance” trilogy consists of *California v. Ciraolo*,²⁶ *Florida v. Riley*,²⁷ and *Dow Chemical Company v. U.S.*²⁸ All three cases were decided in the 1980s. Together, they stand for the proposition that aerial surveillance of any kind over private or commercial property from aircraft that are lawfully in navigable airspace is not a Fourth Amendment search, because there is no reasonable expectation of privacy in an area that is openly visible from above, regardless whether the area is curtilage or an open field.²⁹

²¹ *Oliver v. U.S.*, 466 U.S. 170, 179 (1984).

²² *U.S. v. Dunn*, 480 U.S. 294, 300 (1987).

²³ *Id.* at 301.

²⁴ *California v. Ciraolo*, 476 U.S. 207, 213 (1986).

²⁵ *Vacek*, *supra* note 18, at 680.

²⁶ 476 U.S. 207 (1986).

²⁷ 488 U.S. 445 (1989).

²⁸ 476 U.S. 227 (1986).

²⁹ *Vacek*, *supra* note 18, at 682.

In *Ciraolo*, police flew a fixed-wing aircraft 1,000 feet over a defendant's backyard, the minimum safe altitude required by FAA regulations, and observed marijuana plants with the naked eye. The backyard was not visible due to an extensive fencing system, so the aerial search provided the basis for a search warrant and marijuana plants were found after a physical search. The Court held that a ground fence does not create an expectation of privacy to be free from aerial searches because routine flights exposed the backyard to public view.³⁰

Riley reached the same holding when officers flew a helicopter 400 feet overhead to peer through openings in a greenhouse and determined marijuana was growing inside the defendant's fenced-in home. Again, the Court found that there was no reasonable expectation of privacy because helicopter flight in navigable airspace was a routine, expected occurrence.³¹

And in *Dow Chemical*, the Environmental Protection Agency, acting without a warrant, hired a private commercial pilot to fly over Dow's property to take aerial photos of suspected regulatory violations. The Court upheld this conduct because "such an industrial complex is more comparable to an open field and as such it is open to the view and observation of persons in aircraft lawfully in the public airspace."³²

However, decades later in 2001, in *Kyllo v. United States*,³³ the Supreme Court reminded us that the Fourth Amendment protects people—not just places—from unreasonable searches and seizures. *Kyllo* involved law enforcement's warrantless use of thermal imaging to detect unusual amounts of heat radiating from the defendant's home, indicating the presence of marijuana. *Kyllo* held that this surveillance violated the Fourth Amendment because the technology was not in widespread use. Currently, *Kyllo* limits the ability of law enforcement to rely on infrared/thermal imaging technology, but because the Court's decision was directly linked to the prevalence of the technology, it's an open question whether the Court's limitation would persist if these technologies went into more "widespread use." As one scholar put it, "the test seems to turn on whether

³⁰ 476 U.S. at 215.

³¹ 488 U.S. at 450-51.

³² 476 U.S. at 239.

³³ 553 U.S. 27 (2001).

Wal-Mart sells it or not.”³⁴ Such a question would most likely be tested in a criminal context, where the prosecution seeks to admit evidence obtained through the use of these technologies.

Finally, just last year, in *United States v. Jones*,³⁵ the Supreme Court held that the installation of a GPS tracking device on a suspect’s car for eight days constituted a search under the Fourth Amendment. Although *Jones* did not deal with aerial surveillance, the Court held that the placement of the device was a physical intrusion onto private property for the purposes of obtaining information, as well as the extended monitoring of a person in a public space, both of which constituted a Fourth Amendment “search.” Some scholars have predicted that one potential result of *Jones* is that extended UAS surveillance could constitute a search within the meaning of the Fourth Amendment.³⁶

It is clear from a review of the scholarship and the limited case law that the rate of advancement of these technologies often outpaces the ability of courts to rule upon the validity of their use under the Fourth Amendment. The overall conclusion so far is that aerial surveillance by any method, at a legal altitude, is constitutional if the technology is in general public use and does not trespass upon private property for extended periods of time. Still, the legal landscape has been characterized as “an aeronautical Wild West,” and the current regulatory scheme as “inadequate to deal with the novel issues raised” by the use of UAS, particularly by law enforcement.³⁷

In Alaska, we must consider an additional important factor: Article I, section 22 of the Alaska Constitution guarantees an explicit individual right to privacy. There is no state case law interpreting this clause (or any part of the state constitution) in the context of UAS. However, it is highly possible that the Alaska Supreme Court would interpret the right in favor of the individual asserting it as opposed to deferring to the government. For example, our Supreme Court has interpreted the privacy clause to create a constitutional right to privacy in garbage placed for collection, which contrasts with both state and

³⁴ Vacek, *supra* note 18, at 683.

³⁵ 132 S. Ct. 945 (2012).

³⁶ Kapnik, *supra* note 9, at 495.

³⁷ Vacek, *supra* note 18, at 675-77.

federal case law on the Fourth Amendment.³⁸ The take-away point here is that government conduct that complies with the Fourth Amendment under either the state or federal constitution could *nonetheless* violate the state constitutional right to privacy. And in 2002, at least one member of the Alaska Court of Appeals, albeit in a concurring and unreported opinion, expressed constitutional skepticism at law enforcement's surreptitious use of infrared helicopter technology of the type prohibited under *Kyllo* the year before.³⁹

B. The First Amendment & individual privacy.

In addition to the Fourth Amendment implications of government-operated UAS, these vehicles may also implicate the First Amendment rights of private citizens to collect and gather information. One scholar has recently addressed this issue, noting that for private entities and persons not bound by the Fourth Amendment, the key constitutional question is the extent of these persons' First Amendment right to access information.⁴⁰ The Supreme Court long ago held that the First Amendment protects the act of seeking out news, otherwise "freedom of the press could be eviscerated."⁴¹ And at least one circuit court of appeals has recently held that the First Amendment permits a private citizen to record the actions of people in a public space.⁴² Congress could potentially enact laws to protect individuals from intrusive UAS surveillance by private actors, which would be considered in a First Amendment context of the right to gather and receive information.⁴³ Such bills have been introduced, but none have yet been enacted.⁴⁴ Because the civilian use of UAS is nascent, and there is no controlling Supreme Court

³⁸ Cf. *Beltz v. State*, 221 P.3d 328 (Alaska 2009) and *California v. Greenwood*, 486 U.S. 35 (1988).

³⁹ See *Johnston v. State*, 2002 WL 563609 (April 17, 2002) (Mannheimer, J., concurring) (unpublished opinion).

⁴⁰ Villasenor, *supra* note 2, at 498.

⁴¹ *Branzburg v. Hayes*, 408 U.S. 665, 681 (1972).

⁴² *Glik v. Cunniffe*, 655 F.3d 78, 82 (1st Cir. 2011).

⁴³ See Integration of Drones into Domestic Airspace: Selected Legal Issues, Congressional Research Service, CRS Report for Congress (April 4, 2013).

⁴⁴ *Id.*

case law, it remains to be seen how far First Amendment protections will extend in this area.

The privacy rights of individuals and businesses exist in perpetual tension with the First Amendment rights of non-government actors to gather information, and that tension could give rise to actionable claims for privacy violations. Common law invasions of privacy could occur if UAS use “intrudes upon seclusion” in the home or results in the “publication of private facts,” which are the two main categories of invasion of privacy claims. Intrusion upon seclusion occurs where the intrusion was intentional and would be highly offensive to a reasonable person.⁴⁵ A publication of private facts claim could arise where a UAS takes images of private individuals involuntarily caught up in newsworthy events, and those images conveyed facts not previously known to the public.⁴⁶ Similarly, the use of UAS could potentially give rise to criminal liability under both federal and state anti-stalking and harassment laws.⁴⁷ Finally, UAS could be used by private citizens to investigate or monitor potential health and safety violations by businesses, or engage in corporate espionage. Such conduct raises complex and unanswered questions about a private citizen’s right to do under the First Amendment what the government could not do under the Fourth.

In short, the above concepts are nothing new to the First Amendment and privacy arena, but they must and will be revisited in light of UAS enhanced imaging capabilities, ease of use, and ever-increasing availability. As discussed in detail above, the strong privacy protections of the Alaska Constitution make it highly likely that individual privacy rights implicated by UAS will be more zealously legislated and enforced in Alaska than in other jurisdictions.

C. Property rights, & tort liability; nuisance, trespass, & ground damage.

Property owners could potentially file tort claims for nuisance and/or trespass against operators of UAS. According to a preeminent torts treatise, a trespass claim against an aircraft operator is viable only when the aircraft “enters into the immediate reaches of the air space next to the land” and “interferes substantially with . . . the use and

⁴⁵ Restatement (Second) of Torts § 625B (1977).

