Center for Technology Innovation at BROOKINGS

September 2014

Civilian Drones, Privacy, and the Federal-State Balance

Wells C. Bennett

INTRODUCTION

Wells C. Bennett is a Fellow in National Security Law at the Brookings Institution and Managing Editor of Lawfare.

Some say the federal government should be principally responsible for regulating drones,[1] nongovernmental actors, and privacy; others have suggested a blended approach, with states taking center stage and the national government cast in a supporting role. This essay takes essentially the latter position. As drones are folded further into American airspace, states should take the initiative, both by applying longstanding liability rules and by devising new ones. But we also should take advantage of the Federal Aviation Administration's (FAA) small but growing competence in nongovernmental drones and privacy—and have the agency perform a kind of superintendence function.

Remotely controlled flying robots are increasingly cheaper, and at times more capable of sustained flight, than some manned counterparts. Many can be outfitted with imaging or other recording equipment, which is increasingly more affordable and widely available. An airborne droid might take in more information over a much longer period of time than a human eye or ear; and it might also find its way to areas where other aerial platforms might not be able to go. In this way, drones pose real if manageable privacy risks. And policymakers have aimed to manage them following Congress's call to broaden drones' access to the skies by late 2015. The timing raises any number of big-ticket privacy questions. Two are recurring: which arm of the government (states or feds) ought to balance a proliferating technology's benefits against its privacy costs; and which drones (government or private) will present the greatest threats to privacy.

On one side of the first question are certain members of Congress and civil liberties advocates, who have called for a robust federal approach to drones and privacy.[2] On the other are "drone federalists": scholars[3] and policymakers[4] who generally oppose

enactment of a preemptive, federal drone statute, and who would in any event keep federal regulation to a minimum or reserve it for discrete subjects only. In recent years, only states have passed legislation meant to account for America's drone experiment and its implications for privacy. In that sense, momentum isn't with the feds: the FAA, for example, pointedly refused to regulate privacy in a broad fashion (though, as explained below, it nevertheless undertook some drone privacy work later). And unlike some state houses, the U.S. Congress hasn't seriously considered or passed a bill to set general privacy standards or to regulate drones and privacy specifically.

Meanwhile, state legislators mostly have their sights set on a particular class of drone—that flown by governments. The past few years have seen a raft of proposed and enacted laws, principally or exclusively aimed at restricting drone surveillance by public officials. Some states, like Florida, Utah, and Montana, generally preclude police from using drones, unless officers obtain a judicial warrant founded on probable cause or confront an emergency.[5] Virginia probably takes the gold medal in this regard, having banned, with some exceptions, *all* public drone operation by state personnel until July 2015.[6] We can guess the reasons behind the government-centric approach: the state's unique power to imprison; the Constitution's traditional protections against public rather than private action; and the fact that, like much in the realm of technica, the drone was initially developed for government applications and only afterwards transitioned to private ones. Drones had been a staple of military activities abroad for years, long before Congress even thought about widespread civilian operations. And, owing to the FAA's current licensing scheme, drone pilots are frequently police or border security officers.[7] It thus makes intuitive sense to prioritize policymaking for public aircraft—which the states largely have done that so far.[8]

But that's just the thing: private aircraft matter, too. These days individuals, private universities and companies can and do fly surveillance-capable aircraft, both with and without the specific blessing that the FAA requires.[9] As unmanned flight technology matures and grows ever cheaper, it will find its way into more private hands. The already swift clip will quicken, once the FAA writes rules for wider domestic drone flight. Suffice it to say private actors will soon operate drones in equal if not greater numbers than the government does—and also acquire the potential to undertake just as much surveillance. As pressing as the question of how best to safeguard "public" privacy, is the question of how best to safeguard its understudied counterpart, "private" privacy. The urgency is reflected in a handful of legislative proposals concerning drone surveillance, and in a decision reportedly forthcoming from the Obama Administration. Though details remain sketchy, the White House is set to order the National Telecommunications and Information Administration ("NTIA") to develop, in consultation with various stakeholders, voluntary privacy guidelines for commercial drone use.[10]

This essay examines the current division of labor between state and federal governments, with respect to civilian drones and privacy. It proceeds in three parts, the first of which recognizes

the most compelling reason, put forward by advocates of a state-based regime, for the states' primacy in shielding "private" privacy rights. There's already a state law fabric meant to safeguard those very rights, one woven of common law doctrines, statutes, and laws meant to account for drone surveillance in particular. This body of law will be increasingly relevant as more private drones fly, and civilian drone surveillance becomes more common. And, as the drone federalists rightly point out, currently there is no firm consensus about how best to safeguard privacy rights from non-governmental drone surveillance—something a top-down, federal approach would require.

