Issues in GOVERNANCE STUDIES

Number 55 December 2012

Unmanned at Any Speed: Bringing Drones into Our National Airspace

Wells C. Bennett

Wells C. Bennett is a visiting fellow in National Security Law at the Brookings Institution. He focuses on legal matters related to the war on terror and national security, including the military commission trials at Guantanamo Bay.

EXECUTIVE SUMMARY

On February 14 of this year, President Obama signed the Federal Aviation Administration Modernization and Reform Act of 2012 ("FMRA").[1] The new law's plain-sounding title doesn't tell you, but FMRA encompasses a bold and controversial project: allowing, by a date certain, much wider domestic operation of Unmanned Aircraft Systems ("UAS") – or, as they are more commonly described, "drones."[2]

Reuters: The remotely piloted drone is used to detect undocumented immigrants entering the United States illegally from Mexico.

These machines spark passionate debate. For some, their proliferation spells the demise of our civil liberties: a sky full of flying robots carrying cameras and maybe even weapons. Others dismiss these complaints as caricatures, and insist that UAS should fly more often, and in greater numbers than they do nowadays. Proponents see a cost-effective means of ensuring sustainable agriculture, mitigating the effects of natural disasters, mapping unexplored terrain, detecting atmospheric events, hunting down crooks, and preventing commuter gridlock. FMRA does not resolve these debates, but seems nevertheless to chalk up a win for the second group – if only because the statute makes it easier for more drones to share our airspace.

[1] Pub. L. 122-95 (Feb. 14, 2012). All statutory references are to FMRA unless otherwise noted.

[2] Other acronyms abound, including "unmanned aerial vehicle" ("UAV") and remotely piloted vehicle ("RPV.") The term "drone" is inaccurate, as humans almost always control the aircraft, though not from onboard the aircraft itself.

Under the statute, the task of mainstreaming drones belongs to the executive branch, with the Federal Aviation Administration ("FAA") leading a pack of stakeholder offices including NASA and the Departments of Defense and Homeland Security. The timetable is ambitious. FMRA requires the FAA to develop a long-term policy for bringing UAS into our skies by late 2015. In the interim, the agency also must meet several other milestones: among other things, the FAA must devise a fast-track procedure to permit law enforcement and other government agencies to operate smaller-sized aircraft; and create an experimental program to fly drones in the Arctic.

The timetable is ambitious. FMRA requires the FAA to develop a long-term policy for bringing UAS into our skies by late 2015.

What follows is a brief primer on domestic drone integration. Its first part overviews FMRA's most important deadlines; a second section reviews the FAA's progress in meeting them. The third describes the legal and historical backdrop to FMRA. The piece's fourth part outlines some of the broader policy questions that must be resolved, in order to allow for broader drone use. The primer's fifth section offers concluding thoughts.

The Statutory Timetable

FMRA's UAS provisions function like a big, jumbled timetable.[3] Not all of them contain cut-off dates, or talk about timing issues. One defines terms of art like "small unmanned aircraft" (weighing under 55 pounds) and "sense and avoid capability" (unshockingly enough, the ability to "remain a safe distance from and to avoid collisions with other airborne aircraft").[4] Another directs the FAA to carry out any safety studies needed in order to accomplish UAS integration. And a third generally disallows the agency from promulgating new rules for model aircraft, provided these satisfy certain criteria.[5] At the same time, FMRA's most consequential UAS-related sections each charge the FAA with achieving a particular, drone-related milestone, on or before a particular date.[6] In these, Congress drew on aviation law's longstanding distinction between public aircraft (generally, those operated by governments for

[3] FMRA deals briskly with UAS matters – as good an indication as any of Congress's intention to leave the hard stuff to the FAA and related agencies. For the most part, the project of domestic UAS integration is sketched out in six provisions, themselves spread over a scant seven pages of legislation. *See generally* Sec. 331-336. Elsewhere, the law specifically authorizes research into, among other things, systemic risks caused by UAS integration and the relationship between human- and robot-controlled flights. These provisions do not, however, purport to alter the legal regime regarding domestic UAS operations. *See* Sec. 901(g)(12), 903(a), (b). Yet brief does not necessarily mean simple; quite the opposite in this case.

[4] Sec. 331(5), (6).

[5] Sec. 336(a)(1)-(5) (precluding the issuance of new rules for model aircraft if, among other things, the latter is flown strictly as a hobby or for recreational use, according to guidelines set by a community-based organization, and in a manner that does not interfere with and gives way to any manned aircraft); Sec. 336(c)(1)-(3) (defining "model aircraft" as an unmanned aircraft capable of sustained flight in the atmosphere; flown within visual line of sight of the person operating the aircraft, and as a hobby or for recreational purposes).

[6] *See generally* Sec. 332 (outlining timetable for civil UAS integration), Sec. 333 (obligating Secretary of Transportation to identify any UAS that can be operated safely, pending issuance of long-term policies for private and public UAS), Sec. 334 (outlining timetable for public UAS integration).

governmental purposes) and civil aircraft (generally, those operated on a private basis).[7] The FMRA calendar thus sets forth three kinds of deadlines: one applicable to public UAS only, another to civil UAS only, and a third kind applicable to both.

"Deadline" may be too strong a term. In places, FMRA employs vaguely-worded objectives, and it doesn't always require the agency to take precisely measurable steps. There is no penalty for tardiness in the statute, for example. If the FAA misses a must-do-by date, the agency may have to reckon with congressional pressure and stakeholder disapproval. But there's no formal compliance mechanism to hurry the agency along. In this and other ways, FMRA leaves the FAA some room to maneuver, and can sow confusion about precisely what the agency must achieve between now and 2015.

We examine, below, what FMRA requires of the FAA, and by what dates; and next, what the FAA has done so far in order to comply with the statutory calendar.[8]

Public UAS

Let's start with the first category of UAS: public, or government operated systems. According to FMRA, no later than **May 14, 2012,** the Secretary of Transportation had to "enter into agreements with appropriate government agencies to simplify the process for issuing certificates of waiver or authorization" with respect to UAS operated by first responders – police departments, fire departments, and the like.[9] The statute here refers to the FAA's longstanding *ad hoc* approach to licensing domestic drone operations. Right now, in order to fly their drones in U.S. airspace, federal, state and local governments must apply for and obtain a "certificate of waiver or authorization" ("COA") from the FAA. The arrangement is necessary because UAS cannot literally comply with federal aviation rules, which were designed long ago and with only manned aircraft in mind. The simplifying agreements must provide for approval or disapproval of a first responder's COA application within 60 business days; and "allow a government public safety agency to operate unmanned aircraft weighing 4.4 pounds or less" if, among other things, the UAS is operated within the operator's line of sight, during daylight conditions, and

[7] *See* Sec. 331(4) (defining ''public unmanned aircraft system'' as "an unmanned aircraft system that meets the qualifications and conditions required for operation of a public aircraft (as defined in section 40102 of title 49, United States Code)"; 49 U.S.C. § 40102 (41)(A)-(E) (setting forth criteria for "public aircraft," and generally requiring such aircraft to be operated by or for the benefit of a federal, state or local government).

