Unmanned Aircraft Systems:
Innovation, Integration, Successes, and Challenges

Written Testimony of John Villasenor

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

Visiting Fellow, The Hoover Institution, Stanford University

before the

U.S. Senate Committee on Commerce, Science and Transportation

March 15, 2017

Introduction

Good morning Chairman Thune, Ranking Member Nelson, and Members of the Committee. Thank you very much for the opportunity to testify today at today's hearing on unmanned aircraft. As requested by the Committee, I am focusing my testimony on the question of privacy, principally in relation to unmanned aircraft but also in relation to rapidly changing technologies more broadly.

I am a professor at UCLA, where I hold faculty appointments in the Electrical Engineering Department, the Department of Public Policy, and the School of Management. In addition, I am a visiting professor at the UCLA School of Law where I created and teach a course on "Digital Technologies and the Constitution." I also have several research affiliations outside of UCLA, including an appointment as a Visiting Fellow at the Hoover Institution at Stanford.[1] The views I am expressing here are my own, and do not necessarily represent those of any of the organizations with which I am affiliated.

[1] More information regarding my research, publications, and academic/research affiliations can be found at http://johnvillasenor.com.

Summary

My testimony today can be summarized as follows:

- First, the fact that unmanned aircraft can potentially be used to gather information in ways that violate privacy does not mean, in and of itself, that new federal unmanned aircraft privacy legislation is needed. Rather, the key question is: Do unmanned aircraft put privacy at risk in ways that fall outside the scope of existing constitutional, statutory, and common law privacy protections? As discussed below, there are good reasons to believe that the answer to that question is "no." As a result, I think it is premature to enact broad new federal legislation specifically directed to unmanned aircraft privacy.

- Second, to the extent that federal unmanned aircraft privacy legislation is nonetheless proposed, I would emphasize the importance of ensuring that it does not inadvertently infringe the First Amendment rights of the many unmanned aircraft users[2] who will operate their platforms in responsible, non-privacy-violating ways. It is relatively easy to draft statutes that limit the ability of unmanned aircraft users to acquire, retain, or distribute information. It is far harder to do so in a manner that is consistent with the full scope of the First Amendment.

- Third, while the specific technology under consideration by the Committee at today's hearing is unmanned aircraft, privacy questions also arise in relation to other rapidly changing technologies, including the Internet of Things, autonomous vehicles, location-aware smartphone applications, and always-on consumer devices equipped with video and/or audio capabilities. These technologies raise far-reaching privacy challenges that may need to be addressed in part through new federal legislation. When drafting new statutes to protect privacy in light of these technologies, it is important to keep in mind that while new legislation always comes with a risk of unintended consequences, that risk is particularly elevated when legislating at the privacy/technology intersection.

Given the different legal frameworks that apply to privacy in relation to unmanned aircraft systems (UAS) operated by the government as opposed to UAS operated by non-government entities, I will address those two categories separately. At the end of this testimony, I will also provide some more general comments on the broader issue of legislation aimed at protecting privacy in light of rapidly changing technologies.

Government-Operated Unmanned Aircraft and Privacy

Government unmanned aircraft users are constrained by the Fourth Amendment, which protects against unreasonable searches. It is sometimes suggested that because unmanned aircraft are so far removed from the technologies that existed when the Bill of Rights was written, the Fourth

[2] In this paragraph, I am referring to non-government UAS users.

Amendment will provide insufficient protection. I disagree. As I wrote in a 2012 *Forbes* article on UAS privacy, the Fourth Amendment "has been a cornerstone of privacy from government intrusion since 1791. It has served us well across more than two centuries of technology advances, and there is no reason to expect that it will suddenly lose its protective power when domestic use of unmanned aircraft becomes common."[3]

The Supreme Court has never considered a Fourth Amendment case specifically directed to UAS privacy. However, there have been several cases involving observations from manned aircraft. The most commonly cited such case is *California v. Ciraolo*,[4] a 1986 decision relating to marijuana cultivation in the fenced-in backyard of a home. After receiving a tip regarding the cultivation and finding the ground-level view into the backyard blocked by a fence, police procured a small plane and overflew the property at an altitude of 1000 feet. Police officers in the plane observed and photographed marijuana plants, and then obtained a search warrant based on the information gathered in the overflight. The defendant challenged the constitutionality of the aerial observations. The Supreme Court, however, found no constitutional violation, writing 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."[5]