⁴⁶ Villasenor, *supra* note 2, at 503.

⁴⁷ *Id.* at 505.

enjoyment” of the property by the landowner.”⁴⁸ The navigable airspace regulated by the FAA is considered a public highway, but it appears that anywhere between 50 to 150 feet above the property owner could be considered impermissible interference with private property.⁴⁹ Accordingly, UAS that operate within this window of airspace could potentially raise trespass claims, and UAS that generate noise, light, pollution, or vibration could lead to viable nuisance claims by homeowners.⁵⁰ Additional tort claims could arise if a UAS caused ground damage to personal or real property.

Title 2 of the Alaska Statutes is devoted entirely to the regulation and operation of aircraft (“Aeronautics”). Alaska Statute 02.30.030 provides that “A person may not operate an aircraft in the air or on the ground or water in a careless or reckless manner so as to endanger the property of another.” This statute directs the court, when evaluating such claims, to consider “the standards for safe operation of aircraft prescribed by federal statutes or regulations governing aeronautics.” The phrase “operate aircraft” is defined in AS 02.30.050 as “to use, navigate, pilot, or taxi an aircraft in the airspace over this state, or upon the land or water inside the state.” This chapter does not contain a definition of “aircraft.” However, “aircraft” is defined in the general provisions of Title 2 (Alaska Aeronautics Act of 1949) as “a contrivance used or designed for navigation of flight in the air,”⁵¹ which could be read to include UAS, although this definition was enacted prior to the burgeoning use of civilian UAS. Accordingly, I am uncertain whether UAS would fit into the current statutory definition of “aircraft,” and therefore I think it’s an open question whether a court would find that the foregoing provisions regarding liability for aircraft operation would automatically apply to operation of UAS or whether additional statutory language would be necessary to expand that definition. My instinct is that UAS should be specifically legislated in this manner.

If Alaska chooses to enter this arena by passing laws or regulations, it is advisable for the legislature to also enact a statutory immunity provision. That way, the state may

⁴⁸ American Law Institute, Restatement (Second) of Torts § 159 (2009) cmt. i.

⁴⁹ Rapp, *supra* note 17, at 645 (citing *id.*). See also *United States v. Causby*, 328 U.S. 256 (1946) (rejecting the common law concept that a homeowner owns all the airspace above his property up to the heavens, but rather owns “at least that much space above the ground as he can occupy or use in connection with the land.”).

⁵⁰ *Id.*

⁵¹ AS 02.15.260(2).

avoid liability for damages in tort when two private UAS collide and fragments cause damage to people or property. Such immunity clauses are common and can deflect an argument that the state is liable simply because it has chosen to legislate in a particular topic area.⁵²

D. Environmental concerns.

Scholars have observed the potential of UAS to generate environmental concerns, which could be starker in Alaska than elsewhere. Alaska is already a hotbed of environmental litigation. Many UAS contain batteries, circuitry, and chemicals that could leach into the ground, and the flight of UAS and the noise they cause could disrupt birds and other wildlife habitats.⁵³ Environmental groups and private citizens could potentially raise federal claims regarding the operation of UAS under the National Environmental Policy Act, the Endangered Species Act, or the Noise Control Act.⁵⁴

In Alaska, to the extent UAS and the execution of implementing statutes interfere with state fish, wildlife, and waters, the government could be found in violation of the "common use" and "sustained yield" provisions of the Alaska Constitution, which provide, respectively, that the state, fish, wildlife and waters of the state are reserved to the people for their common use and that replenishable resources belonging to the state must be utilized, developed, and maintained according to the sustained yield principle.⁵⁵

E. Communications interference.

UAS also have the potential to interfere with existing civilian communications systems used to operate cell phones, satellite TV signals, and other wireless and telecommunications technology.⁵⁶ Further, signal loss between UAS and its ground

⁵² See, e.g., AS 09.65.215 (Immunity of peace officer for use of body wire eavesdropping device); AS 09.65.235 (Immunity for negotiated regulation making committee and its members); AS 09.65.250 (Immunity for certain actions related to child support); AS 09.65.330 (Immunity: Use of defensive force).

⁵³ Rapp, *supra* note 17, at 632.

⁵⁴ *Id.*

⁵⁵ Alaska Const. art. VIII, §§3, 4.

⁵⁶ Rapp, *supra* note 17, at 640-41.

control operations could result in a mid-air collision or ground damage.⁵⁷ This problem could be somewhat mitigated by the assignation of UAS to specific frequencies once UAS are fully integrated into the national airspace, but the potential for interference still remains.⁵⁸

Under state law, the Department of Transportation and Public Facilities is responsible for supervising, developing, and promoting "aeronautics and communications inside the state . . ."⁵⁹ The Department could be held responsible for ensuring, through properly adopted regulations and in conjunction with the federal government, that UAS do not unduly interfere with existing civilian communications systems in the state.

F. Mid-air collisions.

Finally, mid-air collisions of UAS with other aircraft and with each other are always a possibility. Most UAS lack the sophisticated collision avoidance systems required of many manned aircraft, and the absence of an on-board pilot who can physically observe other aircraft exacerbates the risk of a mid-air collision.⁶⁰ Furthermore, the "small size and radar profile of [UAS] create significant risk that such craft would damage civilian aircraft, causing both property loss and human casualties."⁶¹

As described above, individual citizens could file tort claims under state law for damages against operators of UAS or the government associated with such accidents. Collisions and near-collisions have already resulted from the use of UAS at the military level, and the scholarship predicts that "[i]t is hard to imagine widespread integration of [UAS] into populated airspace without some level of air-to-air accidents rising."⁶²

⁵⁷ *Id.*

⁵⁸ *Id.*

⁵⁹ AS 02.10.010(a)-(b).

⁶⁰ Rapp, *supra* note 17, at 629; 640-41.

⁶¹ *Id.*

⁶² *Id.*

IV. Conclusion.

There are many more questions than answers surrounding the increased civilian use and operation of UAS, because there is no case law that definitively resolves any of the issues discussed above, and there is a regulatory vacuum. Indeed, "[t]he only certain aspect of the debate about unmanned aircraft and privacy is that it will be contentious."⁶³ However, identifying and analyzing these issues at the executive level is the first step to crafting legislation that attempts to address them. Only when those laws are tested in the courts will we fully come to understand the interplay between the technological advantages offered by UAS, the reach of constitutional protections, and the scope of actionable legal claims.

EMB/tjd

⁶³ Villasenor, *supra* note 2, at 516.



50 Carroll Creek Way, Suite 260, Frederick, MD 21701
Bus (301) 631-2406 Fax (301) 631-2466 singley@alea.org
www.alea.org

June 5, 2013
Mr. Bob Davis
Cadwalader, Wickersham & Taft LLP
700 6th Street, NW, Suite 300
Washington, DC 20001

Dear Mr. Davis:

On behalf of the Airborne Law Enforcement Association (ALEA) and the International Association of Chiefs of Police (IACP) Aviation Committee, we are pleased to submit the following comments regarding the "Privacy Legislation Plan 2013."

To begin, our respective organizations support and promote the IACP Aviation Committee's *Recommended Guidelines for the use of Unmanned Aircraft* (see Exhibit A) and the Association for Unmanned Vehicle Systems International's (AUVSI) *Unmanned Aircraft System Operations Industry "Code of Conduct"* (see Exhibit B). We do not concur with privacy advocates who claim that public safety agencies' utilization of unmanned aerial systems (UAS) poses a greater threat to "privacy rights" than manned aviation. Similarly, we do not concur that said uses pose a greater threat to privacy "rights" than other technologies currently utilized by public safety agencies, both in manned aircraft and on the ground. Furthermore, we do not accept that any legislation is necessary as there are long-standing court rulings upholding our Fourth Amendment protections; but we are particularly opposed to legislation that focus their attention on one technology based on fears of what could occur tomorrow, however unlikely. Aside from recent laws enacted that place outright bans on UAS use, such as that in Charlottesville, VA, many current "anti-drone" bills appear to be more of an attempt to increase protections under the Fourth Amendment without actually altering the U.S. Constitution. The presumption in most of these pieces of legislation is that a reasonable expectation of privacy now exists in places where there has been no such expectation. As such, a warrant must be obtained before UAS can be utilized by public safety.

While U.S. Customs and Border Protection (CBP) has unique operational needs that require larger, longer flight duration aircraft, local, state, and other federal agencies, even if they could afford to acquire and operate similar systems, have no interest in utilizing these types of assets. What they are interested in obtaining are small unmanned aerial systems (sUAS) that are inexpensive, lightweight, portable, and quickly and easily deployable.

sUAS come in two forms: gas powered and battery powered. Within these categories, there are fixed-wing and rotary-wing models. Gas powered sUAS tend to be heavy, loud, and can fly for greater periods of time. Battery powered sUAS are lightweight, relatively quiet, slower, and have short flight durations, especially for the rotary-wing models.

