# B | Governance Studies at BROOKINGS

March 24, 2015

## Unmanned Aircraft Systems: Key Considerations Regarding Safety, Innovation, Economic Impact, and Privacy

Testimony Before the

Senate Committee on Commerce, Science, and Transportation Subcommittee on Aviation Operations, Safety, and Security

#### **OPENING REMARKS**

ood afternoon Chair Ayotte, Ranking Member Cantwell, and Members of the Subcommittee. Thank you very much for the opportunity to testify today on the important topic of domestic unmanned aircraft systems (UAS).<sup>1</sup>

I am a nonresident senior fellow in Governance Studies and the Center for Technology Innovation at the Brookings Institution. I am also a National Fellow at the Hoover Institution at Stanford, and 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, Stanford University or the University of California.

My testimony today can be summarized as follows:<sup>2</sup>



John Villasenor is a nonresident senior fellow at the Brookings Institution, a National Fellow at the Hoover Institution, and a professor of electrical engineering and public policy at UCLA.

<sup>1</sup> The acronym "UAS" is also sometimes expanded to "unmanned aerial systems."

<sup>2</sup> A small portion of this written testimony is excerpted from John Villasenor, *Observations From Above: Unmanned Aircraft Systems and Privacy*, 36 Harv. J.L. & Pub. Pol'y 457 (2013) and from *Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems*, Written Testimony of John Villasenor before the House Committee on the Judiciary - Subcommittee on Crime, Terrorism, Homeland Security, and Investigations (May 13, 2013), available at <a href="http://www.brookings.edu/~/media/research/files/testimony/2013/05/17%20privacy%20drones%20villasenor/villasenortestimonymay17">http://www.brookings.edu/~/media/research/files/testimony/2013/05/17%20privacy%20drones%20villasenor/villasenortestimonymay17</a>.

With respect to privacy:

- When considering the possibly of new privacy laws relating to UAS, it is important not to lose sight of the protections we already have. I believe that that our existing legal framework will provide substantially more protection against privacy-violating misuses of UAS than is commonly recognized.
- UAS-specific privacy legislation at the federal or state level must be carefully crafted to avoid unintended consequences. Absent such care, new legislation could inadvertently end up impeding uses of UAS that pose no privacy concerns at all.
- Privacy legislation that would impact non-government UAS users needs to be drafted in a manner that avoids colliding with the First Amendment freedom to gather information.

With respect to the integration of UAS into the National Airspace System:

- Successful integration of UAS will require fundamentally rethinking our approach to managing the airspace below 500 feet above ground level.
- In future years, with proper design and testing, autonomous, beyond-line-of-sight UAS flight can enable important new applications (such as automated search and rescue operations). Congress should provide a mechanism to allow safe testing of these technologies in appropriately selected subareas within the FAA-designated UAS test sites.

With respect to ensuring America's continued technology leadership:

- Robotics will be one of the key technologies of this century. Ensuring that the United States remains a global technology leader will require ensuring that we have a strong robotics industry, and that in turn will require that we maintain leadership in UAS technology. Congress has a central role to play in achieving that goal.
- The unmanned aircraft hobbyist community—which includes both model airplane hobbyists as well as hobbyists who fly what are commonly called "drones"—is a vital pipeline for careers in aviation and technology. It is important to avoid overly narrow regulatory interpretations that unreasonably limit hobbyists, and that as a consequence also impede America's future capacity for innovation.

#### UAS: GROWING ATTENTION IN CONGRESS, AND MORE BROADLY

Much has happened in the three years since the FAA Modernization and Reform Act of 2012 (FMRA)<sup>3</sup> was signed into law. As Members of this Subcommittee know well, that law addressed both government (more formally, "public") UAS as well as those operated by non-government (i.e., private and commercial) entities (more formally, "civil"). In particular, under the FMRA, the FAA was directed to "develop and implement operational and certification requirements for the operation of public unmanned aircraft systems in the national airspace system"<sup>4</sup> by the end of 2015. In