Still, as the essay's second section explains, the FAA's involvement in private drones and surveillance, though small, has been quietly increasing since 2012. This rather subtle development informs an argument at the heart of the third segment: the FAA's emerging presence in "private" privacy and unmanned aerial surveillance supports a continued role for the agency in addressing the issue. Doing so would be consistent with recent practice. Moreover, incrementally adjusting the *status quo*, perhaps by having federal aviation officials take away the worst privacy violators' drone flying credentials, would even be a good idea. A fourth section offers concluding thoughts.

THE STATES' PRIMACY

Opponents of a federal statutory scheme for civilian drones and privacy have broadly raised two claims, both of them valid.

First, with some important federal-level exceptions, the law of "private" privacy and aerial surveillance largely is state law.[11] It is mostly tech-neutral, and accordingly has protected privacy from varied forms of surveillance by nongovernmental actors over time. When the drones take to the skies in greater numbers, a body of varied state rules will be waiting for them. And it will do much of the work in addressing civilian drone surveillance—though how well remains to be seen.

State privacy laws generally fit into one of three categories. In the first are longstanding statutory and common-law protections against non-governmental intrusions. Often it is both a crime and a tort to trespass on another's property, for example by walking on it without permission.[12] That is arguably just as true of low-level overflight. Thus an unannounced Quadcopter hover, inside a neighbor's back yard barbecue and at hair-parting altitude, could theoretically put a drone operator on the hook for trespassing. This depends on how a state trespassing statute has been written and how far a court is willing to go in interpreting it.[13] Also in play are the classic state-law "privacy" offenses, which largely "cover what most people think of when they think of personal privacy and social privacy norms."[14] The prohibitions against invading privacy, intruding upon seclusion, publishing private facts, and stalking all might be implicated when a drone, heavily sensored up, hears or sees somebody who doesn't wish to be heard or seen.[15] Again, outcomes will depend on the fit between a case's facts and

criteria set by law. Simply filming a private conversation from a drone probably won't tee up a publication of private facts claim, absent some effort on the snooper's part to disseminate the conversation's contents; a quick fly-by, even when paired with video filming, probably won't rise to the level of an intrusion upon seclusion, either. A more sustained look might be a different story.

More specialized rules make up the second group of state privacy laws. These include state wiretap laws, which preclude the recording of images or conversations without both parties' consent. Also, the somewhat rare "Peeping Tom" and anti-voyeurism laws, which bar peeking into the home under certain circumstances; and equally rare paparazzi statutes, which "ban paparazzi from using special technologies to intrude on the personal life and personal spaces of celebrities."[16] Here too it is easy to imagine how drone surveillance might trigger one or more of the foregoing. An industrious Peeping Tom, for example, might acquire a Parrot Drone, and fly it close enough to an unsuspecting neighbor's bathroom window to snap a photo. It also goes without saying that paparazzi most assuredly will make ample use of surveillance technology—drones included—in their relentless and unending quest to keep up with the Kardashians.[17]

To the foregoing we can add a third and growing category: civil and criminal laws designed specifically to block unwanted aerial surveillance from privately owned, unmanned aircraft. So far, thirteen states have enacted these, either standing alone or coupled with statutes meant to account for surveillance from public aircraft. By way of examples, Tennessee handed down two "private" privacy statutes in 2014. One makes it a misdemeanor to conduct drone-based video surveillance of citizens who are hunting or fishing in accordance with state law.[18] Another precludes, with exceptions, the use of an "unmanned aircraft to capture an image of an individual or privately owned real property … with the intent to conduct surveillance on the individual or property captured in the image," when a snooper retains or publicizes the images. (There's an odd and possibly rule-eating catch: one can escape liability by showing that, upon learning the images were obtained unlawfully, the drone operator promptly destroyed or stopped publicizing them.[19]) Wisconsin's new drone law suggests a narrower scope of geographic application than Tennessee's. Under the former, a private individual commits a misdemeanor by using a drone to "photograph, record, or otherwise observe another individual in a place where the individual has a reasonable expectation of privacy."[20]