Of course, it is possible to view this precedent as suggesting that the Fourth Amendment will provide no barrier at all to warrantless government use of UAS. However, I do not believe that is the proper reading. A careful review of the *Ciraolo* ruling as well as of the 1989 opinions in a similar case, *Florida v. Riley*,[6] suggests the use of the naked eye was a key factor in finding the overhead observations constitutional. Those rulings did not consider the high-resolution camera imagery[7] that can be acquired by a UAS; nor did they consider observations from the lower altitudes at which most UAS will be operated. UAS, in other words, enable capture of information that is much more detailed and potentially invasive than the observations in *Ciraolo*

---

[3] John Villasenor, *Will 'Drones' Outflank the Fourth Amendment?*, FORBES, Sep. 20, 2012, https://www.forbes.com/sites/johnvillasenor/2012/09/20/will-drones-outflank-the-fourth-amendment.

[4] 476 U.S. 207 (1986).

[5] *Id*. at 215.

[6] 488 U.S. 445 (1989). *Riley* involved police observations from a helicopter at an altitude of 400 feet through openings in the roof and sides of a greenhouse being used to grow marijuana. The greenhouse was located in the curtilage of a home. The *Riley* decision comprised a plurality opinion delivered by Justice White and joined by Chief Justice Rehnquist and Justices Scalia and Kennedy; an opinion from Justice O'Connor concurring in the judgment; a dissent from Justice Brennan joined by Justices Marshall and Stevens; and a separate dissent filed by Justice Blackmun. Thus, though there was no majority opinion, a majority of the Justices found the observations constitutional.

[7] There was also a case, Dow Chem. Co. v. United States, 476 U.S. 227 (1986), that considered aerial photography of the open areas of an industrial facility. However, this case did not address a home or its curtilage. The Court ruled that the open areas of the industrial facility 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.

and *Riley*. Such observations are far more likely to violate the expectation of privacy that "society is prepared to recognize as 'reasonable,'"[8] and as such, to be found in violation of the Fourth Amendment.

In addition to the substantial protections that the Fourth Amendment can provide, many Americans live in states that have recently enacted laws providing another layer of privacy protection from information acquired from unmanned aircraft operated by state and local government entities. According to a 2016 report from the National Conference of State Legislatures, "18 states—Alaska, Florida, Idaho, Illinois, Indiana, Iowa, Maine, Montana, Nevada, North Carolina, North Dakota, Oregon, Tennessee, Texas, Utah, Vermont, Virginia and Wisconsin—have passed legislation requiring law enforcement agencies to obtain a search warrant to use UAS for surveillance or to conduct a search."[9]

As far as I am aware, to date there have been no UAS-specific rulings, in either federal or state courts, indicating that the Fourth Amendment and/or state UAS privacy laws will be unable to provide protection from privacy-violating government uses of unmanned aircraft. In short, there is insufficient evidence to conclude that existing frameworks have failed.[10]

Privacy and Unmanned Aircraft Operated by Private Entities

Non-government UAS operators are not constrained by the Fourth Amendment. Furthermore, non-government UAS operators have an affirmative right to gather information under the First Amendment. That does not mean, however, that they have an unfettered right to gather privacy violating images. As I have written elsewhere, "[u]se of a UAS to invade an individual's privacy could result in civil or criminal liability. With respect to civil liability, courts in most jurisdictions recognize the two forms of common law invasion of privacy most likely to arise in connection with UAS: intrusion upon seclusion and public disclosure of private facts."[11] In addition, many states also have civil or criminal statutes, or both, related to invasion of privacy.

---

[8] Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

[9] Amanda Essex, *Taking Off: State Unmanned Aircraft Systems Policies*, National Conference of State Legislatures (2016), http://www.ncsl.org/research/transportation/taking-off-state-unmanned-aircraft-systems-policies.aspx, at 14 (internal citations omitted).

[10] While the foregoing discussion has addressed constitutional and statutory frameworks related to government-operated UAS, government entities can play an important role by adopting policies designed to ensure that they operate UAS transparently and in ways that are mindful of and protective of privacy. See, e.g., The White House, Office of the Press Secretary, *Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*, WHITEHOUSE.GOV (Feb. 15, 2015) (in particular, "Section 1: UAS Policies and Procedures for Federal Government Use"), https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[11] John Villasenor, *Observations From Above: Unmanned Aircraft Systems and Privacy*, 36 HARV. J.L. & PUB. POL'Y 457, 500 (2013) (internal citations omitted).