**<sup>3</sup>** Pub. L. No. 112-95, § 331, 126 Stat. 11, 72 (2012)

**<sup>4</sup>** *Id.* § 334(b), 126 Stat. at 76.

addition, the FAA was directed to "provide for the safe integration of civil unmanned aircraft systems into the national airspace system as soon as practicable, but not later than" the end of September 2015.<sup>5</sup>

In February 2015, the FAA released a long awaited Notice of Proposed Rulemaking (NPRM)<sup>6</sup> for civil "small" (defined as weighing less than 55 pounds) aircraft. The process of developing these proposed rules had been ongoing since well before the enactment of the FMRA, and their publication marked a significant milestone in developing a civil UAS integration framework.

The past several years have also seen a high level of activity in state legislatures in relation to UAS. According to the National Conference of State Legislatures, UAS-specific laws were enacted in 13 states in 2013<sup>7</sup> and 10 states in 2014.<sup>8</sup>

#### UAS AND PRIVACY: AN IMPORTANT AND LEGITIMATE CONCERN

It is important to start by acknowledging that the privacy concerns raised by UAS are real and worthy of attention. For the first time ever, UAS are making it easy and inexpensive to obtain overhead imagery. In the coming decade, that capability will be used by dozens of federal government agencies, by hundreds of state and local law enforcement agencies, and by thousands of private companies and individuals.

The overwhelming majority of the time, UAS operators in both the public and private sectors will be mindful of the need to respect privacy. But as the number of UAS users and flights continues to increase, and as imaging technology continues to improve, simple statistics make it inevitable that sometimes, either inadvertently or intentionally, UAS will be used in ways that violate privacy.

That leads to a series of key questions: To what extent are current legal frameworks up to the task of addressing UAS privacy? What new laws, if any, are needed? Should those laws be at the federal or state level, or both? And how can we ensure that any new laws are constitutional and avoid impeding non-privacy-violating uses of UAS?

#### THE FEBRUARY 2015 PRESIDENTIAL MEMORANDUM ON UAS PRIVACY

The UAS privacy question is particularly timely in light of President Obama's February 2015 Presidential Memorandum titled "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems" (hereafter, the "Presidential UAS Memorandum").<sup>9</sup> The Presidential UAS Memorandum addresses UAS operated by the federal government and, separately, those operated by commercial and private entities.

**<sup>5</sup>** *Id.* § 332(a)(3).

<sup>6</sup> Operation and Certification of Small Unmanned Aircraft Systems, 80 Fed. Reg. 9544 (Feb. 23, 2015), available at <u>http://www.faa.gov/</u>regulations\_policies/rulemaking/recently\_published/media/2120-AJ60\_NPRM\_2-15-2015\_joint\_signature.pdf.

<sup>7 2013</sup> Unmanned Aircraft System (UAS) Legislation, NCSL.Org, <u>http://www.ncsl.org/research/civil-and-criminal-justice/unmanned-aerial-vehicles.aspx</u> (last visited on Mar. 15, 2015).

<sup>8</sup> Rich Williams, 2014 State Unmanned Aircraft System (UAS) Legislation, NCSL.ORG (Sept. 16, 2014), <u>http://www.ncsl.org/research/civil-and-criminal-justice/2014-state-unmanned-aircraft-systems-uas-legislation.aspx.</u>

**<sup>9</sup>** 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*WHITE HOUSE.Gov (Feb. 15, 2015), *available at* <a href="https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua">https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua</a>.

With respect to federal government UAS, the Presidential UAS Memorandum provides a series of policies and procedures aimed at protecting privacy and civil liberties and ensuring transparency and accountability. For example, the Presidential UAS Memorandum limits the duration of time that federal agencies can retain information collected using UAS that may contain personally identifiable information.<sup>10</sup> It also requires an agency using UAS to "provide notice to the public regarding where the agency's UAS are authorized to operate in the NAS,"<sup>11</sup> and to "make available to the public, on an annual basis, a general summary of the agency's UAS operations during the previous fiscal year, to include a brief description of types or categories of missions flown, and the number of times the agency provided assistance to other agencies, or to State, local, tribal, or territorial governments."<sup>12</sup>

One important government UAS category not directly<sup>13</sup> addressed by the Presidential UAS Memorandum is state and local government use. The policies identified in the Presidential UAS Memorandum are of necessity limited to federal government agencies using UAS. However, those policies can and should serve as a model for states to consider and potentially adopt, either as is or with modifications.

