Written Testimony of John Villasenor

Nonresident Senior Fellow
The Brookings Institution

and

Professor of Electrical Engineering and Public Policy
University of California, Los Angeles

before the

House Committee on the Judiciary

Subcommittee on Crime, Terrorism, Homeland Security, and Investigations

“Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems”

May 17, 2013
OPENING REMARKS

Good morning Chairman Sensenbrenner, Ranking Member Scott, and Members of the Subcommittee. Thank you very much for the opportunity to testify today on the important topic of privacy and unmanned aircraft systems (UAS).¹

I am a nonresident senior fellow in Governance Studies and the Center for Technology Innovation at the Brookings Institution. I am also a professor at UCLA, where I hold appointments in the Electrical Engineering Department and the Department of Public Policy. The views I am expressing here are my own, and do not necessarily represent those of the Brookings Institution or the University of California. Portions of my testimony today are adapted from a law review article I recently published in the Harvard Journal of Law and Public Policy.²

UAS, often referred to as “drones,” can be employed in an endless variety of civilian applications, the overwhelming majority of them beneficial. However, like any technology, UAS can also be misused. The most common concern regarding domestic UAS relates to their potential impact on privacy. This is a legitimate concern. Existing laws and jurisprudence provide an important foundation, but they also leave many questions unanswered.

For non-government operators, determining when UAS use violates privacy involves the tension between First Amendment freedoms and common law and statutory privacy protections. With respect to government-operated UAS, the Fourth Amendment is of course central to the privacy question. While the Supreme Court has never explicitly considered warrantless observations using UAS, 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.

This does not mean that there is no need for additional statutory UAS privacy protections. However, when drafting new laws it is critical to adopt a balanced approach that recognizes the inherent difficulty of predicting the future of any rapidly changing technology. Although unmanned aircraft pose real and increasingly well-recognized privacy concerns, they also offer real and much less widely understood benefits. A dialog conducted with full awareness of this balance will be much more likely to lead to positive policy outcomes.

¹ The acronym “UAS” is also sometimes expanded to “unmanned aerial systems.”
Unmanned Aircraft Systems

While much of the public and legislative interest in UAS is recent, unmanned flight has a long history. In fact, early research in unmanned aviation laid some of the critical groundwork that was later used by pioneers in manned aviation, \(^3\) including the Wright brothers, who achieved sustained manned heavier-than-air flight in 1903. Unmanned flight received significant attention throughout most of the twentieth century, particularly in the military aviation and model aircraft communities.

The dramatic growth over the last decade in worldwide UAS use is due to a confluence of multiple factors. Continued improvements in electronics have made it possible to equip even very small UAS platforms with sophisticated on-board computational systems for tasks such as image processing and GPS-based navigation. Thanks to advances in digital imaging systems and wireless communications, high resolution images and video acquired by an unmanned aircraft can be transmitted in real time to an observer fifty feet—or 5,000 miles—away. Innovations in airframe design and flight control methods are making it possible to design smaller and more agile UAS.

Unmanned aircraft will dominate the future of aviation as thoroughly as manned aircraft have dominated its past. In the U.S. military, which now has thousands of unmanned aircraft systems, that transition is well underway. Civilian UAS use in the United States is also set to grow rapidly following the enactment of the FAA Modernization and Reform Act of 2012, \(^4\) which provides for the integration of UAS into the national airspace by late 2015. \(^5\)

Unmanned aircraft come in an incredible variety of shapes and sizes. Some, such as the Global Hawk used by the U.S. military, are as large and nearly as fast as business jets. \(^6\) Others are small enough to fit in a backpack or even the palm of a hand. The video-capable Nano Hummingbird, developed by California-based AeroVironment, weighs only two-thirds of an ounce. \(^7\) In May 2013, a team of Harvard researchers reported the successful flight of the RoboBee, a robotic insect weighing less than one three-hundredth of an ounce, and powered by electricity delivered through a thin wire attached to an external power source. \(^8\)

---


\(^5\) Id. §§ 331–336, 126 Stat. at 72–78.