As such, sUAS that are available to public safety, coupled with the Federal Aviation Administration's (FAA) regulations governing the use of UAS by public safety (e.g., cannot exceed 4.4 pounds, cannot exceed 400 feet above ground level (AGL), can only be operated during daylight conditions, and must remain within line of sight of the operator at all times), make this new technology a poor candidate for "spying," as well as for persistent surveillance operations. The fact of the matter is, "spying" and persistent surveillance can be done much more effectively by manned aircraft and ground personnel, than with any sUAS.

With that said, if legislation is to be drafted, we suggest that the following be considered:

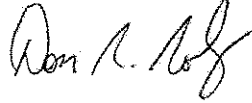
1. The courts have determined in their interpretations of Fourth Amendment cases, that citizens have a "reasonable expectation of privacy." Be cognizant that changing the circumstances under which people have reasonable expectations of privacy can have unintended consequences. If a law enforcement agency determined that the use of a sUAS during a public event was necessary to maintain public safety (assuming that such use would even be permissible under FAA rules), but there is a law requiring that a warrant be issued prior to its use in that capacity, the sUAS could not be used because a judge would have no one to write a warrant for. At the same time, law enforcement conducts these operations regularly with manned aircraft. Why? Because the courts have already determined that there is no reasonable expectation of privacy in such a setting. Does it make sense to have a law that creates a different reasonable expectation of privacy for a UAS from anything else? Will we be seeing legislation developed then for cell phones? GPS? Video cameras? Having more than one "reasonable expectation of privacy" standard is unworkable in law enforcement.
2. Concentrate on sensitive data collection, use, distribution, storage, and purging of data and not on the technology that was used to obtain the data originally. If a person's "reasonable expectation of privacy" is violated by an "unreasonable search and seizure," the device used to create that violation, whether it's a global satellite positioning system, computer, cell phone, video pole camera, manned aircraft camera, unmanned aircraft camera, etc., is irrelevant.
3. Legislation needs to focus on the law enforcement agency utilizing sound policy to govern the use of sUAS technology. The policy should be in accordance with the IACP Guidelines; these Guidelines are a solid starting point for the development of policies for the use of sUAS.

We appreciate the opportunity to have input into this process and look forward to participating in the upcoming roundtable meeting in Washington, DC on August 14.

Sincerely,



Stephen J. Ingley
Executive Director
Airborne Law Enforcement Association



Don R. Roby
Captain
Baltimore County Police Department
Chair
IACP Aviation Committee

Cc: ALEA Board of Directors
IACP Aviation Committee

INTERNATIONAL ASSOCIATION OF CHIEFS OF POLICE
AVIATION COMMITTEE

Recommended Guidelines for the use of Unmanned Aircraft

BACKGROUND:

Rapid advances in technology have led to the development and increased use of unmanned aircraft. That technology is now making its way into the hands of law enforcement officers nationwide.

We also live in a culture that is extremely sensitive to the idea of preventing unnecessary government intrusion into any facet of their lives. Personal rights are cherished and legally protected by the Constitution. Despite their proven effectiveness, concerns about privacy threaten to overshadow the benefits this technology promises to bring to public safety. From enhanced officer safety by exposing unseen dangers, to finding those most vulnerable who may have wandered away from their caregivers, the potential benefits are irrefutable. However, privacy concerns are an issue that must be dealt with effectively if a law enforcement agency expects the public to support the use of UA by their police.

The Aviation Committee has been involved in the development of unmanned aircraft policy and regulations for several years. The Committee recommends the following guidelines for use by any law enforcement agency contemplating the use of unmanned aircraft.

DEFINITIONS:

1. **Model Aircraft** - A remote controlled aircraft used by hobbyists, which is manufactured and operated for the purposes of sport, recreation and/or competition.
2. **Unmanned Aircraft (UA)** - An aircraft that is intended to navigate in the air without an on-board pilot. Also called Remote Piloted Aircraft and "drones."
3. **UAS Flight Crewmember** - A pilot, visual observer, payload operator or other person assigned duties for a UAS for the purpose of flight.
4. **Unmanned Aircraft Pilot** - A person exercising control over an unmanned aircraft during flight.

COMMUNITY ENGAGEMENT:

1. Law enforcement agencies desiring to use UA should first determine how they will use this technology, including the costs and benefits to be gained.
2. The agency should then engage their community early in the planning process, including their governing body and civil liberties advocates.
3. The agency should assure the community that it values the protections provided citizens by the U.S. Constitution. Further, the agency will operate the aircraft in full compliance with the mandates of the Constitution, federal, state and local law governing search and seizure.
4. The community should be provided an opportunity to review and comment on agency procedures as they are being drafted. Where appropriate, recommendations should be considered for adoption in the policy.
5. As with the community, the news media should be brought into the process early in its development.

SYSTEM REQUIREMENTS:

1. The UAS should have the ability to capture flight time by individual flight and cumulative over a period of time. The ability to reset the flight time counter should be restricted to a supervisor or administrator.
2. The aircraft itself should be painted in a high visibility paint scheme. This will facilitate line of sight control by the aircraft pilot and allow persons on the ground to monitor the location of the aircraft. This recommendation recognizes that in some cases where officer safety is a concern, such as high risk warrant service, high visibility may not be optimal. However, most situations of this type are conducted covertly and at night. Further, given the ability to observe a large area from an aerial vantage point, it may not be necessary to fly the aircraft directly over the target location.
3. Equipping the aircraft with weapons of any type is strongly discouraged. Given the current state of the technology, the ability to effectively deploy weapons from a small UA is doubtful. Further, public acceptance of airborne use of force is likewise doubtful and could result in unnecessary community resistance to the program.

4. The use of model aircraft, modified with cameras, or other sensors, is discouraged due to concerns over reliability and safety.

OPERATIONAL PROCEDURES:

1. UA operations require a Certificate of Authorization (CAO) from the Federal Aviation Administration (FAA). A law enforcement agency contemplating the use of UA should contact the FAA early in the planning process to determine the requirements for obtaining a COA.
2. UAS will only be operated by personnel, both pilots and crew members, who have been trained and certified in the operation of the system. All agency personnel with UA responsibilities, including command officers, will be provided training in the policies and procedures governing their use.
3. All flights will be approved by a supervisor and must be for a legitimate public safety mission, training, or demonstration purposes.
4. All flights will be documented on a form designed for that purpose and all flight time shall be accounted for on the form. The reason for the flight and name of the supervisor approving will also be documented.
5. An authorized supervisor/administrator will audit flight documentation at regular intervals. The results of the audit will be documented. Any changes to the flight time counter will be documented.
6. Unauthorized use of a UA will result in strict accountability.
7. Except for those instances where officer safety could be jeopardized, the agency should consider using a "Reverse 911" telephone system to alert those living and working in the vicinity of aircraft operations (if such a system is available). If such a system is not available, the use of patrol car public address systems should be considered. This will not only provide a level of safety should the aircraft make an uncontrolled landing, but citizens may also be able to assist with the incident.
8. Where there are specific and articulable grounds to believe that the UA will collect evidence of criminal wrongdoing and if the UA will intrude upon reasonable expectations of privacy, the agency will secure a search warrant prior to conducting the flight.

IMAGE RETENTION:

1. Unless required as evidence of a crime, as part of an on-going investigation, for training, or required by law, images captured by a UA should not be retained by the agency.
2. Unless exempt by law, retained images should be open for public inspection.



Proposal for American Legislative Exchange Council (ALEC) Unmanned Aerial Vehicle Proposal

Program Objective

The objective of ALEC's Unmanned Aerial Vehicle (UAV) program is to educate our policy makers about the issues surrounding the use of UAVs for domestic purposes. We will inform our state legislator members about considered uses for UAVs in law enforcement, border control, firefighting, search and rescue operations and myriad other uses. We will explore the privacy issues involved and would like to present our members a balanced overview of the topic that addresses some of the misconceptions about UAV capabilities and the benefits of UAV use in the domestic sphere.

Situational Overview

State legislatures are rapidly enacting legislation on domestic UAV use without a complete understanding of the issues involved. As of this writing, 35 states had considered or were considering legislation, including Virginia which passed legislation restricting the use of UAVs, including a two-year moratorium on using UAVs except in university research and search and rescue missions.