Separately, with respect to nongovernment (i.e., commercial and private) UAS, the Presidential UAS Memorandum directed the National Telecommunications and Information Administration (NTIA) to initiate a "multi-stakeholder engagement process to develop a framework regarding privacy, accountability, and transparency for commercial and private UAS."<sup>14</sup> This framework will not have the force of law, but will instead be a set of "best practices" that commercial and private UAS operators will presumably be encouraged to adopt. On March 5, 2014, the NTIA published a request for public comment<sup>15</sup> and identified a set of 16 questions relating to privacy, accountability, and transparency in relation to commercial and private UAS. Comments are due to the NTIA on April 20, 2015. The dialog generated during this process will be vital in identifying any loopholes that might exist in current privacy law in relation to non-government UAS, and that could be addressed with suitably crafted legislation.

#### "PUBLIC NAVIGABLE AIRSPACE"

One of the most interesting and important questions relating to UAS generally, and to the privacy issues they raise specifically, relates to the definition of "public navigable airspace."

Discussions about public navigable airspace in the context of manned aircraft often assert that it is the airspace above 500 feet above ground level. However, that assertion provides an incomplete picture for several reasons. First, it is only partially accurate. Fixed-wing aircraft obviously have a right to use altitudes lower than 500 feet when taking off and landing. In addition, the altitude minimums are higher "[o]ver any congested area of a city, town, or settlement, or over any open air assembly of persons."<sup>16</sup> Furthermore, helicopters are not subject to the same altitude minimums as fixed-wing aircraft as long as "the operation is conducted without hazard to persons or property on the surface."<sup>17</sup>

14 Id. at §2(b).

**15** Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems, 80 Fed. Reg. 11978 (Mar. 5, 2015), *available at* <u>http://www.ntia.doc.gov/files/ntia/publications/rfc\_uas\_privacy\_03052015.pdf.</u>

16 14 C.F.R. §91.119(b).

<sup>10</sup> Id. at §1(a)(ii).

<sup>11</sup> Id. at §1(d)(i).

<sup>12</sup> Id. at §1(d)(iii).

**<sup>13</sup>** The Presidential UAS Memorandum indirectly addresses state and local government use by requiring that "State, local, tribal, and territorial government recipients of Federal grant funding for the purchase or use of UAS for their own operations have in place policies and procedures to safeguard individuals' privacy, civil rights, and civil liberties prior to expending such funds." See the Presidential UAS Memorandum at §1(c)(vi).

<sup>17 14</sup> C.F.R. §91.119(d).

With UAS the picture gets even more complicated because of rules limiting operation of certain classes of small UAS to a *maximum* of 400 or 500 feet.<sup>18</sup> Clearly, then, when it comes to UAS the public navigable airspace must include some altitudes below 500 feet. But just as clearly, it shouldn't include the airspace two inches above ground in a person's backyard.

In a 1946 case involving manned aircraft (*United States v. Causby*), the Supreme Court recognized the need to provide the public with access to the airspace while also recognizing the need to provide property owners with a zone of control over their land: "We have said that the airspace is a public highway," the Court wrote. "Yet it is obvious that if the landowner is to have full enjoyment of the land, he must have exclusive control of the immediate reaches of the enveloping atmosphere."<sup>19</sup>

But exactly how far up should this exclusive control extend? In a November 2014 paper,<sup>20</sup> Professor Gregory McNeal of the Pepperdine University School of Law provided an excellent framing of the complexities involved. Dr. McNeal observes that one component of a solution could be to give property the owners the right "to exclude aircraft, persons, and other objects from a column of airspace extending from the surface of their land up to 350 feet above ground level."<sup>21</sup> Dr. McNeal also notes that a height limit alone won't be sufficient:

Granted a rule extending property rights in a manner to prevent low altitude flights directly over a landowner's property won't preclude the police from asking a neighbor if they can fly above their adjacent property to obtain a better vantage point, just like existing rules don't preclude the police (or a private citizen) from asking a neighbor if they can come inside to look out a second floor window into neighboring property. Similarly, such a rule won't preclude the police from flying above public land (such as sidewalks and streets), but local zoning laws could address flights over public land.22

To that, I would add the additional concern that codifying the specific boundaries of a property owner's zone of control over airspace would also codify a region (e.g., above 350 feet) in which the property owner does *not* have control. It is easy to envision how this could be exploited. And, with improvements in imaging technology, images acquired from just above the upper limit of a property owner's region of control could still be very invasive.

A more fundamental issue is that while height is certainly one of the factors that impacts whether UAS use over (or in the vicinity of) private property is invasive, it is not the only factor. It is also important to consider what the UAS is doing. A UAS that transits quickly and quietly over a property at 320 feet is generally far less intrusive than one that hovers overhead for many minutes at 380 feet. And a UAS equipped with a very advanced imaging system is potentially much more invasive than one with a very basic imaging system.

Given these complexities, I do not think it is feasible to effectively protect privacy by attempting to codify in advance the specific ways in which it is permissible—or impermissible—to overfly private property. I believe that the better

**<sup>18</sup>** The NPRM released in February 2015 (*supra* note 8) identifies a proposed upper limit of 500 feet for small (up to 55 pounds) UAS and an upper limit of 400 feet for the "Micro UAS" sub-classification, which covers UAS up to 4.4 pounds.

**<sup>19</sup>** United States v. Causby, 328 U.S. 256, 264 (1946).

**<sup>20</sup>** Gregory McNeal, Drones and Aerial Surveillance: Considerations for Legislators, The Brookings Institution (Nov. 2014), available at <a href="http://www.brookings.edu/research/reports2/2014/11/drones-and-aerial-surveillance">http://www.brookings.edu/research/reports2/2014/11/drones-and-aerial-surveillance</a>.

<sup>21</sup> Id. at 4.

<sup>22</sup> Id. at 13.

way to address this is to let courts apply tort law and (when applicable<sup>23</sup>) statutory law using the well-established, non-technology-specific standard of a "reasonable expectation of privacy" to the facts specific to any particular case that might arise.

#### HOW PROTECTIVE IS THE CURRENT LEGAL FRAMEWORK?

Of course, in considering new laws addressing UAS privacy, one of the first questions to ask is: What protections do we *already* have? The answer, I believe, is that our existing legal framework will provide substantially more protection against privacy-violating misuses of UAS than is commonly recognized.

The applicable framework for privacy from UAS depends in large part on who is making the observations. For UAS operated by the government, 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," is a key pillar of privacy protection. For privately operated UAS, privacy protections are provided through the common law invasion of privacy tort as well as through civil and criminal invasion of privacy statutes.

#### GOVERNMENT UAS AND THE FOURTH AMENDMENT

It is sometimes suggested that because the Fourth Amendment was ratified over 200 years ago, it will not be effective in providing protection from privacy violations using UAS—a technology that the Founders could scarcely have imagined.

I disagree. To explain why, it is helpful to start by considering several *manned* aircraft cases from the 1980s in which the Supreme Court did *not* find a Fourth Amendment violation—and then to consider why, in light of more recent Supreme Court jurisprudence, I believe that the UAS privacy picture is somewhat more optimistic than those precedents might initially appear to suggest.

The Supreme Court's 1986 decision in *California v. Ciraolo*<sup>24</sup> considered police use of a small airplane to overfly a Santa Clara, California residence at 1000 feet and look into the backyard, where they saw marijuana plants. When presented with the question of whether the observations violated the Fourth Amendment, the Supreme Court found in favor of the government, writing that because the observations of the curtilage of the respondent's home 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."<sup>25</sup> 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."<sup>26</sup>

Also in 1986, in a ruling involving government overflights of an industrial facility, the Court found in *Dow Chemical Co. v. United States* that "the taking of aerial photographs of an industrial plant complex from navigable airspace

<sup>23</sup> Some invasion of privacy statutes codify a "reasonable expectation of privacy" as the standard to use when judgeing whether the statute has been violated.