\(^8\) Press Release, Wyss Institute for Biologically Inspired Engineering at Harvard University, Robotic insects make first controlled flight, May 2, 2013, available at http://wyss.harvard.edu/viewpressrelease/110/.
of 2010, a solar-powered Qinetiq Zephyr weighing slightly over 110 pounds despite having a wingspan of about 74 feet stayed aloft for over two continuous weeks over Arizona.9

The potential applications of UAS are just as varied. UAS can help rescuers identify people in need of assistance following a natural disaster and provide vital overhead imagery to police officers attempting to defuse a hostage standoff. In the commercial world, UAS will be employed for tasks as diverse as surveying, crop spraying, and traffic monitoring. Scientific applications include air quality assessment, wildlife tracking, and measuring the internal dynamics of violent storms. UAS will also generate a number of economic benefits, both by creating jobs in unmanned aircraft design and production and by spurring advances in robotics that will apply well beyond aviation, in fields ranging from manufacturing to surgery.

It is also undeniable that UAS can be used in ways that violate privacy. For privacy from government UAS, the Fourth Amendment provides the key constitutional foundation.

**Supreme Court Fourth Amendment Jurisprudence**

The Fourth Amendment, which provides the “right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures,” has been a cornerstone of privacy from government intrusion for over two centuries. While the Supreme Court has never ruled specifically on when UAS use constitutes a Fourth Amendment search, there is a long list of relevant precedents. Among these are two cases from the 1980s that addressed warrantless observations of the curtilage of a home from manned government aircraft.10

The first of these cases, *California v. Ciraolo,* 11 started with a September 1982 tip to police in Santa Clara, California regarding backyard marijuana cultivation. After finding the yard surrounded by high fencing obscuring the view from the street, the police obtained a small airplane and flew over the residence at 1,000 feet. The officers on the airplane observed and photographed what they concluded to be marijuana plants growing in the backyard. This evidence was used to obtain a search warrant to seize the plants.

---

10 There was also a case, *Dow Chem. Co. v. United States*, 476 U.S. 227 (1986), that considered aerial photography using a mapping camera of the open areas of an industrial facility. The Supreme Court ruled that the open areas were more akin to an “open field” than to the curtilage of a home, and as a result, were “open to the view and observation of persons in aircraft lawfully in the public airspace immediately above or sufficiently near the area for the reach of cameras.” *Id.* at 239.
In a May 1986 decision, the Supreme Court noted that warrantless police observations of curtilage are not necessarily unconstitutional: “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.” Moreover, the Court noted, because the observations were made from “public navigable airspace . . . in a physically nonintrusive manner,” the respondent’s expectation of privacy from such aerial observations was not one “that society is prepared to honor.” The Court concluded that “[i]n an age where private and commercial flight in the public airways is routine, it is unreasonable for respondent to expect that his marijuana plants were constitutionally protected from being observed with the naked eye from an altitude of 1,000 feet.”

Just under three years after Ciraolo, the Supreme Court once again considered the constitutionality of aerial observations of a home’s curtilage by law enforcement. Like Ciraolo, Florida v. Riley arose from a tip involving marijuana cultivation behind a house. In Riley, the observations were made from a helicopter at 400 feet, enabling officers to see the plants through openings in the roof and sides of a greenhouse located behind a mobile home. A majority of the justices in Riley found the observations constitutional.

The Court’s 2001 Kyllo v. United States decision, though it considered ground-based observations of a home, is also relevant to UAS privacy. In 1992, a government agent in a car used a thermal imaging device to measure the external temperature of the roof and outside wall of the home of a person suspected of growing marijuana. The roof and wall were found to be abnormally warm, and a search warrant was issued based in part on this information. Upon execution of the search warrant, marijuana plants were found. In a decision finding the use of the thermal imager unconstitutional, the Court held that when “the Government uses a device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a ‘search’ and is presumptively unreasonable without a warrant.”