On top of these non-UAS-specific privacy protections, a growing number of states (as well as municipalities) have enacted legislation[12] addressing privacy from privately-operated UAS. According to the 2016 National Conference of State Legislatures report cited above, "[a]t least 12 states—Arkansas, California, Florida, Idaho, Kansas, Mississippi, Nevada, North Carolina, Oregon, Tennessee, Texas and Wisconsin—have passed legislation providing privacy protections from other citizens that are specific to drones."[13] [14]

This state-level legislative activity reflects what Ohio State University law professor Margot Kaminski foresaw in a 2013 law review essay on what she termed "drone federalism." Addressing the topic of whether additional federal legislation was appropriate, Professor Kaminski wrote:

> Congress should not preempt states from enacting privacy laws governing civilian drone use. States have served as laboratories for experimentation in achieving a balance between First Amendment rights and privacy protection. Congress should permit them to continue doing just that, until an appropriate balance is struck and federal regulation of civilian drone use might again be considered.[15]

While the First Amendment is often at the forefront in legal scholarship on unmanned aircraft privacy, it has sometimes been given insufficient attention in the state and federal legislative dialog. To see why the First Amendment needs to be front and center, consider a person who is holding a smartphone and standing on a third floor balcony overlooking a public street. Under the First Amendment, this person is free to take a picture of the street scene with his or her smartphone. He or she is also free to use the picture privately or to post it online, and free to delete it immediately or to retain it for years. Now consider an unmanned aircraft operating at the same height and used to acquire an image of the same street that raises no more privacy issues than the smartphone picture taken by the person on the balcony. The government would be on very shaky constitutional ground if it tried to legislate what the unmanned aircraft operator can and cannot do with the image acquired from the unmanned aircraft.

---

[12] State statutes and municipal ordinances relating to unmanned aircraft can raise preemption issues. ("The United States Government has exclusive sovereignty of airspace of the United States." 49 U.S.C. §40103 (a)(1)) In the interest of time, I am not addressing preemption in my testimony today, though it is a very important issue and needs to be considered as part of the broader dialog regarding UAS policy, including but not limited to frameworks for addressing UAS privacy.

[13] Essex, *supra* note 9, at 15.

[14] I am focusing my testimony today on legal frameworks relating to UAS privacy. In addition, there is an important complementary aspect of UAS privacy arising from voluntary frameworks that private entities operating UAS can choose to adopt. One example of this is the NTIA multistakeholder process addressing unmanned aircraft. See Multistakeholder Process To Develop Best Practices for Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems, 80 Fed. Reg. 41043 (Jul. 14, 2015), http://www.ntia.doc.gov/files/ntia/publications/fr_uas_meetings_notice_07142015.pdf.

[15] Margot Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIR. 57, 74 (2013).

To take a variant of this example, consider the following thought experiment: Suppose that Congress were to consider legislation requiring that all smartphone owners—or all companies that use smartphones—develop and publish a privacy policy that would include commitments to regularly publish information identifying where and when the smartphones were used to take pictures and for how long those pictures were retained. No one would seriously contemplate proposing such legislation, as it so clearly runs afoul of the First Amendment. Yet it is also clear that smartphones *can* in fact be used to acquire images that violate privacy. We understand that the way to address that issue is not by enacting new legislation requiring *all* smartphone owners to develop, publish, and implement a burdensome privacy policy, but instead through applying existing statutory and common law frameworks to hold to account the very small percentage of smartphone owners who misuse their devices to acquire privacy-violating images.

Of course, the analogy between smartphones and UAS only goes so far. UAS raise important privacy concerns largely because they make it inexpensive and easy to obtain views from an essentially unlimited number of overhead vantage points, including many that cannot practically be accessed with any other technology. In some situations, photographs from those vantage points can undoubtedly violate privacy. But in many situations, photographs from unmanned aircraft will raise no privacy issues at all. Put another way, unmanned aircraft are not *inherently* a privacy violating technology.

And this is precisely why First Amendment issues are so important in the legislative dialog regarding UAS privacy. The same government-imposed constraints on unmanned aircraft users that would raise no constitutional issues when used to prevent egregious violations of privacy, could, in contexts where they are used to prevent or impede non-privacy-violating information gathering, collide directly with the First Amendment. Put another way, when unmanned aircraft privacy laws are drafted without sufficient attention to the First Amendment, they can create what might be termed a form of unconstitutional prior restraint—not in the traditional sense of preemptively blocking information publication, but instead in the inverse sense of preemptively blocking information acquisition.

Privacy and Technology More Broadly

As I noted earlier in my testimony, while the specific technology under consideration by the Committee at today's hearing is unmanned aircraft, important privacy questions also arise in relation to other rapidly changing technologies, including the Internet of Things, autonomous vehicles, location-aware smartphone applications, and always-on consumer devices equipped with video and/or audio capabilities. Faced with the increasingly complex intersection of technology with privacy, there is a temptation to conclude that privacy challenges created by new technology must always be addressed with new legislation.