<sup>24 476</sup> U.S. 207 (1986).

<sup>25</sup> Id. at 213–14.

<sup>26</sup> Id. at 215.

is not a search prohibited by the Fourth Amendment.<sup>27</sup> The Court in *Dow Chemical* considered the open areas in the 2000-acre industrial facility more akin to an "open field" than to the curtilage of a home, and concluded that those areas 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.<sup>28</sup> And in 1989, in *Florida v. Riley*,<sup>29</sup> a case similar in some respects to *Ciraolo*, the Supreme Court again considered the constitutionality of aerial observations of a home's curtilage by law enforcement. A majority of the justices in *Riley* found the observations constitutional.<sup>30</sup>

In combination, these rulings certainly suggest that some observations from government UAS will be deemed constitutional. However, and critically, that does not mean that *all* such observations will be constitutional. If the government uses a UAS, without a warrant, in a manner violating a reasonable expectation of privacy—either through the duration of the observations or the detail they reveal—then those observations should not pass constitutional muster.

We don't yet know how the Supreme Court would rule in a case involving UAS privacy, but a review of the Court's 21<sup>st</sup> century jurisprudence in relation to other technologies provides cause for optimism. In 2001, for example, the Supreme Court ruled in *Kyllo v. United States*<sup>31</sup> that the warrantless use by the police of a thermal imaging camera to measure the temperature of the walls of a house—and to thereby infer that the occupant was growing marijuana—was a violation of the Fourth Amendment.

In 2014, the Court ruled in *Riley v. California*<sup>32</sup> that when conducting a search incident to arrest, police did not generally have the right to search the contents of the arrestee's mobile phone without a warrant. Writing for the Court, Chief Justice Roberts explained:

Our cases have recognized that the Fourth Amendment was the founding generation's response to the reviled "general warrants" and "writs of assistance" of the colonial era, which allowed British officers to rummage through homes in an unrestrained search for evidence of criminal activity.<sup>33</sup>

And:

Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought. Our answer to the question of what police must do before searching a cell phone seized incident to an arrest is accordingly simple—get a warrant.34

- **31** 533 U.S. 27 (2001).
- 32 134 S. Ct. 2473 (2014).
- **33** *Id.* at 2494.

<sup>27</sup> Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

<sup>28</sup> Id.

**<sup>29</sup>** 488 U.S. 445 (1989).

**<sup>30</sup>** The 1989 *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.

**<sup>34</sup>** *Id.* at 2494-2495, internal citations omitted.

The 2012 *United States v. Jones*<sup>35</sup> decision also sheds light on how some of the Justices view the Fourth Amendment in light of modern technologies. That case 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 decision was unanimous in 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."<sup>36</sup>

In terms of viewing the Fourth Amendment in light of today's technologies, the concurrences in *Jones* were more instructive than the majority opinion. In a concurrence joined by three other Justices, Justice Alito wrote that the question is whether the "respondent's reasonable expectations of privacy were violated by the long-term monitoring"<sup>37</sup> of his vehicle. Because "law enforcement agents tracked every movement that respondent made in the vehicle he was driving"<sup>38</sup> 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"<sup>39</sup> 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.<sup>40</sup>

So we have a total of five Justices—Justice Alito and the three others<sup>41</sup> who joined his concurrence, and Justice Sotomayor in her own concurrence—on record with statements indicating a view that warrantless use of technology to perform long-term tracking violates the Fourth Amendment. This is relevant to UAS both directly and indirectly.

The direct relevance arises because there is one class of UAS, called "High Altitude, Long Endurance" (HALE) UAS, that can stay aloft at very high altitudes for weeks, months, or even years at a time. The concurrences in *Jones* suggest that government use of such platforms to perform warrantless long-term tracking of individuals using this or any other technology would raise serious constitutional concerns for a majority of the Justices.