State legislators are concerned that UAV surveillance could threaten the civil liberties, especially the privacy of their constituents, so the trend in the legislatures is to err on the side of highly restrictive regulations. Unfortunately, these restrictions might ultimately prevent civilian institutions from taking advantage of UAVs as a cost-effective tool to perform their duties more efficiently during a time of shrinking state budgets. In many cases, ALEC legislators are spearheading these restrictive policies, often due to an incomplete understanding of the issues involved and UAV capabilities.

If misconceptions are not corrected in the immediate future, misguided policy will continue to proliferate throughout state legislatures, and this policy is likely to inform future *national* policy on the domestic use of UAVs. As appropriate UAV implementation could help states meet their public safety objectives in a fiscally responsible way, we would like to see the issues surrounding their use explored in a complete and objective manner.

Program Description

A two-pronged approach would be the most effective way to deal with the issue.

ALEC International Relations Task Force (IRTF) Membership

Model policy on the domestic use of UAVs falls under the jurisdiction of ALEC's International Relations Task Force/National Security Subcommittee, and we anticipate that the task force will consider such policy in the very near future. Issues that capture our members' attention the way this one has are generally brought to ALEC. ALEC task force membership would afford the member

the opportunity to participate in the discussions on the model policy and to inform and enrich the debate. The IRTF is relatively small (well over 100 legislators and 6 private sector members) and has the flexibility to consider and vote on model policy for domestic UAV use rapidly. If this policy is passed within the task force and approved by ALEC's Legislative Board of Directors, it becomes official ALEC model policy and can be accessed by all of our state legislators. Other issues that the task force has explored and continues to discuss include Sequestration, Civilian/Commercial Applications for NASA Research, Sustainable Energy Best Practices in the Military and Overseas, H1B visa expansion, Earth Observation, Expanding the Commercial Marketplace for Space Launches, etc.

The issue of our bimonthly magazine *Inside ALEC* that will be distributed at our Annual Meeting in August 2013 in Chicago will focus on International and Energy issues. An article on domestic uses for UAVs would be a welcome addition to the magazine and would automatically be distributed to those in attendance at the meeting – roughly 1,000 state legislators as well as 1,000 policy and business leaders from across the country. Such distribution would give the issue a deserved spotlight. An article in ALEC's blog, *The American Legislator*, could appear before the Annual Meeting.

UAV Educational Sponsorship Opportunity at ALEC Spring Task Force Summit

ALEC's Communications and Technology Task Force will host a panel discussion/lunch to explore the domestic uses of UAVs at ALEC's Spring Task Force Summit on May 3 in Oklahoma City, OK. We expect 30-40 state legislators to attend. Two speakers who favor more restrictions on the use of UAVs have already been confirmed – Jim Harper a noted privacy expert from the Cato Institute and Ryan Kiesel a noted privacy advocate from the American Civil Liberties Union (ACLU). Both will thoroughly cover the privacy challenges UAV technology poses. This will be our members' first exposure to this issue at an ALEC event, and ALEC wants to ensure that we approach the issue in a balanced fashion. We will have presenters who will emphasize some of the benefits of the domestic uses of UAVs, and the sponsor would be able to select two presenters that would offer this point of view. We would also ask the additional panelists to address the general aviation challenges facing domestic UAVs. We would provide travel expenses for four additional ALEC public sector members from the International Relations Task Force to attend and/or moderate the panel from select states currently considering UAV policy.

Annual Meeting Workshop Sponsorship

This year's Annual Meeting will take place in Chicago, IL August 7-10, 2013 where we expect roughly 2,000 state legislators, policy experts and business leaders to be in attendance. Workshops are panel discussions open to all attendees at our Annual Meeting, and we are confident that a panel discussion on the domestic uses of UAVs would be exceedingly popular. We also have workshop sponsorships at our States and Nation Policy Summit in early December 2013 which generally has attendance of 700-800 state legislators, policy experts and business leaders.

Additional Thoughts

This is a timely issue where our members need a better understanding to make informed decisions. However, this topic is also an excellent opportunity to introduce the concept of civilian applications for products that were originally intended for military and/or space applications and to highlight the critical role that public private partnerships in research play in innovation and economic growth.

1 June 2013

**COMMENTS OF
THE ASSOCIATION FOR UNMANNED VEHICLE SYSTEMS
INTERNATIONAL
ON THE AEROSPACE STATES ASSOCIATION
SUGGESTED PRIVACY LEGISLATION PLAN 2013**

I. Executive Summary

The Association for Unmanned Vehicle Systems International (AUVSI)¹ supports the expanded use of unmanned aircraft systems (UAS) and encourages open discussion of privacy concerns and proposed changes to existing rules, regulations, and laws. These discussions should occur concurrently with the integration of UAS into the National Airspace System (NAS)² in order to fully realize the benefits of rapidly advancing UAS technology and so that a greater understanding of UAS technology's potential can be achieved. Enactment of legislation now – before sufficient experience with integration of UAS into the NAS exists – is premature, and will hinder the creation and development of this new industry. Barring unnecessary delays, AUVSI estimates that this new industry is poised to create over 70,000 new jobs and \$13.6 billion in economic impact within the first three years of integration alone.³

New legislation at the federal or state level that is not technology neutral or that is inconsistent with existing privacy rules, regulations, and laws would stifle innovation and cause delay, and may prevent or discourage the use of UAS by public safety agencies and other potential users. Fourth Amendment jurisprudence, existing federal and state privacy laws, and comprehensive Federal Aviation Administration (FAA) regulations already provide extensive guidance that would allow for initial integration of UAS operations. The FAA, for example, has taken steps to address privacy concerns relating to the use of UAS at test sites, which will help gather knowledge and best practices about UAS operations. If the FAA completes its required and pending rulemaking activities for UAS integration, there will be ample opportunities for multi-stakeholder input.

II. Existing Fourth Amendment Protections

The Fourth Amendment and related case law already governs UAS operations by government users, ensures accountability, and guides the use of aircraft in which the cockpit and pilot are on the ground. Federal, state, and local government agents must obtain search warrants when their use of any technology, including UAS, may violate an individual's reasonable expectation of privacy protected by the Fourth Amendment.⁴ These protections are well-established and address many different privacy concerns relating to government adoption and use of advancing technologies, such as UAS. For more than 220 years, the Fourth Amendment has been applied to new technologies used in warrantless

¹ AUVSI – the world's largest non-profit organization dedicated to the advancement of unmanned systems – represents more than 7,000 members from 55 allied countries and 2,500 organizations involved in fields of government, industry and academia.

² The FAA Modernization and Reform Act of 2012 requires FAA to safely integrate UAS into the NAS by September 2015, and mandates, among other things, the creation of UAS test sites and rulemaking proceedings addressing the integration of civil UAS operations. P.L. 112-95, §§ 331-334, 126 Stat. 11, 72-77 (2012).

³ AUVSI, *The Economic Impact of Unmanned Aircraft Systems Integration in the United States* (Mar. 2013), at 2, <http://www.auvsi.org/econreport>.

⁴ See *Katz v. United States*, 389 U.S. 347 (1967).

observations – including several Supreme Court decisions on aerial observations⁵ and, more recently, thermal imaging⁶ and GPS technologies⁷ – and it will continue to be applied to UAS and other future technologies that have not yet been invented. The Court, in a 2013 decision, held that law enforcement use of a highly-trained drug sniffing dog, roaming outside a home, was “an unlicensed physical intrusion” distinguishable from “Girl Scouts and trick-or-treaters,” and was thus an unreasonable search.⁸ UAS technology is not so distinct from other advanced technologies as to require supplemental legislation.⁹ On the contrary, UAS-specific legislation and laws may have unintended effects, including confusing and complicating the application of existing search warrant requirements¹⁰ that have been carefully developed over two centuries.

AUVSI strongly supports the International Association of Chiefs of Police (IACP) recommended guidelines for UAS operations and associated data collection,¹¹ which the Airborne Law Enforcement Association (ALEA)¹² and others have adopted and even the American Civil Liberties Union (ACLU) has praised.¹³ Like IACP, AUVSI recognizes the “proven effectiveness” of UAS and that the “potential benefits [to public safety] are irrefutable.”¹⁴ AUVSI opposes any legislation that hamstrings first-responders.

III. FAA’s Approach to Privacy and Rulemaking

The Congressionally-mandated FAA rulemaking processes for the integration of small UAS (sUAS) will provide ample opportunities for the public to comment on privacy issues relating to UAS operations.¹⁵ Unlike government operators, who are permitted to operate UAS, albeit through a cumbersome process,¹⁶ civilian operators have no practical, legal means of doing so until the FAA

⁵ See *Florida v. Riley*, 488 U.S. 445 (1989) (naked-eye observations through greenhouse roof from helicopter at 400 feet not an unreasonable search); *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986) (precision aerial photographs of industrial complex from 1,200-12,000 feet not a prohibited search); *California v. Ciraolo*, 476 U.S. 207 (1986) (no reasonable expectation of privacy from naked-eye observations of yard from fixed-wing aircraft flying at 1,000 feet).