Strangely, FMRA does not also define the term "civil unmanned aircraft system." That said, federal statutes elsewhere define "civil aircraft" to mean any aircraft except for public aircraft. *Id.* § 40102 (17). It thus stands to reason that any unmanned aircraft system that does not qualify as "public" ought then to be considered "civil" for FMRA purposes – though the statute's text does not literally require this.

[8] Unless otherwise noted, deadlines are derived from FMRA's express language – which, with some exceptions, describes its key dates generally but does not identify them by month, day, and year. "Before November 10, 2012**,**" for example, is derived from the statutory phrase "not later than 270 days after the enactment of this act."

[9] *See* Sec. 334(c)(1). For a summary of FMRA deadlines, see Harley Geiger, "Drone Countdown," Center for Democracy and Technology (Mar. 27, 2012).

below 400 feet in altitude.[10] This was the earliest of FMRA's key deadlines – a reflection of Congress's desire quickly to get more small UAS technology into the hands of law enforcement.

The next milestone came on **November 10, 2012**. On or before that date, the FAA was required to issue "guidance" regarding the operation of public UAS in the United States. In connection with this, the FAA also had to expedite the COA process for government agencies whose drones are not covered by FMRA's fast-track provision for first responders.[11] Finally, the statute hands down an explicit deadline for standards regarding the operation and certification of public UAS. These must be "implement[ed]" no later than **December 31, 2015**.[12] (Notwithstanding its call for implementation, FMRA does not specifically instruct the FAA to engage in a rulemaking regarding public UAS.)

Civil UAS

Civil UAS proceed on a parallel, if slightly slower track. For these, the first key deadline was **November 10, 2012**. On or before that date, the FAA had to "develop" – not "publish" or "make available," but *develop* – a "comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system" (the "Comprehensive Plan").[13] In this document, the FAA was to make recommendations for UAS safety and licensing standards, and employ a "phased-in approach" to integration.[14] Importantly, the Comprehensive Plan also had to harmonize with our country's ongoing transition to the Next Generation Air Transportation System, or "NextGen" – a modernized, satellite-based aviation management scheme that, sometime between now and 2025, will address the exponentially increasing volume of aviation operations in the United States.[15] Having been "developed," the Comprehensive Plan must be submitted Congress, no later than **February 14,**

---

[10] Sec. 334(c)(2)(A)(ii), (C)(i)-(iii).

[11] Sec. 334(a)(1).

[12] Sec. 334(b).

[13] Sec. 332(a)(1).

[14] Sec. 332(a)(2)(A)(i)-(iii), (C).

[15] *Id.* The FAA website describes NextGen as a "wide ranging transformation of the entire national air transportation system – not just certain pieces of it – to meet future demands and avoid gridlock in the sky and in the airports." "Fact Sheet – NextGen" *available at* http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=8145. NextGen encompasses many different reform projects, but its core is Automatic Dependent Surveillance Broadcast, or "ADS-B." According to the FAA, by means of this technology

> [a]ircraft transponders receive GPS signals and use them to determine the aircraft's precise position in the sky, which is combined with other data and broadcast out to other aircraft and air traffic control facilities. When properly equipped with ADS-B, both pilots and controllers will, for the first time, see the same real-time displays of air-traffic, substantially improving safety.
>
> *Id.*

2013.[16]

Agency processes kick in soon afterwards, with separate rulemakings scheduled for "small" UAS – again, those weighing less than fifty-five pounds – and their larger counterparts. With respect to the former, the FAA must publish a final rule no later than **August 14, 2013.**[17] As for the latter, the agency has until **August 14, 2014**, to issue a notice of proposed rulemaking regarding the Comprehensive Plan, with a final rule to follow no less than sixteen months later – that is, sometime prior to **December 30, 2015**.[18]

It thus appears that, in devising the FMRA calendar, Congress didn't do its math properly. Or that it engaged in some clunky and needless wordplay (can the FAA "provide" for integration on one date, accomplish integration afterwards, and still comply with the statute?).

This latter arrangement seems to contradict another part of the statute. Oddly enough, FMRA also contains what it refers to as a "deadline":

> [The Comprehensive Plan] shall provide for the safe integration of civil unmanned aircraft systems into the national airspace system as soon as practicable, *but not later than* ***September 30, 2015***.[19]

It thus appears that, in devising the FMRA calendar, Congress didn't do its math properly. Or that it engaged in some clunky and needless wordplay (can the FAA "provide" for integration on one date, accomplish integration afterwards, and still comply with the statute?). Whatever the legislature's precise objectives, at least this much is clear: Congress undeniably wants the FAA to open our skies to civil UAS, in a systemic fashion, by late 2015. This marks what is perhaps the most important policy shift announced by FMRA. At present, current law disallows private drone operations, save only those involving research and development, market surveys and crew training. But that will change if integration proceeds according to plan. Commercial, for-hire drone activities – think TacoCopter – could be permitted about three years from now.

All UAS

Only one deadline applies to private and public drones alike: **August 12, 2012**. On or before that date, the Secretary of Transportation needed to "determine if certain unmanned aircraft systems may operate safely in the national airspace system before completion of the [Comprehensive Plan and rulemaking for civil UAS] . . . or the guidance required [for public UAS]."[20] Despite the suggestion, a favorable determination does not amount to a green light to fly unfettered. The Secretary still could, for example, require a COA

[16] Sec. 332(a)(4).

[17] Sec. 332(b)(1).

[18] Sec. 332(b)(2).

[19] Sec. 332(a)(3) (emphasis added).

[20] Sec. 333(a).

before the aircraft can operate.[21] The statute thus vests the FAA with discretion to calibrate just how fast, or slow, the pre-clearance scheme would be – and to create an interim process that mostly resembles the *status quo*.

Thus we may yet see a Congressional-Executive agreement on the United States' operation of drones in the Arctic – where, among others, Canada plans soon to fly its drones, too.

The August 12 date governed two more key initiatives. The first was a five-year program of UAS test flights. Sometime before the deadline, "the Administrator [was required to] establish a program to integrate unmanned aircraft systems into the national airspace system at 6 test ranges."[22] This called for, among other things, development of certification standards and air traffic requirements for test flights at the six ranges, coordination with NASA and the Department of Defense, and harmonization with NextGen activities.[23] Experimental projects, moreover, must commence within 180 days of a test site's selection;[24] the agency must report to Congress about these within 90 days of the program's termination, in 2017.[25]

The other all-UAS project concerned the Arctic. With this impenetrable phrase, Congress obligated the Secretary of Transportation, on or before August 12, to

> *develop* a *plan* and *initiate* a *process* to *work* with *relevant Federal agencies and national and international communities* to designate permanent areas in the Arctic where small unmanned aircraft may operate 24 hours per day for research and commercial purposes.[26]

One strains to glean meaning here. Thankfully, Congress opted for clearer language in describing other facets of its agenda for the Arctic. The round-the-clock Arctic drones will fly beyond the line of sight, and over water.[27] In order to ensure that they do, and to carry out FMRA's other objectives regarding the region, the Secretary of Transportation "may enter into an agreement with relevant national and international communities."[28] On the latter, Congress likely has in mind the International Civil Aviation Organization, which has jurisdiction over certain arctic airspace. Thus we may yet see a Congressional-Executive agreement on the United States' operation of drones in the Arctic – where,

[21] Sec. 333(c).