There is also an indirect and far broader relevance that is not specific to UAS. After all, most UAS can only stay aloft only for short periods of time—usually measured in minutes, not hours. They simply cannot be used to perform long-term tracking. They can potentially, however, be misused in ways that would violate reasonable expectations of privacy. The concurrences in *Jones*—as well as the majority opinions in *Kyllo* and in *Riley v. California*—indicate that the Fourth Amendment, when properly interpreted, retains the power to prevent the government from using modern technologies in ways that violate privacy.

<sup>35 132</sup> S. Ct. 945 (2012).

<sup>36</sup> Id. at 949.

<sup>37</sup> Id. at 958 (Alito, J., concurring).

<sup>38</sup> *Id.* at 964.

<sup>39</sup> Id. at 955 (Sotomayor, J., concurring).

**<sup>40</sup>** *Id.* at 956.

<sup>41</sup> Justice Alito's concurrence was joined by Justices Ginsburg, Breyer, and Kagan.

#### 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 ends when it crosses into an invasion of privacy.

Use 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.<sup>42</sup> In addition, some states also have civil or criminal statutes, or both, related to invasion of privacy.<sup>43</sup>

State laws aimed at bolstering privacy protections from non-government UAS should be enacted only if, and to the extent that, current frameworks are insufficiently protective. After all, the set of existing protections against invasion of privacy can be powerful and adaptable precisely because they are not technology-specific, and can therefore be reinterpreted as needed as new technologies emerge. Technology-specific privacy laws, by contrast, risk becoming quickly obsolete as the technology changes. Alternatively, or in addition, they can sometimes lead to unintended consequences that impede uses of the technology that pose no threat at all to privacy.

#### THE IMPORTANCE OF FIRST AMENDMENT CONSISTENCY

There is also an additional consideration to keep in mind: Laws drafted to address privacy with respect to a specific, rapidly evolving technology such as UAS can inadvertently run counter to the goal of a technology-neutral interpretation of the First Amendment freedom to gather information. This can create some problematic consequences.

Consider a photograph of the countryside taken using a smartphone by a passenger<sup>44</sup> riding in a privately owned single-engine airplane as it descends through 350 feet on the way to landing. No one would reasonably deny the passenger's First Amendment right to take that photograph. The owners of properties within the frame of view would not have an ownership interest in the photograph; nor would they have the right to control its use, to require notification that the photograph had been acquired, or to require that it be retained for a certain amount of time.

Now consider a similar photograph taken from a privately-owned UAS 350 feet above the ground, using a camera with similar imaging capabilities.<sup>45</sup> Under some of the UAS privacy laws that have been proposed (and in some states, introduced and adopted), the owners of properties within the frame of view might have substantially more control over the acquisition, use, dissemination, or retention of the UAS-acquired photograph than of the photograph taken by the on-board passenger.

I will emphasize that neither the UAS operator nor the on-board passenger has the right to acquire images that constitute an invasion of privacy. But, assuming that the images are such that no one's privacy is invaded (for example, if the image resolution is low and no private details are contained in the images), why should the UAS operator's right

<sup>42</sup> See William L. Prosser, Privacy, 48 Calif. L. Rev. 383, 389 (1960); see also Restatement (Second) Of Torts §§ 652A–652E (1997).

<sup>43</sup> See, e.g., CAL. CIV. CODE § 1708.8 (West 2011).

<sup>44</sup> I am assuming in this example that the passenger is not a government employee or otherwise acting on behalf of a government entity.

**<sup>45</sup>** Of course, a UAS would not be able to operate in the immediate vicinity of an airport, which is why the photograph could be "similar" but could not be "identical."

to take a photograph be so much more limited than that of the on-board passenger? Put another way, why should the scope of the First Amendment be so much narrower for the UAS operator than for the on-board passenger?

If the First Amendment is in effect narrowed for a particular class of people—UAS users, in this instance—it is easy to see how this could lead to some disturbing unintended consequences. Peaceful demonstrators, for example, might be told that they are not permitted to use a UAS to film a demonstration, on the grounds that the footage might include adjacent buildings owned by people who disagree with their viewpoint.