The most recent Supreme Court ruling with significant implications for UAS privacy is United States v. Jones. Jones considered the government’s installation, without a valid warrant, of a GPS tracking device on a vehicle used by a suspect in a narcotics investigation. The Court’s January 2012 decision was unanimous in

---

12 Ciraolo, 476 U.S. at 213.
13 Id. at 213–14.
14 Id. at 215.
16 The Riley decision comprised an opinion delivered by Justice White and joined by three other Justices and an opinion from Justice O’Connor concurring in the judgment. Thus, while there was no majority opinion, a majority of the Justices found the observations constitutional.
18 Id. at 40.
finding the government’s actions unconstitutional, but there was considerable divergence in the basis for that finding. The majority opinion, delivered by Justice Scalia, found a Fourth Amendment violation in the physical trespass that occurred during the placement of the GPS device on the vehicle. That intrusion, wrote Justice Scalia, “would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.”

In an opinion concurring in the judgment, Justice Alito criticized “the Court’s reliance on the law of trespass” to decide the case. Instead, he wrote, the question is whether the “respondent’s reasonable expectations of privacy were violated by the long-term monitoring” of his vehicle. Because “law enforcement agents tracked every movement that respondent made in the vehicle he was driving” for four weeks—a level of monitoring that Justice Alito felt impinged on reasonable expectations of privacy—Justice Alito concluded that the tracking constituted a search.

Justice Sotomayor, in addition to joining the majority, provided a separate concurring opinion arguing that “the trespassory test . . . reflects an irreducible constitutional minimum” and agreeing with Justice Alito’s view that the respondent’s reasonable expectations of privacy were violated. Justice Sotomayor also expressed concern that the unchecked ability of the government to assemble “the sum of one’s public movements” could enable it to obtain private information regarding political and religious beliefs.

**A “Level of Detail” Test for Constitutionality of UAS Images?**

In *Ciraolo* and *Riley*, the aerial observations of the curtilage of a home were made with the naked eye, a fact specifically noted by the *Ciraolo* Court and in both of the *Riley* opinions that found the government’s observations constitutional. Writing for the plurality in *Riley*, Justice White found no Fourth Amendment violation in part because “no intimate details connected with the use of the home or curtilage were observed.”

In combination, the opinions in *Ciraolo* and *Riley* imply a level of detail threshold beyond which government UAS observations could cross the line into a Fourth Amendment search and thus be unconstitutional without a warrant. This would pose no conflict with *Kyllo*, which stopped well short of endorsing the constitutionality of using technology in general public use. Under a “level of detail” standard, even

---

20 Id. at 949.
21 Id. at 962 (Alito, J., concurring).
22 Id. at 958.
23 Id. at 964.
24 Id. at 955 (Sotomayor, J., concurring).
25 Id. at 956.
26 Riley, 488 U.S. at 452.
widely available UAS technology would lead to a Fourth Amendment violation if used by the government to capture intimate details of a home or its curtilage not normally discernable to a passer-by (or to a person flying over the house in a manned aircraft). By contrast, an image from a UAS camera flown at a very high altitude might raise no constitutional concerns if it reveals very few details.

**Long-term UAS Surveillance of a Home or Curtilage**

For logistical, regulatory, and financial reasons, law enforcement agencies will usually use small UAS. These platforms typically have flight durations measured in dozens of minutes. Thus, the overwhelming majority of law enforcement—and more generally, government—UAS will be incapable of conducting surveillance over a continuous period of days or weeks. But a full consideration of UAS privacy requires acknowledging that some unmanned aircraft do have long flight durations, and could potentially be used by the government to conduct extended surveillance of a home or its curtilage. Would this constitute a Fourth Amendment search?

Lower court rulings related to video cameras installed by the government on fixed structures such as utility poles to surveil private property in the course of criminal investigations are somewhat divergent, but generally recognize the higher expectation of privacy accorded the interior of a home and the fenced-in portion of curtilage.27 In 1987, for example, the Fifth Circuit ruled on a case involving a government-installed video camera on a light pole overlooking a 10-foot fence at the border of a defendant’s backyard. In finding this to be a Fourth Amendment search, the Fifth Circuit wrote that “[h]ere, unlike in *Ciraolo*, the government's intrusion is not minimal. It is not a one-time overhead flight or a glance over the fence by a passer-by.”28 The court concluded that the defendant’s “expectation to be free from this type of video surveillance in his backyard is one that society is willing to recognize as reasonable.”29

A similar line of reasoning should apply to surveillance conducted using unmanned aircraft. The expectation to be free from from extended video surveillance in the curtilage of a home is eminently reasonable, and no less so if the monitoring is performed using a camera mounted on an unmanned aircraft as opposed to on a utility pole. This suggests that the Fourth Amendment will offer strong protection against long-term UAS surveillance of areas of a home or curtilage that a resident has sought to maintain as private.