[22] Sec. 332(c)(1).

[23] Sec. 332(c)(2)(B), (C), (E).

[24] Sec. 332(c)(4).

[25] Sec. 332(c)(5), (a)(1).

[26] Sec. 332(d)(1) (emphasis added).

[27] Sec. 332(d)(1).

[28] Sec. 332(d)(2).

among others, Canada plans soon to fly its drones, too.[29]

The FAA's Progress to Date

Since FMRA's passage, three of its most important dates have passed. The first is **May 14, 2012**, regarding procedures to approve certain UAS flown by law enforcement and other safety agencies. The second, **August 12, 2012**, concerns UAS that the Secretary of Transportation deems safe to fly, pending completion of the FMRA procedure; and programs for experimental UAS flights in the United States and the Arctic. **November 10** is the third. By that date the FAA had to streamline the COA process for government operated UAS, and develop a "Comprehensive Plan" for the widespread deployment of their privately operated counterparts.

On the first, the objective was for the agency to "enter into" agreements with government agencies, so as to permit the latter quickly to fly its smaller-sized UAS.[30] In a report issued this September, the Government Accountability Office ("GAO") found that the FAA had reached a Memorandum of Understanding with the Department of Justice.[31] But the deal was then in draft form; it still had to be finalized and undergo internal legal reviews. Perhaps for that reason, the GAO scored the first responder project as "in process," rather than "completed."[32] The FAA seemed to disagree, though it didn't go so far as to claim that the FAA had executed a legally operative deal with its counterparty: instead, according to the FAA's website, an agreement was "established" on May 14, 2012. "[W]hen [a safety agency] has shown proficiency in flying its UAS," explained the agency, "it will receive an operational COA" – one that will generally authorize the drone's use and not require a first responder to win approval for each drone flight.[33] Curiously, the first responders' agreement "expands the allowable UAS weight up to 25 pounds"[34] – notwithstanding FMRA, which permits public safety agencies to operate a UAS "weighing 4.4 pounds *or less*[.]"[35] That legally dubious maneuver aside, it seems some agreement has existed since the first FMRA deadline of May 14.

Compliance with the second deadline, August 12, is just as difficult to appraise – though again, work is clearly underway. As above, the GAO's

---

[29] Carola Hoyos, "Canada Looks to Patrol Arctic with Drone," FINANCIAL TIMES (May 30, 2012).

[30] Sec. 334(c)(1).

[31] Government Accountability Office, "Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System" at 24-27 (Sept. 18 2012).

[32] *Id.* at 24.

[33] "FAA Makes Progress with UAS Integration," *available at* http://www.faa.gov/news/updates/?newsId=68004.

[34] *Id.*

[35] Sec. 334(c)(2)(C) (emphasis added).

September report found that the FMRA preclearance and Arctic activities both were "in process" – and thus, as logical matter, not yet accomplished.[36] This may have as much to do with FMRA's loose language as the facts on the ground. With respect to the Arctic, for example, the agency's chief obligation is to "*develop* a *plan* and *initiate* a *process* to *work*" with relevant domestic and international players.[37] In any event, the agency indeed has detailed plans, among other things, to establish two permanent flight areas in the Northern and Southern Arctic, and to designate transit corridors from coastal launch sites.[38] Still, the FAA hasn't drawn attention to its work in this area: the FAA's website, for example, says very little about Arctic activities, or the Secretary's obligation to identify any UAS – private or public – that may operate safely, before the FAA issues further guidance or rules. Regarding the latter, it seems the Secretary has taken no action, and thus *de facto* elected to preserve the existing case-by-case regime for UAS approvals.

By contrast, the FAA hasn't been at all shy about the requirement to "establish . . . a program to integrate unmanned aircraft systems into the national airspace system at 6 test ranges."[39] When August 12 arrived, the FAA had not yet named its six proving grounds. A UAS advocacy group wrote to the FAA, seeking an explanation and pressing for a brisk conclusion to the designation process.[40] In a letter response, the FAA insisted that it had not missed any statutory milestones. Acting Administrator Michael Huerta wrote that, consistent with FMRA's language, the UAS test site program in fact had been "*established* on March 9, well in advance of the August 12, 2012, deadline[;]" the FAA also had sought and received comments from interested members of the public.[41] As a nitpicky, textual matter, the agency thus had not flouted FMRA – at least in Huerta's view. (The GAO and Congressional Research Service both disagreed, and concluded the FAA had missed a deadline.[42])

Despite hewing closely to FMRA's express language, Huerta also looked past it in one important respect. His letter also cited privacy, an issue of obvious importance but nowhere mentioned in FMRA itself. Explaining why no sites yet

[36] "Measuring Progress and Addressing Potential Privacy Concerns" at 24.

[37] Sec. 332(d)(1).

[38] Presentation by James H. Williams, FAA UAS Integration Office, "Expanding Use of Unmanned Systems in the Arctic" at 7-9 (July 17, 2002).

[39] Sec. 332(c)(1).

[40] Letter from Michael Toscano, President and CEO, Association for Unmanned Vehicle Systems International, to the Hon. Ray LaHood, Secretary of Transportation (Aug. 20, 2012).

[41] Letter from Michael P. Huerta, Acting Administrator, Federal Aviation Administration, to Michael Toscano, President and CEO, Association for Unmanned Vehicle Systems International at 1 (Sept. 21, 2012).

[42] Bart Elias, "Pilotless Drones: Background and Considerations for Congress Regarding Unmanned Aircraft Operations in the National Airspace System" at 7 (Sept. 10, 2012) (asserting that the FAA was "mandated to identify [test sites] by the summer of 2012."); "Measuring Progress and Addressing Potential Privacy Concerns" at 27 ("FAA has taken steps to develop, *but has not yet established*, a program to integrate UAS at six test ranges, as required by the 2012 Act.").

had been selected, the FAA chief said "privacy concerns have surfaced as a result of increased UAS usage, and this necessitates an extensive review of the privacy impacts of the test site program."[43] Huerta reiterated his privacy-centric view in a November letter Congress – which did not concede the timing question, but recognized that the FAA would not meet its internal goal of naming test sites by "the end of 2012."[44]

The FAA has permitted UAS operations – albeit on a limited and *ad hoc* basis – since as early as 2003. Thus FMRA is mostly an effort to accelerate and expand a policy that has existed, if only in rough form, for nearly a decade.