Technology-specific privacy legislation is sometimes appropriate and necessary. But it should be enacted only after careful consideration of how the statutory language will apply as the technology at issue experiences dramatic advances.

Consider the Electronic Communications Privacy Act,[16] which was enacted in 1986 when e-mail services were still nascent. The ECPA included the Stored Communications Act (SCA),[17] which requires the government to obtain a warrant before accessing "the contents of a wire or electronic communication, that is in electronic storage in an electronic communications system for one hundred and eighty days or less." [18] However, "the contents of a wire or electronic communication that has been in electronic storage in an electronic communications system for more than"[19] 180 days can be accessed with only an administrative subpoena or a court order.[20]

When the SCA was enacted, digital storage was very expensive and storage capacity was correspondingly limited. As a *New York Times* article at the time explained, "most users of [electronic mail] services keep messages only a few months."[21] The overwhelming majority of stored digital communications were under six months old, and those communications were therefore given heightened attention and privacy protection as the SCA was drafted.

Few people in 1986 contemplated a future in which the precise opposite would occur: Today, the majority of our stored digital communications have been stored for *longer* than six months. Ironically, the SCA now has the effect of explicitly *removing* a warrant requirement for the majority of stored communications. With regard to those communications, people would be more protected if the SCA did not exist at all, since it provides a legislative argument that the government can and frequently does employ against those who challenge the constitutionality of warrantless collection of stored communications greater than six months old.

Of course, it could be argued that the problem is not the SCA itself, but the fact that it has not been updated[22] as digital storage has become dramatically less expensive and consumer behavior has changed accordingly. But this, too, illustrates a challenge with enacting digital privacy laws with language reflecting technology at a snapshot in time. Years later, even when nearly

---

[16] Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (1986) (codified as amended at 18 U.S.C. (various sections)).
[17] Codified at U.S.C. §2701 *et seq*.
[18] 18 U.S.C. §2703(a).
[19] *Id*.
[20] 18 U.S.C. §2703(b). The statute provides that the government can access communications older than 180 days without a warrant only "with prior notice from the governmental entity to the subscriber or customer." However, the statute also provides a mechanism, routinely employed in criminal investigations, for delaying notice. In a 2010 decision addressing the constitutionality of warrantless access to e-mails stored for more than 180 days, the Sixth Circuit held that "a subscriber enjoys a reasonable expectation of privacy in the contents of emails" stored with or sent through a commercial ISP and that "to the extent that the SCA purports to permit the government to obtain such emails warrantlessly, the SCA is unconstitutional." United States v. Warshak, 631 F.3d 266, 288 (6th Cir. 2010). However, that decision is binding only in the Sixth Circuit.
[21] Linda Greenhouse, *The Wiretapping Law Needs Some Renovation*, N.Y. TIMES, Jun. 1, 1986, http://www.nytimes.com/1986/06/01/weekinreview/the-wiretapping-law-needs-some-renovation.html.
[22] Statutes created by the EPCA have been amended several times, but the original 1986 provision of the Stored Communications Act that allows warrantless access to communications stored for more than 180 days remains in place.

everyone agrees that technology has long outpaced the language of a statute, it can nonetheless be difficult to obtain agreement on how it should be updated.[23]

None of this is to suggest that Congress has no role in digital privacy, or that there is no need for new digital privacy legislation. Congress has a vital role to play in addressing the privacy challenges raised by emerging technologies. Part of that role involves fostering a dialog among lawmakers, regulators, consumers, the commercial sector, and civil liberties groups so that all parties gain a fuller understanding of the issues. Part of that role involves identifying where existing legal frameworks are working well and where they are falling short. Part of that role involves knowing when *not* to legislate. And part of that role involves enacting carefully targeted legislation at the right time, with an eye on the past to incorporate lessons learned from earlier digital privacy laws, an eye on the future to anticipate where the technology will likely lead, and with the goal of ensuring that any new legislation not only protects privacy, but does so in a way that also promotes innovation and protects constitutional rights.

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

[23] The Email Privacy Act, a bill that would revise the SCA by imposing a warrant requirement on access to stored electronic communications (including those stored for more than 180 days) has been introduced multiple times in recent years, most recently as H.R. 387, 115th Cong. (2017). Earlier versions of the bill introduced in the 113th and 114th Congress did not become law. As of early March 2017 H.R. 387 has passed the House and is under consideration in the Senate.