Two things stand out about this tripartite array. First, there's a good-sized body of general privacy law out there, waiting to absorb the coming influx of domestic drones and associated surveillance. The second is diversity. Not all states define trespassing or drone surveillance in the same way, or apply identical privacy protections to identical places. Between its statutes and court-crafted doctrines, this jurisdiction might take a relatively stringent approach to the safeguarding of "private" privacy, while that one might take a relatively permissive approach.

The phenomenon is most vividly on display with regard to drone-specific statutes; many states don't have one to begin with, and thus accordingly handle nongovernmental privacy intrusions through a mix of laws in categories one and two. In this way, the law of "private" privacy is something of a hodgepodge. Its coverage can be expansive or porous or even non-existent, depending on where you are, and what sort of technology is deployed.

That registers a second, related point in the drone federalists' favor. We don't quite yet know how effective any one's state law will be, as the domestic drone population grows denser and private surveillance more pervasive; or which states' laws will withstand court challenges. And we won't have a better sense on either score for a while, either. The uncertainty will frustrate consensus about how best to regulate drones, snooping, and nongovernmental actors—and thus bolster states' prerogatives in the short run.[21]

So far as "effectiveness" goes, we really don't have enough in the way of data just yet. Though unmanned aircraft are increasingly visible, they also are not yet an everyday feature of American life in the same way that manned craft very much are. This is not to suggest that domestic drone flight lies far off in some wild future or that it is weird or unprecedented. In fact, odds are pretty good you've seen a YouTube video of footage taken from a Quadcopter, or maybe even fiddled with making such a recording yourself. Or perhaps you've read about a safety incident involving a slightly larger but still small drone, or even operated one pursuant to the FAA's licensing scheme. (So far, the FAA says it has authorized only three commercial drone operations, two over water and another over land.)

Yet the odds are just as good that John Q. Citizen can go weeks, maybe even months, without laying eyes on a drone—or, more to the point, without a drone laying *its* eyes on him. The rough probabilities naturally vary from one place to the next. There *is* plenty of unmanned flight ongoing at test ranges, to name one obvious example; and camera-carrying model aircraft likewise probably are thicker in the air above North Dakota than above Washington, D.C. Still, this fact remains. The American drone era is in its adolescent phase, with the machines' numbers steadily increasing, though still remaining small enough to keep civilian drone-snooping out of most peoples' lives, most of the time.

For corroboration, consider that the courts' dockets have been essentially empty—though not because the privacy-minded aren't on the lookout. True, there have been legal challenges involving unmanned aircraft, snooping, and government: think criminal cases involving the acquisition of video or audio recordings in violation of the Fourth Amendment. The FAA's power to enforce its licensing scheme is also in litigation.[22] As far is the author is aware to date, *plaintiffs have yet to bring any case turning on the relationship between individual privacy rights and civilian drone surveillance*. That makes it hard to draw firm conclusions about whether Texas's drone statute makes better sense than Oregon's, and consequently,

just as hard to make intelligent legislative tweaks. That's not to suggest that policymakers are flying blind. As discussed above, there are many useful precedents hailing from other private surveillance contexts, and from more established but similar technologies: helicopters with cameras, reporters with Dictaphones, everyday people with cell phone cameras, and so forth. With these in hand, states have made some educated guesses about what rules will work best vis-à-vis drones.

But the analogies can only go so far. Two core assumptions inform modern drone policy: drones will allow for more aerial surveillance than other airborne platforms have to date, and more drones will soon find their way into more private hands. If these postulates prove even partially true, then drones are unique. And if so, then the precedents from the manned surveillance world will only get policymakers so far. Said differently, the efficacy and legality of new drone regulations will probably only come into relief once private drone flight and private drone surveillance become somewhat more commonplace.

