COMPETITIVE ENTERPRISE INSTITUTE

OnPOINT

October 14, 2015 **No. 211**

Keeping the Skies Open for Drones

A Pro-Market Approach to Privacy and Airspace Management

By Marc Scribner[*]

"Kentucky man shoots down drone spying on 16-year-old daughter."[1]

"Goodbye, privacy: 'Selfie-drones' will hover over vacationers."[2]

These recent, attention-grabbing headlines illustrate the sorry state of the current public discussion on the use of civilian unmanned aircraft systems (UAS).

Not only are UAS, particularly small unmanned aircraft systems (sUAS), often portrayed in a negative light, these reports and commentaries are often riddled with factual inaccuracies and glaring omissions. For example, the Kentucky man who claimed he was protecting his daughter's privacy may not have been entirely truthful to his arresting officers. In the days following the incident, the sUAS operators released data and video footage seemingly contradicting the man's claims.[3]

The notion that we face a binary choice between privacy and enjoyment of UAS services ignores the adaptability of existing privacy and harassment law to deter and hold operators accountable for the breaches that worry so many.

This paper addresses two major concerns often cited by supporters of more government intervention into the emerging UAS market: privacy and air traffic management. Contrary to claims that the only solution to UAS challenges is more government, the private sector and existing laws are well equipped to handle the future deployment of UAS technology.

In any discussion of potential costs, it is important to keep in mind the potential benefits. UAS offer great potential benefits in improved precision agriculture, aerial surveying and photography, infrastructure inspection, disaster response, parcel delivery, and other applications. The commercial UAS market is expected to grow substantially in coming years, with a 2013 industry forecast suggesting total nationwide economic benefits of $82.1 billion by 2025.[4] Policy makers should recognize that misguided policy can have dire consequences for a nascent technology and proceed with caution.

According to the National Conference of State Legislators, as of October 8, 45 states have considered 166 bills related to UAS in 2015.[5] Of these, 20 states passed legislation and four adopted resolutions related to UAS operations.[6] This brings the total number of states with

[*]*Marc Scribner is a fellow at the Competitive Enterprise Institute.*

UAS statutes on the books to 26.[7] In addition, numerous municipalities have attempted to codify UAS operations as either permissible or impermissible.

The aims of UAS-related legislation vary widely. State and local governments have sought to address real or perceived UAS problems associated with critical infrastructure,[8] agricultural use,[9] voyeurism,[10] law enforcement applications,[11] and hunting and fishing,[12] among other concerns. Maryland stands out in that it has explicitly preempted counties and municipalities from regulating or prohibiting UAS operations.[13]

The motivations behind these bills appear sincere. However, other than the Maryland bill preempting localities and attempts to define appropriate law enforcement uses, UAS legislation is at best unnecessary.[14] At worst, it will excessively burden UAS developers and operators in those states.

The Federal Aviation Administration (FAA) is in the process of developing national rules for sUAS.[15] Before proceeding with potential legislative remedies to real or perceived problems associated with civilian UAS operations, state and local governments should at the very least wait until the FAA finalizes the basic sUAS regulatory framework, which the agency is expected to promulgate before the end of the decade.

Privacy. Much of the negative publicity surrounding civilian unmanned aircraft systems involves malicious surveillance, such as spying into the windows of private residences. Several state legislatures have taken up bills to address these perceived privacy risks. However, most of these legislative proposals ignore actual privacy risks and existing laws that protect individual privacy from malicious UAS surveillance.

First, the common law already affords civil remedies to people whose privacy is invaded by UAS.[16] As the *Restatement (Second) of Torts*, an influential treatise that summarizes widely adopted principles of tort law in the United States, explains:

> One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person.[17]

Importantly, under this doctrine, the touchstone of liability is the offensiveness of the intrusive observation. It does not matter *how* a person wrongfully intrudes upon the privacy of another, nor whether the intrusion is visually captured or published.