⁶ See *Kyllo v. United States*, 533 U.S. 27 (2001) (warrantless use of thermal imaging device to see heat emanating from inside home deemed an unreasonable search).

⁷ See *United States v. Jones*, 132 S. Ct. 945 (2012) (month-long tracking with GPS required a warrant).

⁸ *Florida v. Jardines*, 133 S.Ct. 1409, 1415 (2013).

⁹ “In combination, however, [the *Ciraolo*, *Riley*, *Dow Chemical*, *Kyllo* and *Jones*] rulings indicate that the Fourth Amendment is likely to provide significantly more protection from government UAS observations than is commonly assumed.” John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J.L. & PUB. POL’Y 457, 516 (2013).

¹⁰ See Richard M. Thompson II, CONG. RESEARCH SERV., R42701, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses* (Apr. 3, 2013), at 18-21 (reviewing several bills that “establish arguably greater constraints on [UAS] usage than the Fourth Amendment requires.” *Id.* at 18).

¹¹ IACP, *Recommended Guidelines for the Use of Unmanned Aircraft* (Aug. 2012) (“IACP Guidelines”).

¹² ALEA, *Resolution in Support of the International Association of Chiefs of Police Aviation Committee’s Recommended Guidelines for the Use of Unmanned Aircraft* (Aug. 29, 2012), <http://www.alea.org/assets/cms/files/Resolutions/In%20Support%20of%20UAS%20Guidelines.pdf>.

¹³ See Jay Stanley, *Police Chiefs Issue Recommendations on Drones: A Look at How they Measure Up*, ACLU (Aug. 17, 2012, 9:39 AM), <http://www.aclu.org/blog/technology-and-liberty/police-chiefs-issue-recommendations-drones-look-how-they-measure>.

¹⁴ IACP Guidelines, at 1. What appears to be the first documented instance of a human life being saved with a UAS occurred in Canada earlier this year. See *Single Vehicle Rollover - Saskatoon RCMP Search for Injured Driver with Unmanned Aerial Vehicle*, ROYAL CANADIAN MOUNTED POLICE (May 9, 2013), <http://www.rcmp-grc.gc.ca/sk/news-nouvelle/video-gallery/video-pages/search-rescue-eng.htm>. It will certainly not be the last.

¹⁵ P.L. 112-95, § 332 (requiring the sUAS and integration final rules by August 14, 2014 and December 14, 2015, respectively).

¹⁶ FAA, *Unmanned Aircraft Systems (UAS): Certifications and Authorizations*, <http://www.faa.gov/about/initiatives/uas/cert/>; see also Felicity Barringer, *F.A.A.’s Concerns Hold Up Use of Wildfire Drones*, N.Y. TIMES (May 21, 2013), <http://www.nytimes.com/2013/05/22/us/faas-concerns-hold-up-use-of-wildfire>.

completes its legally required, and long-delayed, rulemakings.¹⁷ Recognizing the importance of addressing privacy concerns, the FAA has taken extraordinary measures to permit public participation in determining the privacy policies that will govern UAS test sites – the agency’s first major step toward integration.¹⁸ Indeed, FAA “aim[ed] to assure maximum transparency of privacy policies associated with UAS test site operations in order to engage all stakeholders in discussion about which privacy issues are raised by UAS operations and how law, public policy, and operators should respond to those issues in the long run.”¹⁹ Rather than passing uninformed²⁰ and potentially unenforceable²¹ legislation now, Congress and state lawmakers should wait for the FAA to complete its rulemaking processes.

The FAA’s primary mission is, and must remain, aviation safety. Still, insofar as privacy issues are inextricably linked to the agency’s creation of a regulatory framework for the integration and operation of UAS, the FAA rulemaking process is the appropriate forum to address privacy concerns. The FAA has properly recognized the role that federal and state law enforcement agencies play in enforcing laws regarding the protection of an individual’s right to privacy, as well as its complementary authority to revoke or suspend a UAS operator’s license. Like the Fourth Amendment jurisprudence applicable to public UAS operators, analogous state laws relevant to civil operators that “address trespass, invasion of privacy, harassment, and stalking [are] well established.”²² AUVSI supports the FAA’s position that Fair Information Practice Principles (FIPPs) should inform UAS privacy policies on the collection, storage, and use of data.²³ Clearly, the registration of certain UAS and pilots with the FAA, the equipage of UAS with identification/position broadcast capability, and the guidelines set forth in AUVSI’s UAS Operations Code of Conduct²⁴ could all contribute to the creation of an overall approach to managing privacy concerns. FAA rulemaking proceedings are the proper forum to address all of these important considerations.

IV. Conclusion

AUVSI supports the integration of UAS into the NAS in a safe and responsible manner, while safeguarding the existing right to privacy and ensuring transparency and accountability. Existing federal and state privacy protections should extend to the operations of UAS, just as they do to the operations of any other advanced technology. But before consideration of any supplemental technology neutral privacy legislation, the FAA should be allowed to gain experience through the UAS test site program and to then complete the well-established regulatory processes for UAS integration that Congress has already mandated. Fourth Amendment jurisprudence, federal and state privacy protections, and other existing laws and regulations are sufficiently robust to guide this effort.

drones.html?_r=0.

¹⁷ See Alissa M. Dolan and Richard M. Thompson II, CONG. RESEARCH SERV., R42940, *Integration of Drones into Domestic Airspace: Selected Legal Issues* (Apr. 4, 2013), at 4 (internal citations omitted). Indeed, the FAA’s sUAS notice of proposed rulemaking has already been delayed more than two years beyond the agency’s initially projected publication date of March 10, 2011. DEPT. TRANSP., *Report on DOT Significant Rulemakings* (May 10, 2013), at 13.

¹⁸ See Unmanned Aircraft Test Site Program, 78 Fed. Reg. 12,259 (Feb. 22, 2013); see also FAA, *Transcript of Online Session on UAS Test Site Privacy Policy* (Apr. 3, 2013), <http://www.faa.gov/about/initiatives/uas/media/UAStranscription.pdf>.

¹⁹ 78 Fed. Reg. at 12,260.

²⁰ See *supra* note 9, at 517 (contrasting UAS with other emerging technologies in that the focus on privacy concerns has come before the benefits are widely recognized).

²¹ See *supra* note 17, at 27-29 (noting that state and local regulation of UAS may be subject to challenge on federal preemption grounds).

²² See *supra* note 9, at 514.

²³ 78 Fed. Reg. at 12,260.

²⁴ <http://www.auvsi.org/conduct>.



Unmanned Aircraft System Operations

Industry “Code of Conduct”

The emergence of unmanned aircraft systems (UAS) as a resource for a wide variety of public and private applications quite possibly represents one of the most significant advancements to aviation, the scientific community, and public service since the beginning of flight. Rapid advancements in the technology have presented unique challenges and opportunities to the growing UAS industry and to those who support it. The nature of UAS and the environments which they operate, when not managed properly, can and will create issues that need to be addressed. The future of UAS will be linked to the responsible and safe use of these systems. Our industry has an obligation to conduct our operations in a safe manner that minimizes risk and instills confidence in our systems.

For this reason, the Association for Unmanned Vehicle Systems International (AUVSI), offers this Code of Conduct on behalf of the UAS industry for UAS operation. This code is intended to provide our members, and those who design, test, and operate UAS for public and civil use, a set of guidelines and recommendations for safe, non-intrusive operations. Acceptance and adherence to this code will contribute to safety and professionalism and will accelerate public confidence in these systems.

The code is built on three specific themes: Safety, Professionalism, and Respect. Each theme and its associated recommendations represent a “common sense” approach to UAS operations and address many of the concerns expressed by the public and regulators. This code is meant to provide UAS industry manufacturers and users a convenient checklist for operations and a means to demonstrate their obligation to supporting the growth of our industry in a safe and responsible manner. By adopting this Code, UAS industry manufacturers and users commit to the following:

Safety

- We will not operate UAS in a manner that presents undue risk to persons or property on the surface or in the air.
- We will ensure UAS will be piloted by individuals who are properly trained and competent to operate the vehicle or its systems.
- We will ensure UAS flights will be conducted only after a thorough assessment of risks associated with the activity. This risks assessment will include, but is not limited to:
 - Weather conditions relative to the performance capability of the system

- Identification of normally anticipated failure modes (lost link, power plant failures, loss of control, etc) and consequences of the failures
- Crew fitness for flight operations
- Overlying airspace, compliance with aviation regulations as appropriate to the operation, and off-nominal procedures
- Communication, command, control, and payload frequency spectrum requirements
- Reliability, performance, and airworthiness to established standards

Professionalism

- We will comply with all federal, state, and local laws, ordinances, covenants, and restrictions as they relate to UAS operations.
- We will operate our systems as responsible members of the aviation community.
- We will be responsive to the needs of the public.
- We will cooperate fully with federal, state, and local authorities in response to emergency deployments, mishap investigations, and media relations.
- We will establish contingency plans for all anticipated off-nominal events and share them openly with all appropriate authorities.