On the "legality" point, consider this observation by two scholars: When at last the judiciary applies the law of "private" privacy to drone surveillance, many statutory or common law rules could be narrowed, or even invalidated, on First Amendment grounds. Restrictions made in the service of "private" privacy often will implicate the First Amendment.[23] Of course, the push-and-pull between speech and privacy is at its most acute when the press's information-gathering rights are curtailed, regardless of whether the gathering is accomplished through drone surveillance or other means. But First Amendment limits also come into play when governments seek to limit the rights of private individuals to uncover information antecedent to speech. The law here is largely unsettled. So far courts have been less forgiving of regulations that impinge upon the people's ability to witness and record the words or actions of public officials, or events taking place in public or concerning issues of public interest.[24] That trend may or may not remain stable; there's still line drawing to be done, and the final lines will depend upon further litigation.

How much would, for example, Google trample privacy, if it opted to have unmanned aircraft film the ground below, so as to help the company keep its earth maps current? Would existing privacy rules constrain that effort not at all, too much, or just enough? Relative to State X's drone law, does State Y's drone law under- or over-protect "private" privacy, given the incidence of actual drone flights there? Should states emphasize homeowners' rights against overflight, or the public's right to discover information, or its ability to uncover hidden but unlawful surveillance? There are answers in state law, but they remain momentarily tentative.

We might not get to complete clarity. Different kinds of drones will fly in different jurisdictions, and to different degrees; many jurisdictions already view domestic drone proliferation more or less favorably than others. Together, such facts essentially guarantee a measure of policy

diversity nationwide. At present, the policy landscape hasn't begun to approach even that point. We lack general agreement about what an optimal set of liability rules might look like for drones and "private" privacy—something that a largely or even completely federal approach would seem to require and that the drone federalists have stressed.[25] For now, pragmatism counsels against a heavy-handed federal response, and in favor of regulation at the state level.

THE FAA'S GROWING DRONE PRIVACY COMPETENCE

That the national government hasn't coalesced around a single, optimal approach doesn't mean that policymakers can't come to *any* agreement over standards for nongovernmental drone uses; or that federal officials shouldn't assert some prerogatives in the privacy realm. Certainly recent events suggest otherwise. We don't yet know what the White House's order on commercial drones and privacy will look like. We also don't know the voluntary privacy principles that, in carrying out the order, the NTIA ultimately will promulgate. But that plan's very contemplation presupposes at least *some* federal guidance with respect to "private" privacy. The leading proposal for "drone federalism" likewise assumes that the FAA will use its licensing powers to make it easier for privacy plaintiffs to learn of unwanted drone surveillance.[26] All this makes sense given some recent but mostly unnoticed history. Despite the states' longstanding primacy, the federal presence in civilian drones and privacy, though minimal, has been on the rise for some time now.

This began with a tiny shift in the FAA's responsibilities. By dint of the Federal Aviation Administration Modernization and Reform Act of 2012 ("FMRA"), Congress instructed the FAA to lead several other executive branch agencies in a consequential, tight-timeframe project: to devise, by no later than late 2015, rules for the safe and wider use of drones inside the United States.[27] This was to be a technical, logistical endeavor; the statute's drone provisions nowhere mentioned privacy.[28]

That did not stop the agency from dipping a toe into privacy waters, if somewhat tentatively and at times inconsistently. On one hand, the agency scrupulously disclaims authority to delve deeply into privacy, instead emphasizing the FAA's longstanding focus on aviation safety. On the other hand, aviation officials naturally accept that drones pose undeniable privacy challenges, and the dividing line between safety and privacy is often blurry. Having all this in mind, the FAA has opted for a rather privacy-opportunistic stance. It has put the concept to good use when needed, for example, to explain the agency's slow progress, in keeping to FMRA's quixotically fast calendar. And in one quite narrow context, the FAA has separately added privacy to its traditional slate of activities, if only in limited fashion, while making no commitments to follow suit later.

The impetus for all this was, ironically enough, FMRA itself. Among many other things, the statute called for limited drone flight at special test ranges, in advance of the 2015 deadline for broader drone integration. A new fleet of flying robots couldn't be catapulted into American

airspace overnight; the policy and logistical obstacles obviously were far too numerous and far too difficult for that. FMRA therefore called for a gradual transition, during which the FAA would run a type of beta-testing program. Drones would fly under controlled conditions, on an interim basis, and furnish data needed to resolve some of the tougher dilemmas posed by more widespread flight.[29] The initiative would go forward at six test ranges, which had to be selected by a date certain—on or about August 12, 2012, as the leading drone advocacy group interpreted FMRA's text.