Finally, the FAA already has expedited the COA review process for public UAS, as it had to do on or before **November 10, 2012.** In particular, the agency says it established internal metrics for tracking COA applications, and "developed an automated, web-based process [to ensure that an application] is complete and ready for review."[45] COA durations have also been extended, from 12 to 24 months.[46] Count this, in other words, as apparent compliance with a FMRA deadline.[47]

The same November 10 date governed the development of a "Comprehensive Plan" for integrating civil UAS into the national airspace system – though again, the statute doesn't explain what the FAA must do, exactly, in order to "develop" it.[48] According to the FAA, the Comprehensive Plan ultimately will consist, roughly, of two parts: one, the FAA's "roadmap" for civil and public UAS integration; and two, a Concept of Operations paper, or "ConOps."[49] The FAA has yet to release its draft road map, though the document is believed to exist.[50] Regarding the latter, the Joint Production and Development Office ("JPDO") – an interagency, FAA-led bureaucracy concerned with, among other things, UAS integration – approved a version of the ConOps in September. This 112-page technical document evidently was not intended for publication, but leaked to the press the following month.[51] The ConOps identifies many

[43] Letter from Michael P. Huerta, Acting Administrator, Federal Aviation Administration, to Michael Toscano, President and CEO, Association for Unmanned Vehicle Systems International at 1 (Sept. 21, 2012).

[44] Letter from Michael P. Huerta, Acting Administrator, Federal Aviation Administration, to Rep. Buck McKeon, at 2 (Nov. 1, 2012).

[45] "FAA Makes Progress with UAS Integration," *available at* http://www.faa.gov/news/updates/?newsId=68004&omniRss=news_updatesAoc&cid=101_N_U

[46] *Id.*

[47] *See* "Measuring Progress and Addressing Potential Privacy Concerns" at 24 (describing the COA expediting process as "completed").

[48] Sec. 332(a)(1).

[49] Presentation by Richard Prosek, UAS Integration Office, "UAS and the FAA Modernization and Reform Act of 2012," at 9 (Aug. 9, 2012)

[50] Separately, the FAA has published a "Civil/Public UAS Road Map," a detailed if short – one page - chart illustrating the agency's UAS activities through 2020. *See* FAA Civil/Public UAS Roadmap, *available at* http://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0CDAQFjAA&url=http%3A%2F%2Fwww.faa.gov%2Fabout%2Finitiatives%2Fuas%2Fmedia%2FFAA_Civil_Roadmap.ppt&ei=tyWcUK-JDMeJ0QGK0IDoCA&usg=AFQjCNGQ5htmcEdPgapduP2bCsSEPLHW5A&sig2=ujb18i2lxXJy3Y1ODZ-s5w&cad=rja.

[51] *See generally* "Integration of Unmanned Aircraft Systems into the National Airspace System, Concept of Operations v. 2.0" (Sept. 28, 2012), *available at* http://www.suasnews.com/wp-content/uploads/2012/10/FAA-UAS-Conops-Version-2-0-1.pdf

current challenges to UAS integration, including "the use of instruments to replace the vision of a pilot, as vision is fundamental to the conduct of flight operations;" UAS interactions with air traffic management constitute another obstacle.[52]

It therefore remains for the agency to mash these two components together, and, more dauntingly, to settle on a single set of marching orders for privately-operated drones – which it will hand over to Congress in February of next year.[53]

The Background to Domestic Drone Integration

In carrying its FMRA-mandated assignments, the FAA won't have to paint on a blank canvass: in fact, domestic unmanned flight had been on its radar screen for a good time before the statute's enactment. The FAA has permitted UAS operations – albeit on a limited and *ad hoc* basis – since as early as 2003. Thus FMRA is mostly an effort to accelerate and expand a policy that has existed, if only in rough form, for nearly a decade.[54] (The lone exception here, again, has to do with civil UAS: FMRA contemplates the widespread commercial operation of drones – something the law currently forbids.) To put the point another way: with FMRA, Congress expressed its dissatisfaction with the gradual development of domestic UAS norms. These days, the name of the game is speeding things up.

Officially, the FAA first glanced towards domestic unmanned flight back in 1981, by issuing voluntary standards for hobbyists' use of remote-controlled model aircraft. This terse, one-page document recommended a maximum altitude of four hundred feet and encouraged amateur pilots to fly their aircraft at a reasonably safe distance from populated areas.[55] At the time, no other policies or laws touched on domestic UAS flight, in no small part because, apart from enthusiasts' remote-controlled planes – and experimental projects conducted by the military – unmanned aircraft did not make consistent use of

---

[52] *Id.* at 9, 10.

[53] Sec. 332(a)(4). A bit further down the road is next summer's deadline for the civil operation of small UAS. A final rule must be issued for these aircraft sometime before August 14, 2013. The date is a sore subject within the UAS community, given the government's sluggishness in crafting small UAS procedures. The FAA's Small UAS Rulemaking Committee was established in 2008, and issued the first of many formal policy recommendations in 2009. *See generally* "Comprehensive Set of Recommendations for sUAS Regulatory Development," Small Unmanned Aircraft System Aviation Rulemaking Committee (April 1, 2009). For its part, in July of 2009, the FAA publicly proclaimed its intention to commence with rulemaking sometime in the near term. Report on Significant DOT Rulemaking, "Operation and Certification of Small Unmanned Aircraft Systems (sUAS)" at #6 (Oct. 10, 2012). That has not happened. In fact, the agency repeatedly has postponed the process, on account of "unanticipated issues requiring further analysis," and internal reviews by the Secretary of Transportation and the White House. *Id.* The slowdown prompted one UAS website, "sUAS news," to display on its front page a "FAA Miss-o-Matic" – a running clock that notes the months, days, years and hours since the FAA first began its work on small UAS matters. *See* http://www.suasnews.com/

[54] Of course, drones – private and public, civilian and military – have existed in some form or another for much longer. *See, e.g.*, "Pilotless Drones" at 1 ("During World War I, the Navy funded research to develop a prototype flying bomb called the Hewitt-Sperry Automatic Airplane.").

[55] Air Traffic Service Advisory Circular No. 91-57, "Model Aircraft Operating Standards" (June 9, 1981).

the skies. Nevertheless, by issuing *some* standards, the FAA raised the question of whether, and how, unmanned machines eventually might do just that. The answer has a lot to do with technology. The next twenty years would witness a spike in UAS research, design, and manufacturing, even as UAS remained mostly a military concern.[56] But the more the military harvested the technology, the more evident its civilian applications became. That, in turn, created pressure to relax some of the restrictions on domestic UAS flight.

