WRITTEN QUESTIONS FROM SENATOR LEE

"The Future of Drones in America: Law Enforcement and Privacy Considerations"
Wednesday, March 20, 2013

Michael Toscano (CEO of Association for Unmanned Vehicle Systems International)

1. In your testimony, you stated that there currently is a "robust legal framework" with respect to privacy and the use of Unmanned Aircraft Systems or UAS. With respect to constitutional violations of privacy, the Supreme Court has never spoken directly to the issue of the application of the Fourth Amendment to UAS. And it seems somewhat unclear how the Court would apply precedents such as *Kyllo* and *Jones* to a case in which evidence was obtained using UAS.

    a. What legal framework is currently in place with respect to privacy and the use of UAS and do you think that framework is adequate?

2. There has been some discussion today of the role of the FAA in imposing restrictions on the use of UAS to protect privacy. It is my understanding that the FAA, in implementing its statutory duty to integrate UAS into national airspace, is considering privacy policies.

    a. Do you support the FAA making privacy protection an integral part of their UAS licensing scheme, and if so, what are some of the more important considerations they should include in their analysis?

Response from Michael Toscano

1. Senator Lee, you are correct that there are currently no U.S. Supreme Court cases directly addressing Constitutional privacy issues related to evidence gathered from an unmanned aircraft system (UAS), primarily because this technology is new and only a handful of law enforcement agencies have permission to fly a UAS.

    However, the Supreme Court has reviewed the implications of technology and aerial surveillance for the past several decades, and AUVSI believes these cases provide valuable precedent in which to consider UAS. It is important to recognize upfront that although the vehicle may be different, the system it is carrying, usually a camera or sensor, are often the same used on manned aircraft. Simply removing the pilot from the aircraft does not change the fact that there is always a human responsible for the flight.

    As John Villasenor stated in a recent article, *Observations from Above: Unmanned Aircraft Systems and Privacy*, (36 Harvard Journal of Law and Public Policy 457-517 (2013)) "a careful examination of Supreme Court privacy jurisprudence suggests that the Constitution will provide a much stronger measure of protection against government UAS privacy abuses than is widely

appreciated. The Fourth Amendment has served us well since its ratification in 1791, and there is no reason to suspect it will be unable to do so in a world where unmanned aircraft are widely used. In addition, there are substantial statutory and common law protections that will limit the ability of non-government entities to violate privacy using manned aircraft."

As you know, the Fourth Amendment of the U.S. Constitution prohibits unreasonable searches and seizures and requires search warrants to be based upon probable cause. Although I am not a lawyer, or a Constitutional expert, below are some U.S. Supreme Court cases I believe are relevant to the discussion of the government's use aircraft and technology for surveillance. In talking with law enforcement, they are comfortable with the rules established by the Court, and they are confident they can utilize UAS technology in full compliance with them.

In *Katz v. United States* (1967), the Supreme Court found it unconstitutional to place an eavesdropping device on a closed public phone booth saying, the "Fourth Amendment search occurs when the government violates a subjective expectation of privacy that society recognizes as reasonable". "These considerations do not vanish when the search in question is transferred from the setting of a home, an office, or a hotel room to that of a telephone booth." "Wherever a man may be, he is entitled to know that he will remain free from unreasonable searches and seizures." This case extended an individual's right to privacy outside of their home.

In *California v. Ciraolo* (1986), the Court created the "reasonable expectation of privacy" test, which the Court found the police did not violate when it flew a small manned airplane over private property and photographed marijuana growing in a backyard (within the curtilage of the defendants home). That observation and the photographs taken were used to secure a search warrant to seize the marijuana. The Court found, "the Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares." The Court considered "public navigable airspace" a thoroughfare and found it permissible for the police to fly anywhere the general public has the right to fly.

In *Dow Chemical Company v. United States* (1986), which was decided on the same day as *California v. Ciraolo*, the Court found it permissible for the Environmental Protection Agency to fly a manned aircraft over a business and take detailed pictures from a sophisticated mapping camera, ruling, "The taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."

In *Florida v. Riley* (1989), the Court found it permissible for the police to fly a manned helicopter 400 feet above a greenhouse, which was located behind a home, and use observations made by looking through missing window panels to secure a warrant to seize the marijuana being grown inside. The Court affirmed its reasoning in *Ciraolo*, saying, "Any member of the public could legally have been flying over Riley's property in a helicopter at the altitude of 400 feet and could have observed Riley's greenhouse. The police officer did no more."

In *Kyllo v. United States* (2001), the Court held that the use of a thermal imaging device from a public vantage point to monitor the radiation of heat from a person's home was a search within the meaning of the Fourth Amendment and thus required a search warrant. The Court found that allowing the government to collect information emanating from a house would put people "at the mercy of advancing technology – including imaging technology that could discern all human activity in the home."

Although the Court discussed at length whether or not a "device is in general public use", the fact remains that when people have a Constitutional right to privacy, the police need a warrant to conduct a search, regardless of the technology being used. If it is unconstitutional for the police to use a handheld thermal imaging device from their police car on a public street, it will also be unconstitutional for the police to use a thermal imaging device to look at a house from a manned aircraft, or a UAS, absent a warrant.

Recently, the Court in *United States v. Jones* (2012) found the police violated the Fourth Amendment on trespassing grounds by sticking a global positioning system tracker on a car to monitor a person's whereabouts for an extended period of time. The Court acknowledged that extended electronic surveillance without a physical trespass *may* violate the Fourth Amendment; however, the Court declined to rule on those grounds.

Earlier this year, the Court once again found an unreasonable trespass when it ruled in *Florida v. Jardines* (2013) that the police cannot bring a drug-sniffing dog on your front porch to inspect for drugs without a warrant.