The outfit therefore complained when that date came and went, though without the FAA's having named any of its six proving grounds.[30] In a response sent one month afterwards, the agency's acting administrator, Michael Huerta, interpreted FMRA differently, and denied having missed any legally set deadline. But Huerta nevertheless justified the slower pace. "Privacy concerns have surfaced as a result of increased [drone] usage," he explained, "and this necessitates an extensive review of the privacy impacts of the test site program."[31] The message seemed clear enough. So far as the test sites were concerned, drone work (something very much within FAA's portfolio) was partially privacy work (something pretty well outside of that portfolio, until then anyway). And privacy work was hard and time-consuming, enough to make for some slow sledding.

The agency did make progress, and eventually completed its privacy workup. The agency named six test range operators in late December 2013.[32] And, echoing Huerta's earlier letter, the FAA's release announcing the test site selections also mentioned certain "privacy considerations" that the FAA had taken into account. In particular, the agency said it had developed privacy rules that test site operators would have to follow.[33]

After draft rules were issued, the public was offered an opportunity to comment; the agency then weighed the public's input before formulating some quite modest, final privacy requirements, in November 2013. They were essentially as follows: before proceeding, site operators would have to sign special contracts with the FAA. The contracts in turn would obligate each site operator to keep records of all drone flights, and to require each operator to have a written plan for use and retention of drone-collected data. Relatedly, the contracts also required the site operator: to maintain an openly available "privacy policy," the contents of which were left up to the operator, and compliance with which would be assessed by the operator annually, in a manner accessible to the public; to obey any applicable privacy laws, then existing and subsequently enacted; and to acknowledge that the FAA might suspend test site authorization, upon the commencement of civil or criminal proceedings by the government, for violation of applicable privacy laws. The FAA might even terminate the authorization outright, if litigation later "demonstrates [that the test site's] operation was in violation" of those laws.[34]

In this way, privacy became part of the FAA's long-term planning for unmanned aircraft. Recall that advocacy groups initially had pushed hard for the FAA to regulate privacy issues in a sweeping fashion. The agency resisted,[35] but acknowledged privacy's obvious centrality to the enterprise of bringing more drones to more of America's airspace. Thus the privacy rules, which, amidst a soup of qualifications and legalese, still managed to back the FAA into some modest, temporary duties in ensuring solicitude for privacy rights. At least theoretically, for so long as the test sites are in business—until February 2017 at the latest[36]—the FAA can yank the authorizations for sites where egregious privacy violations are committed.[37] In that sense, the FAA tenuously *has* claimed a new kind of privacy jurisdiction.

That jurisdiction is no doubt narrow and time-limited—two things the agency has emphasized, in seeking to tamp down expectations and avoid setting precedents. The final privacy rules govern *only* the six test sites. They do not commit the FAA to any forms of future privacy activity. Substantively, the rules also are pretty flimsy: site operators must have privacy policies, but just how rigorous or forgiving is up to the operators alone. Operators also must agree to obey current or future privacy law, mostly the state laws noted above—but that's something operators would have to do anyway, whether or not the FAA ever took an interest in test range activities. Finally, the FAA's power to suspend or rescind test site authorizations is conditioned upon prior action by state law enforcement or other regulators. A lawsuit by a private party, it seems, won't suffice. Regardless of who brings the case, proving a privacy violation to the FAA's satisfaction might well take considerable time and effort, maybe longer than a given test site's life span. Swish all this around, and the FAA's privacy standards (such as they are) start to seem pretty undemanding.