---

27 See, e.g., *United States v. Cuevas-Sanchez*, 821 F.2d 248 (5th Cir. 1987) and *United States v. Jackson*, 213 F.3d 1269 (10th Cir. 2000).
28 *Cuevas-Sanchez*, 821 F.2d at 251.
29 Id.
Long-Term Location Tracking

Like multiple other technologies, unmanned aircraft could be used to acquire images of pedestrian and vehicular traffic, and thus to potentially track people as they move about in public. In fact, the imaging technology to support this already exists. The DARPA-funded ARGUS-IS sensor merges data from an array of 368 imaging chips to form a single 1.8-gigapixel image. When used on an unmanned aircraft from a height of approximately 17,000 feet, ARGUS can take in a field of view covering many square miles while still retaining sufficient resolution to see six-inch objects on the ground.\(^{30}\) Completely independently, Boeing is under contract with DARPA to develop the SolarEagle, a solar-powered UAS that will be able to stay aloft in the stratosphere for five continuous years.\(^{31}\) Mounting an imaging sensor such as ARGUS on a UAS platform like the SolarEagle would create a system that could track all vehicle and pedestrian movements over many square miles on an extended basis.

The prospect that the government might someday be able to use unmanned aircraft to capture—and then use at will—this level of information about the movements of private individuals is sobering. It is therefore even more sobering that very similar tracking is already being conducted using the increasingly extensive networks of ground-level cameras and license plate readers deployed in many American cities. These systems collect information that, when aggregated, can track our travels just as thoroughly as a bank of cameras on a solar-powered unmanned aircraft turning slow circles in the stratosphere.

The existence of multiple technologies that can perform extended warrantless location tracking in no way diminishes the privacy concerns that would be raised when any one technology is used for this purpose. But the underlying constitutional question raised by location tracking by the government is not technology specific: Do we have a reasonable expectation of privacy from government monitoring of the totality of our public movements over extended periods? Most people would answer this question in the affirmative, and the opinions in *Jones* suggest that a majority of the Supreme Court Justices would answer affirmatively as well.

For the *Jones* majority, the physical trespass involved in attaching the tracking device was sufficient to find the government’s actions unconstitutional. Justice Scalia’s majority opinion noted that while the Court had previously found traditional visual surveillance using a large team of agents to be constitutional, extended location tracking using technologies such as GPS may be different: “It

---

\(^{30}\) Ryan Gallagher, Could the Pentagon’s 1.8 Gigapixel Drone Camera Be Used for Domestic Surveillance?, SLATE, Feb. 6, 2013, http://www.slate.com/blogs/future_tense/2013/02/06/argus_is_could_the_pentagon_s_1_8_gigapixel_drone_camera_be_used_for_domestic.html.

may be that achieving the same result through electronic means, without an accompanying trespass, is an unconstitutional invasion of privacy, but the present case does not require us to answer that question.”\(^{32}\)

However, five of the Justices wrote or joined concurrences that went further. In a concurrence joined by three other Justices, Justice Alito expressed a view that extended warrantless electronic surveillance of public movements is unconstitutional, writing, “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy.”\(^{33}\) In a separate concurrence, Justice Sotomayor noted her agreement with this statement.\(^{34}\) Notably, Justice Alito’s classification of the tracking as a search was a direct consequence of its extended length:

In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark.\(^{35}\)

We will have to wait for a future case to know whether the Court itself would adopt such a view as the basis for finding a search unconstitutional. But in the aggregate, the Jones opinions indicate that the Fourth Amendment will indeed provide protection against extended warrantless location tracking using technologies such as GPS or unmanned aircraft.