### INTEGRATING UAS INTO THE NAS: MEETING THE CHALLENGES

Without in any way diminishing the importance of the issue of UAS privacy, I would also like to offer some more general comments regarding the integration of UAS into the NAS.

The airspace in the United States is a complex, busy place. It is shared every day by thousands of manned aircraft, including single-engine private planes flying at 100 miles per hour and 500-ton commercial passenger aircraft<sup>46</sup> travelling at well over 500 miles per hour. At this moment, and in fact at most times during most days, there are many thousands of manned aircraft in the air over the United States.<sup>47</sup> We take it for granted that nearly all of the time, all of these aircraft share the airspace without incident, in all types of weather, day and night. Anyone who spends a few minutes watching the radar tracks of airplanes above a major U.S. metropolitan area will come away amazed by the complex, three-dimensional choreography involved in keeping our skies safe.

To this already complicated mix, we will be adding thousands of new unmanned aircraft. For UAS integration to occur as safely and successfully as possible, we will need to rethink management of the airspace below 500 feet above ground level. In addition, we should recognize that autonomous flight can play an important longer-term role. And, we should provide a mechanism to enable safe testing of autonomous, beyond-line-of-sight UAS operation.

#### THE AIRSPACE BELOW 500 FEET: THE NEED FOR A NEW APPROACH

We need to rethink management of the airspace below 500 feet above ground level. The paradigms developed for manned flight that generally occurs above 500 feet are much less well suited to unmanned flight that will occur below 500 feet. Instead, we need a new approach that recognizes 1) the important stake of property owners in how sub-500-foot altitudes will be managed and used, 2) the fact that UAS will outnumber manned aircraft at those altitudes, and 3) that since so much of the low-altitude traffic will be unmanned, the traditional assumption that every aircraft must have at least one human pilot devoting his or her full attention to flying it will, in the long term, need to be revisited. This last point ties directly to the role of autonomous flight technologies that, with proper design, have the potential to improve both safety and efficiency in the lower airspace.

**<sup>46</sup>** The gross takeoff weight of an Airbus A380 is over one million pounds.

**<sup>47</sup>** Air Traffic NextGen Briefing: Keeping America's Skies Safe, FAA.Org (last modified Sept. 18, 2014), <u>https://www.faa.gov/air\_traffic/briefing/</u> (last visited on Mar. 15, 2015).

#### AUTONOMOUS FLIGHT

"Autonomous" UAS flight refers to a UAS that is flown without being actively and continuously controlled by a ground-based human pilot.<sup>48</sup> Autonomy is actually a continuum, including fully autonomous flight as well as flight that is mostly under the control of a human pilot. It is also possible to have a UAS that flies autonomously during some, but not all, portions of a flight. (In some respects, this isn't so different from what routinely occurs today in the context of manned flight using technologies like autopilot.) In discussions about UAS integration, there is often an assumption that autonomous unmanned UAS will pose more dangers than human-piloted UAS. I believe that is an oversimplification.

Certainly, autonomous UAS flight without the proper safeguards would pose very real safety risks. But when the algorithms used to control flight are designed with sufficient care and properly tested, autonomous flight has the potential to deliver very important benefits, including enabling new applications such as the automated search and rescue scenario that I discuss below.

### AUTONOMOUS, BEYOND-LINE-OF-SIGHT UAS OPERATION

UAS flight that is both autonomous and beyond-line-of-sight (BLOS) is another important area of technology development. BLOS refers to operation in which the UAS cannot be seen by a person overseeing its operation—either because it is obscured by intervening objects such as trees or buildings, or because it is over the horizon.<sup>49</sup>

BLOS and autonomous flight are not necessarily coupled. Today's technology makes it possible (though it is not generally permitted<sup>50</sup> in the current regulatory environment) for a ground-based human pilot to fly a UAS beyond the line of sight using a computer, console, or other display system showing live video from a UAS-mounted camera. The pilot sees what he or she would see from onboard the UAS, and can navigate the aircraft accordingly, despite not being able to actually see the UAS from his or her location on the ground.<sup>51</sup> This is an example of BLOS flight that is *not* autonomous. Conversely, autonomous UAS flight could be performed in very close proximity to—and within view of—the person who initiated the flight. This is an example of autonomous flight that is *not* BLOS.