Still, those standards *do* exist. Like the FAA's trotting out of privacy as justification for slowly naming test ranges, they imply a subtle evolution in the FAA's job description, one occasioned by the singular complexity of domestic drone integration. This helps to explain why the FAA seems to embrace and to run from the concept at the same time. In issuing final test-range rules, the agency stressed the FAA's abiding goal of "provid[ing] the safest, most efficient aerospace system in the world, *[something that] does not include regulating privacy*."[38] Elsewhere in the same document, the agency explained that, by imposing privacy standards on test site operators, the FAA sought not to enter the privacy arena, but instead only to "inform the dialogue among policymakers, privacy advocates, and industry regarding the impact of UAS technologies on privacy."[39] It was literally true that the FAA wasn't making any new rules, and thus not "regulating" privacy; but clearly it also wasn't rejecting privacy policy as none of its business. The FAA's "roadmap" for domestic drone integration, also issued last year, sounds this note: it too denies a regulatory function for the FAA in privacy, while acknowledging at least some FAA efforts in the area.[40]

Congress apparently has caught on to this. Consistent with the above, it quietly has reaffirmed the FAA's small interest in privacy matters, while nevertheless emphasizing that the agency's job function remains essentially unchanged. Explanatory materials appended to the Consolidated Appropriations Act of 2014 observed "the primary mission of the FAA is to protect the safety of civil aviation and provide an efficient national airspace. Nothing in the [document] is intended to change that mission or hinder the FAA's ability to fulfill it."[41] These magic words uttered, Congress still went on to fiddle with the FAA's mission, if only just a little, by asking for it to undertake further privacy research:

> Without adequate safeguards, expanded use of UAS and their integration into the national airspace raise a host of concerns with respect to the privacy of individuals. For this reason, the FAA is directed to conduct a study on the implications of UAS integration into national airspace on individual privacy. The study should address the application of existing privacy law to UAS integration; identify gaps in existing law, especially with regard to the use and retention of personally identifiable information and imagery; and recommend next steps for how the FAA can address the impact of widespread use of UAS on individual privacy as it prepares to facilitate the integration of UAS into the national airspace.[42]

Note the "next steps" phrase and its gesture towards future FAA privacy work.

It would be wrong to over-read the language above, much as it would be wrong to over-read the FAA's malleable privacy rules for drone-test ranges. Congress is not making the FAA the foremost guarantor of privacy rights in the United States; it is not giving the FAA the authority to sue for egregious privacy lapses; it is not calling for the FAA to become some aviation-focused outpost of the Federal Trade Commission. Instead, the legislature is simply doing what the FAA has been doing for a while: reiterating the FAA's traditional remit in aviation safety, rejecting any implied dilution of its safety portfolio, and yet also quietly imposing modest new privacy responsibilities. It's more mission creep than power grab.

That mission creep should inform our thinking about civilian drones, "private" privacy, and federal-state cooperation. The work of the FAA since 2012 can be plotted out as data points on a white board. And when connected, these suggest a slightly upward trajectory. Federal regulators gradually are taking on (unilaterally, or on instructions from Congress) more work, in addressing the privacy and technology tradeoffs posed by domestic drones. Call this "informing dialogue," "regulating privacy" or something else; the label doesn't matter especially. More important is the fact that federal oversight of civilian drones—marginal though that oversight may be—is on the upswing.

A TEMPLATE FOR "PRIVATE" PRIVACY, DRONES AND AERIAL SURVEILLANCE: STATE LAW FOUNDATION WITH MODEST FEDERAL SUPERINTENDENCE

We thus can review the bidding: states have a loose, largely untested framework in place for regulating nongovernmental, aerial surveillance. This in turn is supplemented by tiny pockets of federal activity, which have expanded modestly since 2012. The nascent trend is to tinker with this arrangement rather than to reshape it radically—say, by enacting an all-encompassing, state-law-preempting privacy statute. Exhibit A is Congress's command to the FAA to study privacy issues further, following the agency's issuance of FAA-enforced privacy rules for test sites; Exhibit B, the White House's order and forthcoming NTIA principles. The latter reportedly will not address *all* privacy dilemmas associated with *all* forms of unmanned surveillance. Instead, after consulting with various stakeholders, NTIA eventually will issue voluntary privacy guidelines, which in turn will apply to commercial drone operations only, and which, as before, will reserve the defense of "private" privacy largely to background law.[43]

It is easy to imagine policy ideas that would keep the above architecture intact. By way of example, Congress could condition authorization to fly on a pledge to respect privacy. The FAA might insist that before receiving permission to operate an unmanned aircraft, a business or individual first would have to commit to observing applicable privacy laws.[44] Thereafter, the FAA would have discretion to rescind the operator's flight credentials, upon submission of proof that a court or similar body has faulted the operator for serious privacy violations under state law. The "seriousness" criterion here also could—and, so as not to jack up the cost of deploying a critical technology too much, likely should—be made stiff enough so as to capture only the worst varieties of unmanned aerial surveillance.[45]