Second, states universally offer additional privacy protections through criminal statutes.[18] Much like privacy torts, these statutes focus not on the specific devices used to commit surveillance crimes, but on the underlying nature of the conduct. As UAS legal expert Brendan Schulman notes: "If I'm taking pictures through a window and I use a broom stick instead of a drone, it's the invasive behavior that concerns lawmakers—not what you use."[19]

Some states offer more robust criminal surveillance protections than others. For instance, Alabama offers perhaps the weakest protections, as its criminal surveillance statute proscribes video and still photography only if such surveillance is conducted while trespassing on private property.[20] Given that malicious UAS operators may not always commit the act of trespassing in the traditional sense, Alabama's statute could offer stronger protections that better reflect public expectations of privacy. To strengthen the privacy protections contained in the state's criminal surveillance statute, lawmakers should consider two legislative approaches.

First, Alabama could expand the reasonable expectation of privacy standard already contained in its *aggravated* criminal surveillance statute, which does not turn on whether the offender engaged in trespassing. Instead, that statute makes it a crime to "intentionally engage[] in surveillance of an individual in any place where the individual being observed has a reasonable expectation of privacy, without the prior express or implied consent of the individual being observed, for the purpose of sexual gratification."[21] However, the voyeurism requirement that the offender surveil the individual being observed do so "for the purpose of sexual gratification" is obviously too narrow to protect against potential UAS privacy violations that concern the public.

Second, Alabama could extend property rights further into the air so that the trespassing standard becomes more effective in protecting against a broader class of UAS privacy violations. Applying property rights to airspace is rooted in precedent. The Supreme Court held in *United States v. Causby* that "airspace at this low altitude is so close to the land that continuous invasions of it affect the use of the surface of the land itself. We think that the landowner, as an incident to his ownership, has a claim to it, and that invasions of it are in the same category as invasions of the surface."[22] *Causby* involved a North Carolina farmer whose chickens kept dying due to regular military overflights as low as 83 feet above his property. While rejecting the common law *ad coelum* doctrine, which held that a property owner's rights extend to the heavens,[23] the Court nonetheless ruled in Causby's favor and granted him compensation under the Fifth Amendment's Takings Clause.

In a recent Brookings Institution paper, Pepperdine University law professor Gregory McNeal proposed to amend state laws to provide property owners with a cause of action when a UAS operator flies below 350 feet above ground level for the purpose of violating privacy.[24] This would provide a 150-foot buffer between private property and the minimum navigable airspace altitude of 500 feet.[25] To be sure, punishing trespassers who aim to violate another's privacy within the 350-foot column above private land would not protect against all UAS privacy violations, but it would offer far more protections from UAS invasions of privacy than current law.

McNeal's approach is intriguing and avoids many of the pitfalls of technocratic regulatory approaches. However, under current FAA guidance that limits UAS operations to 400 feet above ground level, this would allow only 50 feet of airspace for UAS to operate without risking accusations of unlawful surveillance.[26] This meager operating window is unlikely to satisfy recreational, commercial, and research UAS operators, and may retard UAS testing and development.

In addition, California legislators recently attempted to codify a 350-foot trespassing standard.[27] The problem, as McNeal noted, is that the California bill would have deemed any UAS operating below 350 feet above ground level without the express permission of the private property owner to be trespassing, regardless of whether the operator knowingly did so or intended to snoop on someone.[28] Thankfully, California Governor Jerry Brown vetoed the bill.[29] Unfortunately, the aborted California approach is likely to reappear in future legislation.

Given these policy alternatives and tradeoffs, the best current course of action is likely no action, beyond perhaps restricting law enforcement use of UAS.[30] The UAS sector is expected to grow substantially in the coming years. In addition, at the direction of President Obama,[31] stakeholders are currently working within a National Telecommunications and Information Administration framework to develop national UAS privacy and civil liberties best practices.[32] Exercising policymaking restraint as this nascent technology evolves may prevent early political missteps that have the potential to lock in counterproductive legal regimes.