But some of the most compelling future applications of UAS involve flight that is *both* autonomous *and* BLOS. Consider the challenge of looking for a lost hiker in the wilderness at night, several miles from the nearest road. It could be very helpful to be able to program a UAS to fly autonomously to the search area, and then to fly automated search patterns, using a thermal imager to identify heat signatures that may indicate the lost hiker. Upon finding a possible match, the UAS could then alert a human pilot, who would then retake control and use the UAS to perform a closer inspection to see if the hiker had indeed been located. To take this example one step further, it would be possible to have half a dozen UAS collaboratively perform a search. This would allow searches to be conducted much faster and much more cost effectively than is possible today using manned aircraft.

**<sup>48</sup>** Autonomy is actually a continuum, depending upon the level of control over the flight maintained by an on-the-ground human pilot.

**<sup>49</sup>** I am referring here to beyond the *visual* line of sight, in which the UAS operator cannot see the UAS. In some other contexts, the term "line of sight" is used to in association with whether or not there is direct radio communication with the UAS, without any need to relay the radio signal through an intermediate location.

<sup>50</sup> There is an exception under which, in regions of arctic Alaska, certain beyond-line-of-sight UAS operations are permitted. See <u>http://www.faa.gov/news/updates/?newsId=73981</u>

<sup>51</sup> This type of flight is called "first person view" or "FPV."

Under current regulations (as well as those proposed in the recent NPRM), a UAS flight operation of this sort would not be permissible.<sup>52</sup> In addition, it is currently very difficult for companies or government agencies interested in developing this capability to even *test* these capabilities. Rules at the six UAS test sites recently chosen by the FAA currently prohibit flight that is simultaneously BLOS and autonomous. This forces developers of this technology to either limit their testing to the small confines of indoor spaces, or to test overseas in a country where the rules relating to autonomous UAS flight offer more flexibility.

Today, UAS technology is not yet sufficiently mature to allow autonomous, beyond-line-of-sight UAS operations in the regular (outside of suitable test sites) airspace. But I think it is important to move towards a regulatory framework that could provide a mechanism to safely test and refine these technologies. This could occur, for example, in regions within the already-designated FAA test sites and/or on large parcels of private property owned or leased by the company performing the tests.

#### PROMOTING INNOVATION AND ECONOMIC PROSPERITY

In the coming years, UAS will be used to improve agricultural yields, to perform scientific research, to spot and fight forest fires, to perform search and rescue, and to support disaster response. Developing the UAS technologies to enable these and many other applications will involve new business models, new companies, and new jobs. But that will only occur if there is a regulatory climate that fosters a thriving community of companies and individuals with an interest in investing their time, money, and energy to create the safest, most innovative unmanned aircraft technologies of the future.

While there has been plenty of attention to the important issue of commercial UAS, I would also like to highlight the importance of the unmanned aircraft hobbyist community. This community, which includes both model airplane hobbyists as well as those who fly what are commonly called "drones," provides a critically important pipeline for careers in aviation and technology. I would urge the FAA and Congress to ensure that as we navigate the complex process of making and interpreting rules for unmanned aircraft, we keep in mind the vital importance of the hobbyist community for our future innovation capacity.

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

#### **GOVERNANCE STUDIES**

The Brookings Institution 1775 Massachusetts Ave., NW Washington, DC 20036 Tel: 202.797.6090 Fax: 202.797.6144 brookings.edu/governance

PRODUCTION & LAYOUT Nick McClellan The views expressed herein are those of the author and should not be attributed to the staff, officers or trustees of the Brookings Institution.

<sup>52</sup> Under the NPRM, operators of "small" UAS would be required to be "visually capable of seeing the small UAS", i.e., BLOS operations would not be permitted.