Respect

- We will respect the rights of other users of the airspace.
- We will respect the privacy of individuals.
- We will respect the concerns of the public as they relate to unmanned aircraft operations.
- We will support improving public awareness and education on the operation of UAS.

As an industry, it is incumbent upon us to hold ourselves and each other to a high professional and ethical standard. As with any revolutionary technology, there will be mishaps and abuses; however, in order to operate safely and gain public acceptance and trust, we should all act in accordance with these guiding themes and do so in an open and transparent manner. We hope the entire UAS industry will join AUVSI in adopting this industry Code of Conduct.



May 31, 2013

Mr. Robert Davis
Cadwalader, Wickersham & Taft LLP
700 6th Street, NW, Suite 300,
Washington, DC 20001

Lt. Gov. Mead Treadwell
The Aerospace States Association
107 S. West Street, Suite 510
Alexandria, VA 22314

Dear Mr. Davis and Lieutenant Governor Treadwell,

Thank you for the invitation to participate in the Aerospace States Association's efforts to draft model privacy legislation to regulate unmanned aerial systems (UAS).

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. Our organization has, for the last few years, been extensively involved in privacy and civil liberties issues raised by unmanned aircraft (UA),¹ commonly referred to as drones. 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

Legislation regulating drone use to protect privacy must, at a minimum, address three main points:

1. Law enforcement use of drones requires a warrant;
2. Commercial drone use must be subject to privacy protections and reporting requirements;
3. Regulations on private and media use of drones must strike an appropriate balance between the First Amendment and privacy.

Law Enforcement Drone Use Requires a Warrant

UAS have the potential to fundamentally change the nature of policing in the United States. The technological advances in surveillance provided by drones may provide important benefits to law enforcement. For example, drones could be employed in dangerous situations to avoid risk of harm to an officer or to search in areas challenging to traverse. Drones will also make aerial surveillance much less costly for cash-strapped law enforcement agencies.

¹ For links to EFF's drone-related work, 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>.

815 Eddy Street • San Francisco, CA 94109 USA

voice +1 415 436 9333 fax +1 415 436 9993 web www.eff.org email information@eff.org

However, these same advances will 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. Without strong limitations on how this sophisticated technology can be used, we risk a society where we may all be subject to government surveillance at any time.

For this reason, any legislation regulating law enforcement UAS use must require that officers obtain a warrant based on probable cause before using the UAS for criminal investigations. Such a warrant must have limitations on duration and content recorded, much like a wiretap order does today,³ and must apply whether the drone flies over private or public space.⁴ The warrant requirement must also apply when law enforcement seeks access to data gathered by a drone that is owned or flown by a separate entity, whether that entity is a private party, commercial entity or another public agency.⁵

The warrant requirement can only be subject to limited exceptions for emergency situations such as imminent threats to life or of great bodily harm and only where a warrant could have been obtained but for the time constraints of the situation. And legislation establishing a warrant requirement must have a meaningful enforcement mechanism that allows persons subject to drone surveillance to move to suppress the evidence in any case brought against them.

Commercial Drone Use Must Be Subject to Privacy Protections and Reporting Requirements

Congress has mandated that by 2015, the skies will be open to commercial drone flights.⁶ In fact, the FAA has predicted that, in addition to the hundreds of drones currently used domestically by the military and law enforcement, there will be roughly 10,000 commercial drones flying in the US skies in just five years.⁷ In reality, many small drone operators are already flying UAVs for

³ See, e.g., *Berger v. New York*, 388 U.S. 41 (1967) (describing particularity requirements for wiretap warrants). In *Berger*, the Supreme Court indicated that the Fourth Amendment triggers heightened scrutiny when surveillance is undertaken as “a series or a continuous surveillance” rather than as “one limited intrusion.” See *id.* at 57. Therefore, a statute that regulates “a series or a continuous surveillance” must include special privacy protections or risk invalidity under the Fourth Amendment. See *id.* at 56.

⁴ See, e.g., *U.S. v. Jones*, 132 S.Ct. 945 (2012) (Alito, J., concurring; Sotomayor, J. concurring) In *Jones*, which held law enforcement must get a warrant before affixing a GPS tracking device to a car, five justices took issue with the pervasive nature of surveillance possible with the device, even though the device tracked travel that occurred in public.

⁵ Legislatures must also establish laws limiting the use of drones by non-law enforcement public agencies such as departments of forestry or agriculture. These should include requirements that images, footage or data pertaining to humans obtained by a public agency should not be disseminated outside the collecting agency and should not be used for purposes other than that for which it was collected. And all public agencies, including law enforcement, should be subject to annual reporting requirements to the public on any UAV purchases and how UAVs have been used.

⁶ See FAA Modernization and Reform Act of 2012, Pub. L. 112-95.

⁷ *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.

commercial purposes.⁸

For these reasons, it is critical that legislatures enact laws establishing privacy protections for commercial drone flights. These laws should set out standards that limit the collection, use, sharing, retention and disclosure of data gathered by UAVs. They should also include requirements that the commercial entity establish notice procedures on the type of data gathered by a UAV, how it's gathered and for what purpose, as well as the location the UAV is flown, how long data is retained, with whom it's shared, and how it's disclosed.⁹

Balancing the First Amendment and Privacy in Private and Media Use of Drones

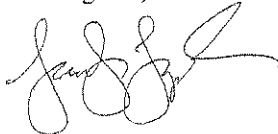
Regulations on private and media use of drones need to strike a balance between protecting privacy and not hampering First Amendment protected speech and associated activities.

As UAV use becomes more prevalent throughout society, private parties and the media will likely also want to fly UAVs for their own and for newsgathering purposes. Some of these activities might include using a UAV to report on a public figure, to monitor law enforcement activities at a political rally, or to record the aftermath of a natural disaster in an urban area. Each of these may impact privacy interests—of the public figure, of the police officer, or of the victims of the natural disaster—but also involve First Amendment-protected activities.¹⁰ For this reason, any law designed to protect privacy must be sufficiently cabined to provide room for these activities. Acceptable limitations could include, for example, duration limits (such as limitations on how long a drone may be used to monitor a specific person), location limits (such as restrictions on monitoring of private spaces like a home or backyard) or could require a finding that the monitoring impinges on an objectively reasonable privacy interest, is highly offensive to a reasonable person, and causes emotional distress.

Conclusion

EFF welcomes the ASA's efforts to craft model legislation to regulate public and private drone use. Please let me know if I can answer any questions or provide further information.

Best regards,



Jennifer Lynch
Staff Attorney
Electronic Frontier Foundation

⁸ See, e.g., Chris Franciscani, *From Hollywood to Kansas, Drones are Flying Under the Radar*, Reuters (Mar 3, 2013) <http://www.reuters.com/article/2013/03/03/us-usa-drones-domestic-idUSBRE92206M20130303>.

⁹ See, e.g., Drone Aircraft Privacy and Transparency Act of 2013, H.R. 1262, 113th Cong. 1st Sess. (1st Sess. 2013) § 339 (b).

¹⁰ For more information, see, e.g., Bill Kenworthy, *Photography & the First Amendment*, First Amendment Center (Jan. 1, 2012), <http://www.firstamendmentcenter.org/photography-the-first-amendment>; Alissa Dolan & Richard Thompson, *Integration of Drones into Domestic Airspace: Selected Legal Issues*, 17-19, Congressional Research Service (Apr. 4, 2013) available at <http://www.fas.org/sgp/crs/natsec/R42940.pdf>.



ELECTRONIC PRIVACY INFORMATION CENTER

Statement of

Amie Stepanovich, Director
EPIC Domestic Surveillance Project¹

for the

Aerospace States Association

regarding

Privacy Legislation Plan 2013

May 31, 2013

On February 14, 2012, President Barack Obama signed the Federal Aviation Administration Reauthorization Act of 2012 ("FAA Act"). The Act provided for funding for the Federal Aviation Administration ("FAA"), advanced the Next Generation Air Transportation System ("NextGen"), and implemented several other aviation-related provisions to increase air traffic safety and reduce accidents.