The progression evidently was on Congress's mind in 2003, when it passed the Vision 100 —The Century of Aviation Reauthorization Act. In broad strokes, this statute sketched out an ambitious transformation of the aerospace industry and of the regulation of domestic air traffic. Essential to this was the creation of the Next Generation Air Transportation System or "NextGen" – a modernized, satellite-based aviation management scheme that, Congress hoped, would address the exponentially increasing volume of aviation in the United States.[57] As legislators imagined things, NextGen essentially would "accommodate a wide range of aircraft operations, including airlines, air taxis, helicopters, general aviation, and *unmanned aerial vehicles*."[58] A special entity within the FAA, the Joint Planning and Development Office, was established in order to realize that objective, along with the others Congress had set forth in Vision 100.[59] Of course none of this meant changing federal law immediately, so as to permit domestic UAS flights. Still, by including unmanned aircraft in its long-term revamping of the aviation sector, the legislature made explicit what the FAA had implied so many years earlier, when it issued its model aircraft standards. In the not-too-distant future, more and more aircraft would not have a human pilot inside.

The gap between that future and the present had narrowed by 2003, as more public and private entities sought authorization to utilize their UAS. The uptick underscored a growing problem within existing law: were UAS "aircraft," and thus subject to regulation by the FAA? Under federal law, "aircraft" means any "device that is used or intended to be used for flight in the air."[60] Drones handily met this sweeping definition, and thus appeared to come within the coverage of laws that – until recently – had applied only to aircraft flown by in-cockpit pilots. But some of these rules, or "Federal Aviation Regulations," do not obviously implicate drones. Consider: the windshields and windows on an "aircraft" must meet certain placement and durability criteria.[61] These and similar aviation regulations obviously don't come into play when an airplane has neither pilots

---

[56] "Pilotless Drones" at 1-3 (describing military development of drone technology, and burgeoning hobbyist and commercial drone activities).

[57] *See generally* "Fact Sheet – NextGen" *available at* http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=8145.

[58] Pub. L. 108-176, Sec. 709(c)(6) (Dec. 12, 2003) (emphasis added).

[59] *Id.* at Sec. 709(a)(1).

[60] 14 C.F.R. § 1.1.

[61] *Id.* § 23.775.

nor passengers – and thus neither windshields nor windows.

Other regulations do come into play, though, and can frustrate unmanned flight. This category includes some of the FAA's bedrock safety principles, like the requirement that "vigilance shall be maintained by each person operating an aircraft so as to see and avoid other aircraft."[62] Not even the most lens-laden drone can "see" neighboring air traffic like an ordinary pilot can. Sure, a ground-based operator or observer might be able to see passing planes with his or her naked eye – but only if the UAS does not stray beyond the line of sight, the skies are clear and sufficient daylight remains. For these reasons, in 2005, the FAA publicly concluded that UAS could not meet the "see and avoid" standard – and thus also could not fly in strict accordance with federal law.[63] *See* and avoid being out of the question, the UAS community has focused instead on developing a means for UAS to "*sense* and avoid" potential collisions.[64]

The COA and SAC procedures differ: in theory, for example, a COA may issue for any public purpose; by contrast, an SAC authorizes private drone flights only for research and development, market survey and crew training objectives.

Of course, simply because a drone cannot satisfy every jot and tittle of federal aviation law does not mean it can never be operated safely. The FAA long has recognized this, by authorizing domestic UAS operations on a case-by-case basis. The agency's approach has been to consider individual requests to exempt UAS from otherwise prohibitive aviation rules. There are two exemption regimes. Which one applies depends upon the intended use of a particular UAS. For a "public" use – say, a survey of a controlled fire's progress through a national park – the applicant must obtain a Certificate of Waiver or Authorization ("COA") from the FAA before it may operate the UAS. Conversely, if the UAS operation is private in nature – or "civil," to use the aviation jargon – then another body of regulations is triggered. Private concerns wishing to fly a UAS must apply for a "Special Airworthiness Certificate" in the "experimental" category ("SAC").

The COA and SAC procedures differ. In theory, for example, a COA may issue for any public purpose. By contrast, an SAC authorizes private drone flights only for research and development, market survey and crew training objectives. (Again, Civil UAS cannot fly on a for-hire basis.) And because governments drive most of today's drones, the COA process naturally has done the bulk of the exemption work. Early this year, the FAA claimed that, since 2006, it had approved between 700 and 750 COAs[65], as opposed to only 94 SACs

[62] *Id.* § 91.113.

[63] Memorandum, "Unmanned Aircraft Systems Operations in the U.S. National Airspace System – Interim Approval Guidance" at 2 (Sept. 16, 2005) ("While considerable work is ongoing to develop a certifiable "detect, sense and avoid" system, an acceptable solution to the "see and avoid" problem for [UAS] is many years away. If [UAS] operators were held rigorously to the "see and avoid" requirements . . . *there would be no [UAS] flights in civil airspace.*") (emphasis added).

[64] *See, e.g.*, Andrew Lacher, Andrew Zeitlin, David Maroney, Kelly Markin, Duane Ludwig, and Joe Boyd, "Airspace Integration Alternatives for Unmanned Aircraft" at 2 (Feb. 1, 2010) ("The community has coined the term "*sense and avoid*," to describe a technical capability that could be developed to mitigate the lack of a *see and avoid* capability") (emphasis in original).

[65] *See* Jennifer Lynch, "FAA Releases List of Drone Certificates – Many Questions Left Unanswered," Electronic Frontier Foundation (April 19, 2012), *available at https://www.eff.org/deeplinks/2012/04/faa-releases-its-list-drone-certificates-*

– though the FAA last tallied SAC numbers in July of 2011.[66] Still, regardless of whether the applicant seeks a COA or an SAC, the point of the exercise is the same. Either way, the FAA examines the proposed UAS project, and asks if, despite the failure to meet this or that safety standard, the applicant nevertheless can mitigate the risks of non-compliance. If the answer is "yes," then a COA or SAC will issue – and the UAS can fly, subject to the conditions imposed by the FAA in granting the exemption. The agency might, for example, insist on flight within the operator's visual line of sight, or with a manned aircraft tailing along.

Such has been the FAA's method since at least 2003, when it permitted the Department of Defense to operate, on a nation-wide basis, Northrop Grumman's Global Hawk Aerial Reconnaissance System. The criteria underlying that authorization were spelled out two years later, in what appeared to be the first official FAA policy regarding the temporary licensure of domestic drones.[67] Among other things, the agency said it would require UAS pilots to understand the aviation rules relevant to the airspace where their robots planned to fly; the UAS also would have to possess a "lost-link" capability, so as to permit the aircraft's safe recovery in the event of a break in communications between operator and aircraft.[68] Such guidance accompanied an increase in drone approvals. In 2005, for example, the FAA blessed a bid by General Atomics to fly, on an experimental basis, its Altair UAS.