Keep in mind the scope. The FAA's regulatory powers don't extend everywhere and to every mode of unmanned flight. The limitation has implications for any FAA measure affecting privacy. For example, hobbyists' "model aircraft" are mostly exempted from FAA regulation.[46] Going forward, how you feel about the evident regulatory gap probably has to do with how you feel about likely sources and locations of unmanned aerial surveillance. Thus, if you worry most about rampant Quadcopter eavesdropping, then the above proposal might not do that much to assuage you; such machines seemingly *can* be operated as "model aircraft," and thus require no FAA license. Conversely, an FAA-based oversight approach to privacy might help considerably, if you predict that the most intrusive surveillance technologies will be paired with larger-sized drones—that is, drones likely to come within the FAA's jurisdiction, and to require operator certification and training.[47]

A proposal like the above (or one like it) would mean only incremental change. After all, the FAA already exercises a comparable authority over operators of the six test ranges established under FMRA. It wouldn't take too much to have the FAA carry forward, on a permanent basis and with respect to unmanned aircraft within its jurisdiction, a variant of the humble privacy responsibilities it already has taken on unilaterally. Doing so would not obligate the FAA to

"regulate privacy" in some broad or agency-inappropriate fashion, either. Instead the states would do the regulating, and afterwards, private litigants and state regulators would do the litigating and state courts the adjudicating. The FAA would only get into the mix afterwards, and only in the most deserving of cases.

Of course, that the above or any other policy change would fit nicely with existing institutional arrangements does not justify that policy's adoption. But there are good reasons to extend federal oversight of drones and "private" privacy, while the adequacy of the underlying state law framework comes into sharper focus. Take the idea sketched out above. The largest companies have the greatest ability to acquire the most sophisticated unmanned aircraft, and thus also to engage in the most far-reaching surveillance. It happens that those same companies could be best situated to withstand the kinds of *ex post* remedies courts typically impose upon rampant privacy violators—injunctions, money damages, and the like. In that respect, the scheme above might prove helpful, by deterring the worst privacy violations—not the marginal or the really bad, but the *worst*—in advance of wholesale domestic drone integration, and in advance of long and uncertain litigation in state courts. But whatever the policy might ultimately look like, the federal government's competence in civilian drones and privacy, such as it is, should be brought to bear.[48]

CONCLUSION

A lack of mission-critical data cuts against having the federal government dive headlong into crafting liability rules for civilian drones and privacy. It would be hard to design a preemptive, national-level policy without knowing more about what sorts of drones will fly, what sorts of privacy rules will survive a first round of legal review, and so forth. State regulation and drone integration together will furnish some key answers to those questions over time. To put the point somewhat differently, the principal "drone federalist" arguments seem mostly correct.

But there's a downside, and it hints at small regulatory space that federal officials shouldn't be shy about filling. A lot of surveillance, intrusions on privacy, and First Amendment litigation will have to happen before workable and broadly applicable solutions come fully into view. As that process goes forward, the national government—the FAA in particular—has sufficient experience to minimize the short-run privacy costs.

It should take further steps to minimize them as domestic drone integration proceeds, and without fretting too much about diluting the agency's heartland expertise in aviation safety. The dividing line between safety and privacy isn't especially neat or obvious, as the post-FMRA years amply demonstrate.[49] And when all is said and done, the FAA will have a basic fluency in drone privacy, as well as a broad and deep understanding of drone safety, perhaps the two most critical pieces of the of domestic drone puzzle. The combination is unique and should not go to waste, as civilian drones grow less novel and more commonplace, and the country mulls the best approach to "private" privacy and aerial surveillance.

ENDNOTES

1 The very word "drone" suggests near or even total autonomy, and thus incorrectly describes the workings of unmanned aircraft, which typically obey the commands of human, ground-based pilots. Despite the inaccuracy, "drone" has become pervasive. I thus use the term here, in light of its widespread acceptance.

2 *See, e.g.,* Drone Aircraft Privacy and Transparency Act of 2013, S. 1639, 113th Cong. § 3 (2013) (amending rulemaking process required by federal domestic drone integration statute, and obligating Secretary of Transportation to "establish procedures to ensure that the integration of unmanned aircraft systems into the national airspace system is done in compliance with [] privacy principles.").