The FAA Act also provided for the increased and expedited licensing of drones within the United States National Airspace System ("NAS"). Prior to the FAA Act, drones licenses were uncommon, and could only be obtained by a government entity, or, even more rare, by a private entity with an "experimental" limitation. Less than seven formatted pages in length, the relevant sections of the FAA Act fail to address many of the problems inherent in increased domestic drone use. The most significant of these issues is that of privacy.

There are significant privacy concerns involved in the use of drones over domestic soil. Drones are uniquely designed to carry invasive technology that may potentially erode the rights of individuals in the United States to be free of government surveillance under the Fourth Amendment of the Constitution. In addition, drones operated by private entities open new doors to spying, harassment,

¹ EPIC law clerks Adam Marshall and Heather Nodler helped with the drafting of this statement.

and stalking that are not addressed under current law. Finally, the failure of the FAA to implement a drone licensing system that implements the principles of transparency and public access means that many of these intrusions into our private lives will go unnoticed and undocumented.

EPIC'S PETITION TO THE FEDERAL AVIATION ADMINISTRATION

In February 2012, EPIC, joined by over 100 organizations, experts, and members of the public, petitioned the FAA to consider privacy as a key factor in its efforts to streamline and increase drone licensing in the United States. The FAA responded to EPIC's petition in February 2013 and agreed to make privacy a primary factor in its selection of six nationwide test sites for drones in the United States. The FAA requested public comment on its proposed privacy policy and guidelines for these test sites. In response, EPIC asked the FAA to maintain a public database for drone operators, including their geographic area of operation and the surveillance equipment that the drone will carry. EPIC also asked that the FAA implement data collection and retention policies to ensure public notice of domestic drone surveillance operations.

The FAA's actions indicate that the Agency has recognized that new protections are necessary to remedy the privacy threats proposed by drone surveillance. Effective solutions require affirmative action not only from the FAA, but also from other federal agencies and law enforcement bureaus seeking to operate drones domestically, state and local governments, and Congress.

DEVELOPMENTS IN THE STATES

There has been a recent surge in state drone legislation. In total, 43 states have introduced laws that relate to drone surveillance and privacy. Governors of six of these states have now signed measures into law, including Florida, Idaho, Montana, North Dakota, Tennessee, and Virginia. Moreover, six additional states have adopted resolutions on drones: Alabama, Alaska, Idaho, Indiana, Nevada, and Pennsylvania. A drone law in Texas has passed both chambers and awaits the Governor's signature.

The laws in Florida, Tennessee, and Idaho define what drones are and restrict drone use by law enforcement. They require either a warrant or an emergency situation. In Idaho, the law also allows drone use with reasonable suspicion of criminal conduct. The proposed Texas law details numerous situations in which law enforcement may use drones, with and without a warrant. The laws in Florida, Tennessee, and Montana limit the admissibility of evidence obtained by drones, with the standard varying from requiring a warrant to reasonable suspicion.

The law passed in Idaho and the proposed Texas laws restrict private drone use. The Texas draft law carves out numerous exceptions for both public and private use, including border security, mapping, scholarly research, real estate brokerage,

and maintenance of utilities. The laws in Florida, Tennessee, Montana, Virginia, and North Dakota place no restrictions on private use.

The laws in Florida, Idaho, Tennessee, and Texas are written to provide remedies for parties harmed by improper drone use.

In April 2013, Virginia passed legislation prohibiting the use of drones by state agencies dealing with law enforcement or regulatory violations. There are exceptions for Amber and Blue Alerts, search and rescue operations, and uses by the National Guard and educational institutions. The ban lasts until July 2015. In the interim, state agencies have been asked to develop model protocols for drone use. The Alaska and Indiana legislatures have also adopted resolutions calling for the creation of drone task forces to study and make recommendations on their use.

A bill in North Dakota was recently sent to the Governor that would apportion one million dollars to pursue having the FAA designation as a drone test site, and an additional four million in operations funds if it is chosen.

EPIC'S RECOMMENDATIONS TO CONGRESS

In testimony before the Senate Judiciary Committee in 2013, EPIC proposed numerous recommendations for protections that Congress could adopt in order to build privacy protections in to U.S. drone operations. These recommendations include:

- A requirement for drone operators to submit detailed public reports on drones' intended use. Issuance of a license should be contingent on the completion of this reporting, and a privacy right of action and other penalties should ensure that the operators' behaviour complies with the representations made in the report;
- Warrant requirements for law enforcement use of drones, with narrow exemptions for exigent circumstances. The use of drones by law enforcement should be subject to mandatory public reporting requirements, such as those found in the Wiretap Act;
- A prohibition on broad and untargeted drone surveillance by law enforcement;
- A federal Peeping Tom statute, recognizing the enhanced capabilities of aerial drones, should be implemented in order to provide baseline privacy protections for individuals in the home;
- Random independent audits and third-party oversight should be mandated for all drone operators within the United States.

As drone surveillance technology continues to leap ahead, the United States needs to be ready with accompanying measures to ensure that individual rights are not eroded. EPIC looks forward to participating in a public conversation about how to best protect privacy and civil liberties in the development and use of drones throughout the Country.

RESOURCES

- EPIC, *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, <http://epic.org/privacy/drones/>.
- EPIC Spotlight on Surveillance, *"Unmanned Planes Offer New Opportunities for Clandestine Government Tracking"* (Aug. 2005), <http://epic.org/privacy/surveillance/spotlight/0805/>.
- EPIC, *Comments to the Federal Aviation Administration of the Department of Transportation* (April 23, 2013), <http://epic.org/privacy/drones/EPIC-Drones-Comments-2013.pdf>.
- EPIC, *Comments to the Federal Aviation Administration of the Department of Transportation* (May 8, 2012), <http://epic.org/apa/comments/EPIC-FAA-2012-0252.pdf>.
- *Hearing on "Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?" Before the Subcomm. on Oversight, Investigations, and Management of the H. Comm. on Homeland Security*, 112th Cong. (2012) (statement of Amie Stepanovich, Associate Litigation Counsel, Electronic Privacy Information Center), *available at* <http://epic.org/privacy/testimony/EPIC-Drone-Testimony-7-12.pdf>.
- *Field Forum on the Impact of Domestic Use of Drone Technology on Privacy and Constitutional Rights of All Americans, Sanctioned by the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. (2012) (statement of Amie Stepanovich, Associate Litigation Counsel, Electronic Privacy Information Center), *available at* <http://epic.org/privacy/drones/EPIC-Drones-Testimony-102512.pdf>.
- EPIC, *Domestic Drones Petition* (March 2013), http://epic.org/drones_petition/.
- EPIC *Petition to the Federal Aviation Administration* (Feb 24, 2012), <http://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf>.

Two major issues have captured the public's attention over the last two years regarding unmanned aerial vehicles (UAVs), (also known as UAS, or unmanned aircraft systems, RPAs, or remotely piloted aircraft, or "drones," as they are often misleadingly referred in the mass media). The first is the controversial use of UAV-launched missiles and bombs to neutralize threats to U.S. security from terrorists or others hostile to the United States, which have included U.S. citizens. The second arises from concerns over potential violations of privacy or indiscriminate, warrantless surveillance by law enforcement agencies using small, non-tactical fixed-wing or rotorcraft UAVs. A related concern is the perceived threat that U.S. intelligence agencies and military units will "bring home" the sophisticated ISR (Intelligence, Surveillance, Reconnaissance) UAVs that are currently used for counterterrorism and military operations in theater and deploy them to spy on U.S. citizens (although such activity is clearly prohibited by federal law).

Caught up in the whirlwind of popular culture, media hysteria, and political forces is a large international community of scientists, researchers, government agencies and civilian or private operators of UAS who promote and support the peaceful use of the technology for a wide variety of humanitarian and potential commercial applications that have nothing to do with law enforcement or national defense and security.

By way of example, the Arctic is a critically important environment, exerting strong influence on the global climate. The effect of climate change is exaggerated in the Arctic, and, as a result, the Arctic region (north of the Arctic Circle, 66° 33'N latitude) is undergoing very rapid change. Because of these rapid changes, scientists are urgently trying to understand the many climate processes and mechanisms of the Arctic. Use of UAS for environmental research in the Arctic has been ongoing since 1999, and continues to this day. More examples of scientific applications of UAS abound, and a comprehensive list would fill a multi-page appendix.

As a result of similar activities around the globe, the UAS sector has been a growth industry for over a decade, fueled primarily by the Department of Defense and the U.S. intelligence services, but supplemented by a rapidly growing civilian sector devoted to non-military applications such as law enforcement, agricultural remote sensing, atmospheric science, wildlife management, power line and pipe line inspection, fisheries observation and enforcement, border protection, firefighting, flood protection, disaster response, and the like.