Clearly, there are lots of ways to track someone's whereabouts, or monitor activities electronically, and it would not be surprising if someday the Court takes up a case, similar to *Kyllo*, where they address an individual's right to privacy, without ruling on trespass grounds. However, given that cases are fact specific, it is too early to tell how the Court will rule on electronic surveillance without a trespass.

If Congress wants to consider legislation addressing UAS privacy issues, it should do so in a technologically-neutral way. Ultimately, the issue is about data. Does the government have the right to collect and use data it gathers by any sort of means against you?

As you know, the government uses a lot of tools that can collect information on us; however, they do not routinely violate our privacy rights because they have policies and procedures in place. The best way to ensure government does not abuse its power is to ensure transparency and accountability. In the event the police use technology improperly, the judicial system is there to hold the government in check. Evidence gathered improperly is not allowed to be used. To echo John Villasenor's comments, our current system has served us well for over 222 years, and there is no reason to think we cannot handle this new technology.

AUVSI does not believe the FAA is the appropriate agency to govern the privacy implications of UAS operations. The FAA should focus on its stated mission, which is to provide the safest, most efficient aerospace systems in the world.

Other federal agencies with expertise dealing with privacy issues, such as the U.S. Department of Justice, the Department of Homeland Security, as well as the judicial system, could address privacy. The FAA's criteria for permitting access to the airspace should solely be based on safety.

AUVSI believes information gathered by a UAS should be treated no differently than information gathered by a manned aircraft, or any other electronic means, as was discussed above in my answer to your first question. Any new legislation or regulation addressing privacy should be technology neutral.

2. You are correct to point out that the FAA is currently soliciting public comments on how to address privacy issues related to the establishment of six UAS test sites around the country, which Congress called for in the FAA Modernization and Reform Act (Public Law 112-95). However, nowhere in the FAA law did Congress direct the FAA to regulate UAS based on privacy issues.

   The FAA intends to use the Congressionally-mandated UAS test sites to collect valuable safety data, which will help it create safety rules. However, in response to privacy concerns raised by the public and some in Congress, the FAA has published a notice of availability and request for comments in the Federal Register (Docket No. FAA-2013-0061). In addition to collecting safety data, the UAS test sites will also help educate the public about UAS and provide best practices for community engagement, transparency, and accountability.

   Below are the UAS test site privacy policy requirements the FAA is currently soliciting public comment on:

   (1) The Site Operator must ensure that there are privacy policies governing all activities conducted under the OTA [Other Transaction Agreement], including the operation and relevant activities of the UASs authorized by the Site Operator. Such privacy policies must be available publically, and the Site Operator must have a mechanism to receive and consider comments on its privacy policies. In addition, these policies should be informed by Fair Information Practice Principles. The privacy policies should be updated as necessary to remain operationally current and effective. The Site Operator must ensure the requirements of this paragraph are applied to all operations conducted under the OTA.

   (2) The Site Operator and its team members are required to operate in accordance with Federal, state, and other laws regarding the protection of an individual's right to privacy. Should criminal or civil charges be filed by the U.S. Department of Justice or a state's law enforcement authority over a potential violation of such laws, the FAA may take

appropriate action, including suspending or modifying the relevant operational authority (e.g., Certificate of Operation, or OTA), until the proceedings are completed. If the proceedings demonstrate the operation was in violation of the law, the FAA may terminate the relevant operational authority.

(3) If over the lifetime of this Agreement, any legislation or regulation, which may have an impact on UAS or to the privacy interests of entities affected by any operation of any UAS operating at the Test Site, is enacted or otherwise effectuated, such legislation or regulation will be applicable to the OTA, and the FAA may update or amend the OTA to reflect these changes.

(4) Transmission of data from the Site Operator to the FAA or its designee must only include those data listed in Appendix B to the OTA. (Appendix B to the OTA is available as part of the SIR [Screening Information Request] at *http://faaco.faa.gov.*)

The FAA anticipates that test site operator privacy practices as discussed in their privacy policies will help inform the dialogue among policymakers, privacy advocates, and the industry regarding broader questions concerning the use of UAS technologies. The privacy requirements proposed here are specifically designed for the operation of the UAS Test Sites. They are not intended to pre-determine the long-term policy and regulatory framework under which commercial UASs would operate. Rather, they aim 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 the industry practices should respond to those issues in the long run.

AUVSI supports the development and advancement of UAS technology in a safe and responsible manner, while respecting existing privacy laws and ensuring transparency and accountability. AUVSI supports the registration of unmanned aircraft and pilots with the FAA, much like they do for manned aircraft. AUVSI supports the creation and enforcement of policies governing the collection, use, storage, sharing, and deletion of data, regardless of how it is collected. Those policies should be available for public review, and they should outline strict accountability for unauthorized use.

Furthermore, AUVSI supports the International Association of Chiefs of Police recommended guidelines for UAS operations and their recommendations on data collection. AUVSI supports the Fourth Amendment's requirement that the government obtain a search warrant whenever someone's reasonable expectation of privacy is violated, and AUVSI supports holding accountable individuals who misuse any technology to violate privacy laws. AUVSI does not condone the use of UAS for illegal surveillance.

As Congress and regulators continue to examine UAS and work towards implementing UAS into the airspace, it is important to tread carefully. Onerous laws or rules, aimed at restricting UAS development and use, will stifle a new industry that has the potential to create 70,000 new jobs and bring over $13 billion in economic growth within the first three years of integration. There should be no doubt, the future of aviation is unmanned, and the United States can remain the global leader in this new competitive field; however, only if this new industry is allowed to grow without undue burdens.

AUVSI looks forward to continuing to work with you, the Senate Judiciary Committee, and the Congress as this technology develops.