**Non-Government Unmanned Aircraft and Privacy**

Private entities are not bound by Fourth Amendment restrictions that apply to the government, and have an affirmative First Amendment privilege to gather information. However, while that privilege is extensive, it is not unbounded, and can end when it crosses into an invasion of privacy. While most companies and individuals will endeavor to use unmanned aircraft responsibly, there will inevitably be some operators who observe less restraint. For example, it would be optimistic in the extreme to expect paparazzi to always operate UAS in a manner respectful of privacy considerations.

Invading an individual’s privacy using a UAS could result in civil or criminal liability. Courts in most jurisdictions recognize two forms of common law invasion of privacy that could arise in connection with UAS: intrusion upon seclusion, and public disclosure of private facts. In addition, many states have civil or criminal statutes, or both, related to invasion of privacy. A person who is photographed in

\(^{33}\) Id. at 964 (Alito, J., concurring).
\(^{34}\) Id. at 955 (Sotomayor, J., concurring).
\(^{35}\) Id. at 964 (Alito, J., concurring).
his or her own home by a UAS hovering just outside an otherwise inaccessible window would thus have strong grounds for a valid cause of action.

Although privacy expectations are greatly reduced outside the home, use of an unmanned aircraft to capture images and other information in a public setting could sometimes constitute an invasion of privacy. A 1998 California Supreme Court ruling in Shulman v. Group W Productions, Inc.\textsuperscript{36} regarding filming that occurred following a car accident is instructive in this regard. In Shulman the victims of the accident were subjected to video and audio recording (using a traditional news camera held by a camera operator on the ground, combined with audio from a microphone worn by the flight nurse from a helicopter rescue crew) without their consent for a television program. The California Supreme Court found that a woman injured in the accident “was entitled to a degree of privacy in her conversations with [the nurse] and other medical rescuers at the accident scene.”\textsuperscript{37} It was improper, the ruling stated, to conclude that the “plaintiffs had no reasonable expectation of privacy at the accident scene itself because the scene was within the sight and hearing of members of the public.”\textsuperscript{38} At the time of the rescue, the vehicle was located “in a ditch many yards from and below” a highway, rendering it “unlikely . . . that any passerby on the road could have heard” the conversation of the victim with the nurse and other rescuers.\textsuperscript{39}

The Shulman ruling provides important guidance regarding newsgathering and UAS with respect to intrusion upon seclusion by drawing a distinction between the information about a newsworthy event available to passersby and the potentially greater amount of information available only to those intimately involved in the event itself. Under some circumstances, there will be no difference: If a crowd of people has gathered around an assault victim who is being treated by paramedics, the conversation between the victim and the paramedics may well be audible to all, and the victim’s reasonable expectation of privacy correspondingly lower. But there will be many cases in which, as in Shulman, passersby have far from complete information about an unfolding event. Using an unmanned aircraft to fill in the gaps would carry a risk of crossing the line into intrusion.

There is an opportunity to strengthen state invasion of privacy statutes to add UAS to the list of recited technologies that could be used to violate privacy. For example, a bill currently pending in the California State Legislature would amend the California civil code statute relating to constructive invasion of privacy to identify a “device affixed to or contained within an unmanned aircraft system” as one of the visual or auditory enhancing devices that could be used to violate a plaintiff’s

\textsuperscript{36} Shulman v. Group W Productions, Inc., 955 P.2d 469 (Cal. 1998).
\textsuperscript{37} Id. at 491.
\textsuperscript{38} Id.
\textsuperscript{39} Id.
reasonable expectation of privacy. The same bill would also amend the California penal code to explicitly provide that eavesdropping upon or recording a confidential communication using “a device affixed to or contained within” an unmanned aircraft is punishable by a fine or imprisonment.

**Business Privacy**

In 2011, a Texas man flew an unmanned aircraft over land near a Dallas-area meat packing plant and acquired images appearing to show environmental violations. He contacted the Coast Guard, and in early 2012 the Texas Environmental Crimes Task Force served a search warrant on the company. Once on the property, investigators found a pipe that “originate[d] in the back of the slaughterhouse” that appeared to be channeling pigs’ blood into a nearby river and “[was] not linked to a waste water system.”