Airspace Management. Congress is currently considering major reforms to U.S. air traffic control, likely by spinning off the FAA's Air Traffic Organization into an independent, nonprofit air navigation service provider, similar to the reforms that led to the creation of Nav Canada in the 1990s.[33] At the same time, the agency is busy attempting to comply with the FAA Modernization and Reform Act (FMRA) of 2012, in which Congress ordered the FAA to complete "the safe integration of civil unmanned aircraft systems into the national airspace system as soon as practicable, but not later than September 30, 2015."[34]

The FAA has not met the FMRA airspace integration deadline, but the reality is even worse. It was only in February 2015 that it opened its required UAS integration rulemaking—which only applies to sUAS under 55 pounds.[35] Further, its proposed rules rely on dubious legal authority and would prohibit a variety of useful UAS operations such as flying beyond an operator's line of sight, flying at night, autonomous flying, and other activities.[36] A recent Government Accountability Office report found that the FAA is unlikely to finalize its sUAS rule until late 2016 or 2017—a partial step toward complying with Congress's 2012 FRMA airspace integration mandate and over a year late.[37]

Clearly, the FAA has bungled the integration of UAS into the airspace. What can be done to improve the regulatory landscape?

While the FAA will retain safety regulatory authority under any of the alternative institutional frameworks, one reasonable possibility is transferring UAS air traffic management responsibility away from the FAA and to another entity. This option is supported by many in the UAS industry.

The National Aeronautics and Space Administration (NASA) has convened a group of stakeholders to develop an Unmanned Aerial System (UAS) Traffic Management (UTM)

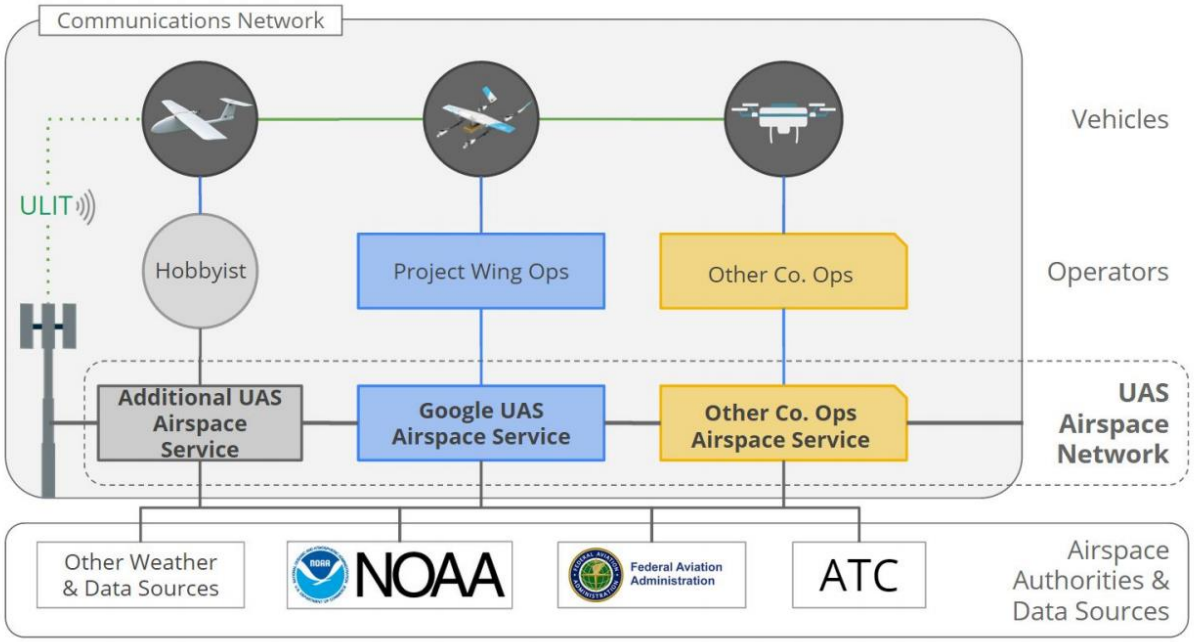
framework for low-altitude sUAS.[38] Noted private participants include Amazon, Google, and Verizon. As currently envisioned, there will be two forms of UTM: portable and persistent.[39] Portable UTM can be deployed on the fly to support operations such as precision agriculture and disaster relief. Persistent UTM relies on a fixed infrastructure continuously covering a specific geographical area, enabling regular operations such as parcel delivery.