A major challenge for the UAS community is identifying the public policies that should drive the next phase of technical development, and, more recently, the influence that the question of personal privacy should have, if any, in the evolution of those policies. State and local governments are grappling with the role that government should or will play in this public debate. The choices for local and state government are: To be active advocates for UAS technology, thereby supporting the anticipated economic impacts from the creation of highly skilled, high paying jobs, but taking no position on the legal and privacy issues; to devote the necessary time

and resources to develop a model privacy policy that could be adopted by other governmental entities; or to do nothing and take no position on privacy, thereby conceding the policy question to the federal government or the private sector.

The issue of privacy and the potential for invasions of personal privacy by individuals and/or government by the use or misuse of remotely piloted aircraft equipped with cameras and other surveillance devices has generated proposed legislation, both state and federal, and aggressive publicity campaigns intended to drastically limit or even outlaw RPAs for any purpose whatsoever. Indeed, the "right to privacy," or the "right to be let alone," has been recognized by the U.S. Supreme Court in a number of cases as being among the fundamental rights guaranteed American citizens by the U.S. Constitution. The seminal treatment of the subject was an article published in the Harvard Law Review, authored by Louis Brandeis and Samuel Warren ("The Right to Privacy" HLR 4, no. 5 (1890): 193-220), in which the authors argued that the time had come for the courts to recognize a common law right to privacy. The article can be read today with virtually no changes and still be as relevant and prescient as it was in 1890.

In our age of electronic exhibitionism and voyeurism, it can be argued that privacy no longer has the meaning that it did over 75 years ago when laws were passed to prohibit the government from wiretapping telephones without a search warrant (although illegal wiretapping in violation of the requirements of the Fourth Amendment apparently still occurs). Dean Prosser's four invasion of privacy torts (intrusion upon a person's seclusion or solitude, or into his private affairs; public disclosure of embarrassing private facts about a person; publicity that places the person in a false light in the public eye; and appropriation, for the someone's advantage, of another person's name or likeness), are no less important concepts now than they were when he described them in his landmark article in the California Law Review over 50 years ago (*Privacy*, 48 Calif. L. Rev. 383 (1960)). But these four categories of invasions of privacy are civil wrongs that provide the basis for an award of monetary damages against the violator. The current media-driven angst over the potential for privacy intrusions from the utilization of unmanned aircraft by law enforcement agencies at all levels (federal, state and local) seems to derive from fear of "Big Brother" (apologies to Orwell) type of broad area, warrantless surveillance of the general population, although no law enforcement agency has publicly stated that it has any intention of ever using UAS for that purpose. Yet, manned aircraft (primarily helicopters), have been used for decades for that precise purpose, with little objection from the public. News helicopters hover over every event from a traffic jam in Los Angeles to a natural disaster in Oklahoma, state highway patrols enforce speed limits with aviation assets, and police departments and first responders routinely use aircraft (often equipped with cameras) to support their law enforcement and firefighting activities.

Some also argue that there is no fundamental difference between carrying a high resolution or infrared camera or some other sensing device on a UAS and deploying the same payload on a manned aircraft, and the Supreme Court has repeatedly held

that observations of law violations from a manned aircraft in the navigable airspace do not violate the Fourth Amendment, even when a warrant is not first obtained.

As a result of pressures applied to legislators, local governments and policy makers by these diverse interests, laws have been proposed in a number of states that are intended to either restrict the use of UAS in many applications or ban them outright, whether the intended use is by law enforcement agencies, or civilians. The FAA has been compelled to conduct public forums on the privacy issue as a result of language in the FAA Modernization and Reform Act of 2012, and is being pressured to propose rules or publish guidelines dealing with the privacy issue.

Thus, the evolving legal issue is whether any local legislation can legitimately regulate an activity that heretofore has fallen under the exclusive jurisdiction of the Federal Aviation Administration. A related policy issue is whether the FAA's statutory mandate dictates that it should have any interest in privacy, or whether it should limit its oversight to traditional aviation concerns such as safety, airworthiness, certification, production standards and airspace rules. The overarching issue is whether there should be any legal restrictions beyond the Fourth and Fifth Amendments on the use of unmanned aircraft by law enforcement agencies or private individuals or entities.

The principle stakeholders in the ongoing privacy debate are a diverse and sometimes unlikely assortment of advocacy partners, often entities or organizations that might ordinarily occupy opposite extremes in philosophy, joining forces to oppose something that they both find threatening or unacceptable. At one extreme lies the UAS industry, represented by many small entrepreneurs, as well as the large defense and aerospace concerns that largely serve the needs of the U.S. military and intelligence services. At the other extreme are civil liberties advocates such as the ACLU, EPIC (Electronic Privacy Information Center), EFF (Electronic Frontier Foundation) and others, who represent the concerns for potential intrusions into personal privacy by government, as well as private citizen exploitation of technology to engage in spying, eavesdropping, data mining, and identity and financial data theft, among others. In the middle of the debate resides the FAA, which has jurisdiction over all activities in the navigable airspace of the U.S.

Potential customers of the industry consist of public safety agencies desiring to acquire small UAS as affordable supplements to existing law enforcement and first responder technology; state and federal science and technology agencies that view UAS as an additional tool to carry out their missions; public and private research universities that similarly seek the use of the technology for a wide variety of research purposes; and, advocacy organizations like AUVSI whose members are engaged in the research and development of this rapidly evolving technology.

The stakeholders are many, the issues are fundamental, and the collective wisdom of all concerned will be needed to solve the problem. ASA is an ideal facilitator to fill that role.

NATIONAL ASSOCIATION OF CRIMINAL DEFENSE LAWYERS
COMMENTS ON PROPOSED DRONE LEGISLATION
MAY 31, 2013

Use of Domestic Drones

The increasing number of bills introduced in states across the country addressing the use of unmanned aerial vehicles, also known as 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 of these rapidly advancing surveillance tools. That is why the National Association of Criminal Defense Lawyers (NACDL) created its own model legislation, promoting protection of fundamental Fourth Amendment rights. The model legislation is available [here](#).¹

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. 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 the drones have high-tech capabilities, that are not in the "general public use,"² to conduct surveillance on areas in plain view and not in plain view, such as the inside of a home.³ 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. Unmanned aircrafts may be outfitted with surveillance equipment to include high resolution cameras, thermal heat imaging devices, and geolocation tracking devices.

Additionally, any evidence obtained in violation of the legislation should be inadmissible in a criminal trial. It is important that this 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 include exigent circumstances or the assessment of an environmental or weather related catastrophe. Exigent

¹ <http://www.nacdl.org/WorkArea/DownloadAsset.aspx?id=26568&libID=26537>.

² *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (reasoning that the police used a device, a thermal heat imaging device, not in the "general public use" to gather information about the inside of a private home.).

³ *Id.* (holding that using thermal imaging to obtain information from inside a home constituted a search under the Fourth Amendment.).

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.

Access to Third Party Records

Drone legislation should address the “third party doctrine.” Third party records are records created and stored by private companies in their ordinary course of business. Today, these records go beyond bank records or dialed phone numbers, and can include all emails, geo-location information, a record of visited websites, and even internet search terms. The Supreme Court has held that individuals have no reasonable expectation of privacy in records shared or generated by a third party. By giving up information to a third party, a person “assumes the risk” that the company would reveal that information to the government. In other words, law enforcement may be able to access drone surveillance data, without a warrant, obtained by a private company for use as evidence in a criminal trial.

In a recent Supreme Court decision, *United States v. Jones*, which involved the placement of a GPS locator on a suspect’s car by police officers without a valid warrant, the Court held that the use of a GPS device constituted a search under the Fourth Amendment.⁴ Justice Sotomayor’s concurrence in particular questioned the use of the third party doctrine in the digital age. She said “[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.”⁵ This has great implications for the use of drones to monitor, collect, and store information that can then be shared with the Government under an outdated third party doctrine.

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. Each individual state should be familiar with its own laws on third party records in determining whether or not such a provision needs to be included in that state’s drone legislation.

Conclusion

NACDL encourages the implementation of the above suggestions into model legislation regulating the use of domestic drones. We look forward to working with you. Please contact NACDL’s National Security and Privacy Counsel, Mason Clutter, with any questions. She may be reached at mclutter@nacdl.org or 202-465-7658.

⁴ *United States v. Jones*, 132 S.Ct. 945 (2012) (“We hold that the Government’s installation of a GPS device on a target’s vehicle, and its use of that device to monitor the vehicle’s movements, constitutes a ‘search’. . . The Government physically occupied private property for the purpose of obtaining information.”).

⁵ *Id.* at 10.

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.