Though few would rush to defend a slaughterhouse that may be in violation of environmental codes, the ability of private citizens or groups to easily inspect for such violations via overflights raises complex issues. To the extent that overflights are lawfully conducted and reveal activities that may be endangering public health, they are obviously valuable. But what happens if a well-meaning but overzealous environmental group conducts daily flights over a large, fenced-in manufacturing facility and repeatedly reports “violations” to the government that turn out, after costly and time-consuming on-the-ground inspections, not to be violations after all? Does the company that owns the facility have grounds to ask a court to enjoin the environmental group from further overflights? What if the group posts pictures from its daily aerial surveillance missions on the Internet, and in doing so exposes information that the company regards as a trade secret? What if the group were to use an unmanned aircraft to examine the interior of buildings at the facility using an advanced thermal imager that, if in government hands and used to inspect a home, would be unconstitutional under *Kyllo*?

In many respects these questions involve issues that go well beyond unmanned aircraft. And in most cases, they will best be resolved through the courts as opposed to through new legislation aiming to solve a business UAS privacy problem of still-uncertain scope and nature.

---

42 *Id.*
43 *Id.*
Conclusions

The Founders of this country certainly did not have unmanned aircraft in mind when drafting the Bill of Rights. But neither were they contemplating thermal imaging—a technology that the Fourth Amendment proved to be eminently capable of addressing hundreds of years later.

The Supreme Court’s Fourth Amendment jurisprudence indicates that the government will indeed have some latitude in acquiring information using unmanned aircraft. But it also conveys the existence of important bounds. Use of an unmanned aircraft to resolve details of a home or its curtilage unavailable through naked-eye observations, or to conduct long-term observations of a home’s curtilage, or to perform extended location tracking could be credibly challenged as unconstitutional without a warrant.

Of course, the only way to know with certainty how the Fourth Amendment will be interpreted with respect to unmanned aircraft observations is to wait for the courts—and ultimately, the Supreme Court—to rule. In the meantime, however, it would be a mistake to draft legislation driven by an assumption that the Fourth Amendment will offer no protection from UAS observations, no matter how invasive. A far better approach is to view privacy legislation for government UAS as complementary to a constitutionally protected right “to be secure . . . against unreasonable searches and seizures” that will still have force and meaning in a world in which unmanned aircraft are common.

There is also a legislative role—mostly at the state level—to provide enhanced privacy protection from UAS operated by non-government entities. State statutes relating to trespassing, invasion of privacy, harassment, and stalking should be examined and updated as appropriate to address potential privacy abuses using UAS.

When considering potential new statutory privacy protections, it is helpful to keep in mind what has occurred with the Internet and mobile telephones, two technologies that are associated with privacy threats that are in some respects much more significant than those that will arise from unmanned aircraft. Usage of both the Internet and mobile phones grew as fast as their underlying technologies enabled. As a result, the public and legislative dialog regarding how best to address the privacy issues they raise has been conducted with a strong appreciation of their benefits. By contrast, while the privacy concerns associated with domestic UAS are real and deserving of attention, they are getting significant focus long before the potential benefits of the technology are widely recognized.

If, in 1995, comprehensive legislation to protect Internet privacy had been enacted, it would have utterly failed to anticipate the complexities that arose after the turn of
the century with the growth of social networking and location-based wireless services. The Internet has proven useful and valuable in ways that were difficult to imagine over a decade and a half ago, and it has created privacy challenges that were equally difficult to imagine. Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose years later.

This doesn’t mean that there is no role for new privacy initiatives. But in developing these initiatives, it is important to recognize the near impossibility of predicting all of the ways that a rapidly developing technology can be used—for good or for ill—in future years. Some of the best privacy protection may in fact lie not in statutory text drafted with a keen eye on the latest innovations in unmanned aircraft technology, but instead in constitutional text drafted over two hundred years ago.

Thank you again for the opportunity to testify on this important topic.