UTM conference organizers still officially plan to turn over the system to the FAA once it is completed, estimated in 2019. However, both Google and Amazon have proposed UTM frameworks that rely on the delegation of traditional FAA air traffic control responsibility to private parties.[40]

Google's model is most explicit in this regard, as the figure below shows a federated system of private sUAS air navigation service providers (ANSP), each of which manages specific sUAS product lines or activities.

Google's UTM diagram of federated UAS airspace network managers

ASPs connect data and authorities (ATC) to UAS operators and vehicles over comms networks.



ASPs can be implemented by any qualifying organization. These ASPs comprise a federated network.

Source: Google UAS Airspace System Overview

Under this federated approach, airspace managers can implement UAS technology that best suits their and their customers' needs. In addition, these UAS ANSPs would be privately funded and operated, perhaps excluding the hobbyist market. Again, the FAA would retain safety regulatory and licensing authority, but would not face the common tension—and fiscal constraints—between the competing missions of managing the airspace efficiently and managing it safely. Adopting something similar to Google's approach to airspace

management would greatly speed the deployment of new sUAS technology and resulting benefits to firms and consumers.

One harmful airspace management technique that has been gaining steam is requiring all UAS include what is known as geofencing technology, which can prohibit operations within a certain predefined area.[41] No-fly zones can be established either by preprogrammed software aboard the UAS that has a registry of prohibited areas or by ground infrastructure that sends a radio signal to a receiver on the UAS to prevent it from entering a geofenced zone or shut it down as it enters geofenced area. Sen. Charles Schumer (D-N.Y.) has been the most vocal proponent of a geofencing mandate and will likely to try to include legislative language to accomplish as much in the forthcoming FAA reauthorization.[42]

There are two major problems with Sen. Schumer's approach. First, concerns over malicious airspace invaders—whether peeping toms or terrorists—are unlikely to be addressed by a geofencing mandate. When Chinese UAS manufacturer DJI began including geofencing technology on its Phantom series vehicles, a hack was posted online within four days of DJI's firmware update.[43] As UAS safety consultancy Wolf Unmanned Air Systems notes:

> Geofencing is only reliable in conditions where full communications to either a GPS satellite, a remote control operator, or both, are maintained. So, this technology is only reliable in the conditions where UAVs are least likely to cause a problem. Furthermore, the software required to delineate an "off-limits" area or height is easily accessible and manipulated.[44]

Second, there is the question of what to do with the existing civilian UAS fleet in the U.S., whose number is estimated at approximately 1 million. Would a mandate, which would take years to develop and risks locking in obsolete technology, require a nationwide retrofitting of pre-mandate UAS? Who would pay for this? How would it be enforced? These are questions proponents of geofencing mandates have been unable to answer.[45] Until they can—which appears unlikely—wise policy makers should ignore their calls for more intrusive government regulation.

Conclusion. UAS technology offers to transform the way we live and work. This will bring many benefits, but as with any new technology, there are challenges. UAS can be used by criminals and could potentially complicate airspace management. Yet, this does not mean that government must engage in a flurry of legislating and rulemaking. On the contrary, existing law and the private sector are clearly equipped to deal with many of these challenges.