Next, in 2006, the agency established its Unmanned Aircraft Program Office. This quickly became "the focal point for all [aviation safety-related] UAS activity, including any proposed certification projects"[69] – which continued to grow, as the FAA issued a formal policy on "Unmanned Aircraft Operations in the National Airspace System," in February of 2007.[70] The latter echoed guidance that the agency had put forth earlier, and underscored that "no person may operate a UAS in the National Airspace System without specific authority" – a COA or an SAC, or the voluntary model aircraft standards established more than

---

leaves-many-questions-unanswered ("In a meeting with the FAA today, the agency confirmed that there were about 300 active COAs and that the agency has issued about 700-750 authorizations since the program began in 2006"). The Electronic Frontier Foundation sought historical COA data by means of the Freedom of Information Act ("FOIA"). *See* Jennifer Lynch, "FAA Releases Thousands of Pages of Drone Records," Electronic Frontier Foundation (July 13, 2012), *available at https://www.eff.org/deeplinks/2012/07/faa-releases-thousands-pages-drone-records*. In response to EFF's requests, the FAA released four tranches of historical COA information – including application materials by law enforcement agencies, as well as the COAs themselves. *See* "Unmanned Aircraft Systems," *available at http://www.faa.gov/about/initiatives/uas/* (setting forth COA files for downloading and review).

[66] *See* "Fact Sheet: Unmanned Aircraft Systems (UAS)" *available at http://www.faa.gov/about/initiatives/uas/media/uas_fact_sheet.pdf* ("Since July 2005, the FAA has issued 94 SAC-EC, to 13 civil operators covering 20 unique UAS and OPA types. The FAA works with these operators to collect technical and operational data to improve the UAS airworthiness certification process.").

[67] Memorandum, "Unmanned Aircraft Systems Operations in the U.S. National Airspace System – Interim Operational Approval Guidance" (Sept. 16, 2005).

[68] *Id.* at 6, 7.

[69] Memorandum, "Unmanned Aircraft Systems (UAS) Certification Status" at 1 (Nov. 16, 2006).

[70] Docket No. FAA-2006-25714, "Unmanned Aircraft Operations in the National Airspace System" (Feb. 6, 2007).

twenty years earlier.[71] At roughly the same time, the U.S. House of Representatives passed legislation that, among other things, would have required the FAA to develop a comprehensive program for domestic drone activities in the United States, and directed the FAA to determine which drones, if any, were safe enough for operation outside the COA framework.[72] The proposal, which anticipated FMRA, did not pass the Senate.

Development of more and more UAS "resulted in an increased demand for the FAA to process a large number of applications to review for operational approvals."[73] That prompted the FAA, in 2008, both to issue additional interim guidance on the limited, domestic use of UAVs,[74] and to create a special committee to study issues unique to small UAS – the category of unmanned craft which was, in the agency's view, likely to "experience the largest near-term growth."[75] In 2011, Congress passed the National Defense Authorization Act for 2012. In it, the legislature ordered the Secretary of Defense, in consultation with Administrator of the FAA, to report back on the rate of "progress" in integrating UAS into the national airspace system; and on "the potential for one or more pilot program or programs on such integration at certain test ranges to increase that rate of progress."[76]

In this iterative fashion, the FAA has created a rough process for deciding which UAS can fly and which UAS cannot. The process still is not standardized, but a process it is nonetheless, one articulated through policies, orders, and guidance that the agency has handed down since 1981. Congress thus did not have to create domestic drone integration out of whole cloth. By the time of the FMRA, integration had been ongoing for some time already, albeit in a slow and unstructured fashion. What remained was to broaden and accelerate the United States' nascent approach to domestic drones.

Overview of Select Domestic UAS Policy Issues

FMRA speeds the transition by setting forth the fast-paced calendar described in Section One. But the statute announces few wholesale policy changes – save only a significant, future alteration to the civil UAS regime. Thus the bulk of the substantive work is left to the FAA and other UAS stakeholder agencies. The issues before them are as easy to identify as they are difficult to resolve. Among these, perhaps the most significant are air safety, security,

---

[71] *Id.* at 5.

[72] *See generally* H.R. 2881, 110th Cong. §§ 321-24 (2007).

[73] Unmanned Program Office, "Unmanned Aircraft Systems Operations in the U.S. National Airspace System" at 2 (Mar. 13, 2008).

[74] Unmanned Program Office, "Unmanned Aircraft Systems Operations in the U.S. National Airspace System" (Mar. 13, 2008).

[75] Order 1110.150, "Small Unmanned Aircraft Systems Rulemaking Committee" at 1 (April 10, 2008).

[76] Pub. L. 112-81, Sec. 1074(a)(1)-(2) (Dec. 31, 2011).

cybersecurity, and privacy.[77]

Two qualifications: first, resolving these issues will be as much a bureaucratic project as a normative one. Different arms of the government claim jurisdiction over different areas, and agencies' bailiwicks often overlap. For example, the Transportation Security Administration, a unit of the Department of Homeland Security, takes the lead in guaranteeing aviation security; under FMRA the FAA, a unit of the Department of Transportation, is charged with ensuring the safe integration of UAS into our national airspace system.[78] Obviously security matters must be addressed, if integration truly is to be accomplished by 2015. Doing so thus will depend not merely on setting an optimal policy, but also on close cooperation between interested components of the executive branch. Thus the JPDO, which brings UAS stakeholder agencies together under a single bureaucratic roof.

The idea is gradually to move away from plane transponders and radar, and instead to require "satellite navigation and control of aircraft, advanced digital communications, and enhanced connectivity between all components of the national air transportation system."

Secondly, a lot of UAS integration issues are not new. The executive branch has grappled with cyber matters involving airplanes, for example, since 9/11; even more so with the NextGen transition and the gradual increase in *ad hoc* UAS approvals. The same holds true for aviation safety: even at the time of the very first FAA-approved drone flight, it was clear that the government might have to figure out how, if at all, more such machines could fly safely. What *is* new is the shift announced by FMRA, from case-by-case licensure to stable rules allowing for widespread UAS operation; and the resulting increase in domestic drone numbers. There's obviously little time remaining between now and 2015. Thus the long-brewing policy questions will have to be answered more comprehensively, and soon – rather than piecemeal, and gradually.

An overview of those questions follows.

Air Safety

As it pushes forward with domestic drone integration, the FAA's primary concern is air safety – including the ability of UAS to sense and avoid other aircraft, and vice versa. Earlier this year, the GAO concluded that small UAS lacked adequate sense and avoid capabilities, and therefore could not make consistent use of the national airspace system.[79] The reason? Such drones, GAO

[77] There's also this vexing procedural problem: whatever standards the FAA may settle on, precisely how will it impose them? Again, federal aviation regulations apply to "aircraft," but right now do not distinguish between manned and unmanned. Thus the FAA has either to create a new and freestanding body of UAS-specific regulations, or to scrub and rework existing regulations so as to account for both manned and unmanned flight. *See* Joseph J. Vacek, "Civilizing the Aeronautical Wild West," 23 AIR & SPACE L. 18, 21-22 (2011) (arguing that an "incremental approach to UAS regulation involving amendments of parts 23, 43 and 91 of the [Federal Aviation Regulations] would only serve to increase regulatory complexity and inefficiency"); *see also* Presentation by Douglas Marshall & Ernest Anderson, *Analysis of 14 CFR Parts 91 & 43 for UAS Applications*, (June 2008) (cataloging existing federal regulations which clearly apply to UAS operations already, may apply to such operations by interpretation, could only apply through further revision, or do not apply at all).