The biggest risks with respect to UAS are well-meaning but overzealous policy makers eager to legislate or regulate in a manner that would restrict or prohibit future UAS applications. This does not mean legislators and regulators should not follow the evolution of UAS closely. To be sure, statutory and regulatory changes will be needed in the future. But policy makers must understand that UAS technology is currently in its infancy and that rash actions, however well-intentioned, are likely to do more harm than good.

Notes

[1] Mike Wehner, "Kentucky man shoots down drone spying on 16-year-old daughter," The Daily Dot, July 30, 2015, http://www.dailydot.com/technology/kentucky-drone-shooting/.
[2] Stephanie Rosenbloom, "The Selfie-Drone: Invasion of the Vacation Snatchers," *The New York Times*, August 31, 2015, http://www.nytimes.com/2015/09/06/travel/selfie-camera-drones.html.
[3] Cyrus Farivar, "Video: Kentucky drone only hovered for about 22 seconds before being shot down," Ars Technica, August 10, 2015, http://arstechnica.com/tech-policy/2015/08/video-kentucky-drone-only-hovered-for-about-22-seconds-before-being-shot-down/.
[4] Darryl Jenkins and Bijan Vasigh, "The Economic Impact of Unmanned Aircraft Systems Integration in the United States," Association of Unmanned Vehicle Systems International, March 2013, https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf.
[5] National Conference of State Legislators, "Current Unmanned Aircraft State Law Landscape," NCSL website, August 26, 2015, http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx.
[6] Ibid.
[7] Ibid.
[8] Ark. Code § 5-60-103 (2015).
[9] 2015 La. Sess. Law Serv. Act 166 (S.B. 183).
[10] 2015 Miss. Laws Ch. 489 (S.B. 2022).
[11] 2015 Me. Legis. Serv. Ch. 307 (H.P. 24) (L.D. 25).
[12] 2015 New Hampshire Laws Ch. 38 (S.B. 222).
[13] 2015 Maryland Laws Ch. 164 (S.B. 370).
[14] However, attempts to prevent potential law enforcement abuses may well go awry. Marc Scribner, "Did North Dakota Just Authorize Pepper-Spraying Police Drones?" Competitive Enterprise Institute blog, August 27, 2015, https://cei.org/blog/did-north-dakota-just-authorize-pepper-spraying-police-drones.
[15] Operation and Certification of Small Unmanned Aircraft Systems, *Notice of Proposed Rulemaking*, FAA-2015-0150, 80 Fed. Reg. 9543 (February 23, 2015) [hereinafter sUAS NPRM].
[16] Restatement (Second) of Torts § 652B (1977). William L. Prosser, "Privacy," *California Law Review*, Vol. 48, No. 3, August 1960, pp. 383-423.
[17] Ibid.
[18] For a recent compilation of state surveillance statutes, see National District Attorneys Association, "Voyeurism Statutes 2009," March 2009, http://www.ndaa.org/pdf/voyeurism_statutes_mar_09.pdf.
[19] Christina Sterbenz, "Should We Freak Out About Drones Looking In Our Windows?" Business Insider, September 24, 2014, http://www.businessinsider.com/privacy-issues-with-commercial-drones-2014-9.
[20] Ala.Code 1975 § 13A-11-32.
[21] Ala.Code 1975 § 13A-11-32.1.
[22] *United States v. Causby*, 328 U.S. 256 (1946).
[23] Ibid. See also *Black's Law Dictionary* (10th ed. 2014), ad coelum doctrine: "The common-law rule that a landowner holds everything above and below the land, up to the sky and down to the earth's core, including all minerals."
[24] Gregory McNeal, "Drones and Aerial Surveillance: Considerations for Legislators," Brookings Institution, November 2014, p. 15, http://www.brookings.edu/~/media/Research/Files/Reports/2014/10/drones-aerial-surveillance-legislators/Drones_Aerial_Surveillance_McNeal_FINAL.pdf.
[25] 14 C.F.R. § 91.119(c).
[26] Federal Aviation Administration, *Model Aircraft Operating Standards*, Advisory Circular 91-57A, September 2, 2015, § 6(e): "Model aircraft operators should follow best practices including limiting operations to 400 feet above ground level (AGL)."
[27] Senate Bill 142, 2015-2016 Reg. Sess. (Cal. 2015).
[28] McNeal, "California's Drone Trespass Bill Goes Too Far, Forbes.com, August 11, 2015, http://www.forbes.com/sites/gregorymcneal/2015/08/11/californias-drone-trespass-bill-goes-too-far/.
[29] California Gov. Jerry Brown, Veto Message for Senate Bill 142, September 9, 2015, https://www.gov.ca.gov/docs/SB_142_Veto_Message.pdf.

[30] Unfortunately, we have already observed the unintended consequences of legislators attempting to restrict law enforcement use of UAS. Scribner, "Did North Dakota Just Authorize Pepper-Spraying Police Drones?"
[31] Barack Obama, *Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems*, Presidential Memorandum, February 15, 2015, https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.
[32] Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems, *Request for Public Comment*, Docket No. 150224183-5183-01, 80 Fed. Reg. 11978 (March 5, 2015).
[33] For a comprehensive review of air traffic control reform options, and the experience in Canada, see Robert W. Poole, Jr., "Organization and Innovation in Air Traffic Control," Hudson Institute, November 2013, http://dev.hudson.org/content/researchattachments/attachment/1199/poole_hi_res.pdf.
[34] FAA Modernization and Reform Act of 2012, Pub. L. 112-95, 126 Stat. 73 (2012).
[35] sUAS NPRM, *supra* note 15.
[36] Comments of the Competitive Enterprise Institute in re: sUAS NPRM, April 24, 2015, pp. 1-3, https://cei.org/sites/default/files/Marc%20Scribner%20-%20Comments%20of%20Competitive%20Enterprise%20Institute%20in%20FAA-2015-0150.pdf.
[37] Government Accountability Office, "Unmanned Aerial Systems: FAA Continues Progress toward Integration into the National Airspace,"GAO-15-610, July 16, 2015, http://www.gao.gov/products/GAO-15-610.
[38] National Aeronautics and Space Administration, "UTM Fact Sheet," UTM website, accessed September 16, 2015, http://utm.arc.nasa.gov/docs/UTM-Fact-Sheet.pdf.
[39] Ibid.
[40] Amazon.com, Inc., "Revising the Airspace Model for the Safe Integration of Small Unmanned Aircraft Systems," UTM website, accessed September 16, 2015, http://utm.arc.nasa.gov/docs/Amazon_Revising%20the%20Airspace%20Model%20for%20the%20Safe%20Integration%20of%20sUAS[6].pdf; *and* Google Inc., "Google UAS Airspace System Overview," UTM website, accessed September 16, 2015, http://utm.arc.nasa.gov/docs/GoogleUASAirspaceSystemOverview5pager[1].pdf.
[41] Kevin Poulsen, "Why the U.S. Government Is Terrified of Hobbyist Drones," *Wired*, February 5, 2015, http://www.wired.com/2015/02/white-house-drone/.
[42] Michael Balsamo, "Schumer wants to keep drones way from airports, major events," Associated Press, September 13, 2015, http://hosted.ap.org/dynamic/stories/U/US_DRONES_AIRPORTS.
[43] Wolf Unmanned Air Systems, "Does GeoFencing Work? No." Wolf UAS website, February 2, 2015, http://wolfuas.com/2015/02/02/does-geofencing-work-no/.
[44] Ibid.
[45] Alan Levin, "Can You Curb Wayward Drones with a Dog Fence in the Sky?" Bloomberg, August 31, 2015, http://www.bloomberg.com/news/articles/2015-08-31/aerial-dog-fences-can-t-be-counted-on-to-curb-wayward-drones.