[78] Aviation and Transportation Security Act ("ATSA"), Pub. L. 107-71; *see also* "Pilotless Drones" at 14 ("Under [ATSA], responsibility for aviation security was transferred from FAA to the newly formed Transportation Security Administration (TSA) in 2001. TSA has not specifically addressed the security concerns arising from the operation of drones in domestic airspace.").

[79] Statement of Gerald L. Dillingham, Director, Physical Infrastructure Issues, before the House Committee on Homeland Security, Subcommittee on Oversight, Investigations and Management at 5-6 (July 19, 2012).

noted, likely will use the same airspace as smaller manned craft, which often "do not transmit an electronic signal to identify themselves and, even if they did, many small UAS do not have equipment to detect such signals if they are used and may be too small to carry such equipment."[80] This, among other things, is why some in the UAS community expect the long-awaited small UAS rule to take a restrictive approach – perhaps by limiting such craft to daytime flights, within the visual line of sight of a ground observer or a manned chase aircraft.

Sense and avoid is just as tricky for larger UAS. FMRA acknowledges as much, by ordering that UAS integration take place in parallel with the nation's ongoing transition to NextGen.[81] Again, that is shorthand for the "Next Generation Air Transportation System," Congress's sweeping overhaul of all civil aviation. The idea is gradually to move away from plane transponders and radar, and instead to require "satellite navigation and control of aircraft, advanced digital communications, and enhanced connectivity between all components of the national air transportation system."[82] NextGen's centerpiece is ADS-B, or "Automated Dependent Surveillance-Broadcast," a technology that permits aircraft and air traffic control constantly to transmit and receive detailed data from GPS satellites. With this, we can expect a smarter allocation of airspace among aircraft; and, more importantly, better collision avoidance.[83] Another possibility for mitigating collision risk is the Army's "ground based sense and avoid" system for UAS, which it successfully tested this year.[84] Whatever the technical solution, the FAA has tasked a federal advisory committee, the Radio Technical Commission for Aeronautics ("RTCA"), with developing minimum sense and avoid standards. RCTA reportedly will issue these in December 2013.[85]

Does the safety game turn entirely on sense and avoid rules? Not by a long shot. Among many other things, the FAA also must standardize its approach to "lost-link" scenarios, in which UAS lose communications with their operators. (The set of possible solutions, though small, still presents some tough choices: a UAS can hover until communications are reestablished, return to its takeoff location or another spot, or even attempt a controlled crash.) There's also the matter of qualifications: must a drone operator be pilot-rated, as the Air Force

---

[80] *Id.* at 6.

[81] *See*, *e.g.*, Sec. 332(a)(2)(I) (requiring incorporation of the Comprehensive Plan "into the annual NextGen Implementation Plan Document (or any successor document) of the Federal Aviation Administration"); Sec. 332(c)(2)(E) (program for UAS flights at six specially-selected test ranges must be "coordinated with the Next Generation Air Transportation System[.]").

[82] "NextGen Overview," *available at* http://www.jpdo.gov/About_Us.asp

[83] "Pilotless Drones" at 8 ("Using ADS-B, aircraft will broadcast precise global positioning system (GPS) location information to air traffic controllers and other air traffic, potentially including unmanned aircraft.")

[84] C. Todd Lopez, "Army Radar to Allow UAS to Fly in National Air Space" (July 2, 2012).

[85] "Pilotless Drones" at 9.

currently requires? Or consider the role of the air traffic controller. In an emergency, will a controller talk only to drone operators on the ground, or also instruct a drone, directly, to climb or dive as needed? The FAA will have to answer all of these questions and more – or at least start to – before civil UAS can fly, on a consistent basis, in our national airspace.

Physical Security

A corollary to aviation safety is physical security – ensuring that bad actors (corporate spies, drug smugglers, or terrorists) cannot exploit UAS technology for illegal or otherwise improper purposes. The issue came into focus earlier this year, when Rezwan Ferdaus pleaded guilty to a terrorist conspiracy that included, among other things, an attempt to fly a bomb-laden drone into the Pentagon.[86] The smallest UAS out there are sold with no security protocols whatsoever – though to be sure, many other potentially misused technologies also change hands freely. Still, under the right conditions, a malefactor might prefer UAS to some other alternatives: for example, like a balloon or helicopter, a UAS can be operated remotely, but with more agility and less visibility. The question is whether, and why, the executive branch would want to regulate the UAS market more tightly than the market for comparable technologies.

And even if a bad guy can't easily buy his own drone, then he could try to overpower somebody else's. Congress and the executive branch have addressed this phenomenon before, if in somewhat different contexts. Take the federal air marshal program, a longstanding initiative that swelled in importance after 9/11. These specially-trained undercover officers ride along on commercial planes within the United States, in order to deter, detect, and, if necessary, to counter in-flight attacks. There's a similar if lesser risk for UAS operations, too, only not onboard the UAS itself. UAS operators and observers must be able to carry out their business without fear of hijacking, no less than the in-cockpit pilots must be able to carry out theirs.

Cybersecurity

As much as UAS physical security, the executive branch has also to reckon with the exceedingly serious issue of cybersecurity. (By nature, UAS rely on networked computers, which present heightened cyber vulnerabilities.) A terrorist would love nothing more than to commandeer a large drone's control mechanisms, and quickly transform it into a flying missile. Remote hijacking is but one nightmarish scenario. By severing or jamming the linkages between UAS and ground-based personnel, cyberattackers also can increase the chances of a crash with other aircraft, or with people or objects on the ground. Of course, an attack need not cause damage in order to be successful: it may be enough, for example, temporarily to prevent an overflying UAS from transmitting video to disaster relief personnel, during the aftermath of a hurricane.

[86] Jess Bidgood, "Massachusetts Man Gets 17 Years in Terrorist Plot," N.Y. TIMES (Nov. 2, 2012).

Just how much use will UAS make of that and other airspace – for surveillance, among myriad other purposes? The FAA reportedly believes that as many as 30,000 unmanned craft could take to our skies by 2020.

What makes that possible? Unlike their manned counterparts, private drones have no dedicated radiofrequency spectrum on which to relay command information. (Obtaining one will be absolutely critical – but could involve separate international and domestic regulatory process.[87]) And GPS systems, which some drones employ, likewise are "open access" – freely available to any and all – and thus relatively easy to jam, intrude upon, and otherwise disrupt. Professor Todd Humphreys and his students at the University of Texas demonstrated this. This February, and at the request of the Department of Homeland Security, Humphreys' group managed to commandeer a civil UAS – a Hornet Mini, manufactured by Adaptive Flight for use by, among others, law enforcement personnel – by means of a GPS spoofing attack. With specially-designed technology, Humphreys and company fooled the Hornet into accepting their false navigation instructions. "By inducing a false upward drift in the UAV's perceived location," Humphrey later testified to Congress, "the spoofer fooled the UAV's flight controller into commanding a dive."[88] The professor acknowledged the attack's complexity, and thus also, the low likelihood of its replication by laymen. But, Humphreys cautioned, "emerging tools of software-defined radio and availability of GPS signal simulators are putting spoofers within the reach of ordinary malefactors."[89]

The NextGen transition, and the widening role of ADS-B and related technologies, only compound the problem's urgency. For all of its benefits, ADS-B is both unencrypted (its transmissions are open) and unauthenticated (its transmissions contain no unique marker, with which recipients can be assured of the originator's identity). Thus, by injecting false data into ADS-B, a cyberattacker theoretically could cause air traffic controllers or pilots – of manned or unmanned aircraft – to detect other airplanes that aren't really there.[90]

Anti-spoofing measures exist already. For its part, the FAA insists that NextGen is secure, and that classified technologies can detect and fend off hacker assaults like that described above.[91] The Department of Defense's UAS likewise employ a Selective Availability Anti-Spoofing Module ("SAASM"), in order to fend off intrusions during military operations; the technology is effective, and could easily transfer to the private market, according to congressional testimony

[87] "Pilotless Drones" at 13 (observing that "the appropriate forum for [radiofrequency spectrum] determinations is [the] International Telecommunication Union (ITU), the United Nations agency responsible for global information and communications technologies;" that frequency must be allocated by national authorities; and that the "FCC has addressed radiofrequency licensing for UAVs on a case-by-case basis, much as FAA has done for certifying drone flight operations.").

[88] Statement of Todd Humphreys, before the House Committee on Homeland Security, Subcommittee on Oversight, Investigations, and Management at 4 (July 18, 2012).

[89] *Id.* at 1.

[90] Kim Zetter, "Air Traffic Controllers Pick the Wrong Week to Quit Using Radar," *Wired* (July 26, 2012).

[91] *Id.; see also* Brad "RenderMan" Haines, "Hackers + Airplanes: No Good Can Come of This," Presentation to Defcon20 Hacker Conference (July 21, 2012).

by a UAS advocacy group.[92] Finally, some UAS carry redundant navigation equipment, which can take over in the event of an attack on GPS systems.[93]

Privacy

UAS pose serious privacy challenges. The reasons are straightforward. When mounted on a remotely-piloted craft, today's sensors can scoop up quite a lot of information, at times more easily or more broadly than can helicopters, airplanes, or ground-mounted surveillance equipment. There's also the relevant but outdated case law: the Supreme Court has suggested that warrantless surveillance, if conducted from FAA-defined "public navigable airspace," will not trigger a violation of the Fourth Amendment.[94] Just how much use will UAS make of that and other airspace – for surveillance, among myriad other purposes? The FAA reportedly believes that as many as 30,000 unmanned craft could take to our skies by 2020. Having all of this in mind, the groundswell of privacy concerns seems pretty well justified.

The question is how privacy fits with the FAA's integration effort. Some legislators want to ensure the agency's engagement with privacy issues, by adding them to FMRA's task list. Rep. Edward Markey (D-MA) would amend FMRA, by (among other things) directing the Secretary of Transportation to identify privacy threats posed by domestic UAS endeavors, and by precluding the FAA from licensing domestic UAS unless and until the operator has explained, in detail, how he or she will mitigate possible harms to third-party privacy interests.[95] Other proposals focus on the FAA's independent authority. Just days after the FMRA's signing, advocacy organizations wrote to the FAA's Acting Director, Michael Huerta, and urged his agency to "conduct a rulemaking to address the threat to privacy and civil liberties that will result from the deployment of aerial drones within the United States."[96] The FAA balked at that request, but similar ones followed. Others have urged the FAA to account for privacy matters, as the agency works through the FMRA timetable.

That latter approach seems to have caught on. As discussed in Section Two, the Acting FAA Administrator, Michael Huerta, publicly cited the need to resolve privacy concerns before selecting experimental UAS flight ranges. Why

---

[92] Statement by Michael Toscano, President and CEO, Association for Unmanned Vehicle Systems International, before the House Committee on Homeland Security, Subcommittee on Oversight, Investigations and Management at 4 (July 17, 2012).

[93] *Id.*

[94] *See California v. Ciraolo*, 476 U.S. 207, 215 (1986); *Florida v. Riley*, 488 U.S. 445, 450-51 (1989).

[95] Discussion Draft Bill, "To Amend the FAA Modernization and Reform Act of 2012 to Provide Guidance and Limitations Regarding the Integration of Unmanned Aircraft Systems into United States Airspace" (Aug. 1, 2012). Similarly, Senator Rand Paul would disallow, with some exceptions, the gathering of "evidence or other information pertaining to criminal conduct or conduct in violation . . . except to the extent authorized in a warrant that satisfies the requirements of the Fourth Amendment[.]" S. 3287, "Preserving Freedom from Unwarranted Surveillance Act of 2012" (June 12, 2012).

[96] Letter from American Civil Liberties Union, Electronic Frontier Foundation and other organizations to Michael P. Huerta, Acting Administrator, Federal Aviation Administration at 1 (Feb. 14, 2012).

do so if, as some have suggested, the FAA has no special jurisdiction over the issue? One answer has to do with expediency; the FAA might have thought that, regardless of its FMRA obligations, the agency nevertheless must address a matter of tremendous significance to the public. Another theory is that the FAA indeed views itself as legally bound to resolve privacy issues as they arise – though this does not follow from FMRA's plain text, and also doesn't neatly jibe with some legislative proposals to shunt privacy into the FMRA process. The latter would not be necessary if, indeed, FMRA already obligated the FAA to account for privacy concerns.

Whatever the explanation, one thing is certain. By emphasizing privacy's centrality to the test site selection exercise, the Acting Administrator's response effectively commits the FAA to tackling other privacy problems in the future, as it reaches other statutory milestones. Although its mission is only to ensure safe flight within the national airspace system, the agency now is officially in the privacy game, for better or worse.

Conclusion

Over the next two years and change, FMRA requires the executive branch to address a slate of interconnected UAS policy dilemmas. These involve a pretty familiar tradeoff: a looser regime means more benefits for the public, lower end-user costs, and a boon to an industry eager to realize its growth potential – but also more risk to safety and civil liberties. A tighter one will mean the converse, with the public getting less bang for its technology buck, and the UAS sector growing at a slower clip – but with fewer drones crashing, and fewer citizens complaining about unwanted surveillance or insecure networks.

But here's the (obvious) trouble: familiar does not mean easy. Instead the key questions are awfully hard – even though, as noted above, the FAA and other agencies have wrestled with some of them for a good while now. The difference is FMRA's clock, which crams the core policymaking into a period of just under four years. The time is running out, and the most difficult work is yet to come.

Email your comments to gscomments@brookings.edu

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

Editor
Christine Jacobs
Stephanie C. Dahle

Production & Layout
Mitchell R. Dowd