3 *See, e.g.*, Margot Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 Cal. L. Rev. 57, 67 (2014) (arguing that "Congress should defer to states on privacy regulations governing civilian drone use for video and audio surveillance," provided, among other things, that federal aviation officials condition the issuance of civilian drone licenses on the use of certain tracking mechanisms); Margot Kaminski, "Should States Determine if Drones Can Record Your Conversations?" *Constitution Daily* (Sept. 19, 2013) (similar).

Other scholars do not strictly oppose federal regulation of drones and privacy, but nevertheless believe the FAA should not take on any additional privacy duties, while also trying to figure out how to bring drones safely into American airspace. *See, e.g.,* Benjamin Wittes and John Villasenor, "FAA Regulation of Drones Will Challenge Our Privacy Expectations," *Washington Post* (April 19, 2012).

4 The Congressional Bi-Partisan Privacy Caucus does not oppose all federal privacy regulation, but argues that "federal privacy laws should not preempt *stronger state privacy laws.*" *See* "Congressional Bi-Partisan Privacy Caucus," *available at* http://joebarton.house.gov/congressional-bipartisan-privacy-caucus/ (emphasis added).

5 *See, e.g.,* Fl. Stat. § 934.50; Ut. Code § 63G-18-101; Mt. Code Ann. § 46-5-109-110. Similar legislation has been proposed at the federal level. *See, e.g.,* Preserving Freedom from Unwarranted Surveillance Act of 2012, S. 3287, 112th Cong. (2012).

6 *See* H.B. 2012 (April 3, 2013) (awaiting codification). Virginia's statutory ban sounds more rigorous than it actually is: notwithstanding the statute, drones still can fly lawfully, at an experimental drone test range operated under the auspices of Virginia Tech.

7 According to the Federal Aviation Administration Modernization and Reform Act of 2012 ("FMRA"), the agency has until late 2015 to set up rules for widespread flight by private and public drones. Pub. L. 122-95 § 332 (Feb. 14, 2012). In the meantime, public drone uses are authorized by the FAA on an *ad hoc* basis. *See generally* "Certificates of Waiver or Authorization" *available at* https://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/. As for private uses, the FAA likewise claims that these are generally barred, save only for operations involving research and development, market surveys and crew training; the agency has so far authorized only a handful of commercial operations. *See generally* "Special Airworthiness Certification," *available at* https://www.faa.gov/aircraft/air_cert/airworthiness_certification/sp_awcert/experiment/sac/; "Busting Myths About the FAA and Unmanned Aircraft," *available at* http://www.faa.gov/news/updates/?newsId=76240.

8 *See* "Status of 2014 Domestic Drone Legislation in the States" (April 22, 2014), *available at* https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states ("Like last year, almost all of the bills we're seeing require law enforcement to get a probable cause warrant before using a drone in an investigation."); *see also* Gregory S. McNeal, "Poorly Drafted Drone Laws May Shield Crimes From View," *Forbes* (July 8, 2014) ("Much of the anti-drone activists efforts, and the ACLU's in particular, are aimed at the threat of persistent and pervasive surveillance of the population by the government—that's an understandable and well grounded fear.")

9 As noted above, the FAA generally bans the commercial operation of unmanned aircraft, and issues *ad hoc* permission for such operation only sparingly. The agency only recently issued its first, ad-hoc approval for a small unmanned aircraft to survey certain parts of the Alaskan arctic. Earlier, the agency had given permission for two commercial drone flights over water. Federal Aviation Administration, "FAA Approves First Commercial UAS Flights Over Land," (June 10, 2014) http://www.faa.gov/news/press_releases/news_story.cfm?newsId=16354.

This rather unyielding approach has not deterred many civilian operators; in particular, businesses have tested the FAA's mettle, by flying drones in defiance of existing policy. The FAA has responded with various forms of enforcement action, including cease and desist orders. *See, e.g.,* Jason Koebler, "These Are the Companies the FAA has Harassed for Using Drones," *Vice* (Feb. 6, 2014). Local law enforcement also has sought to stop drone enthusiasts,

too. *See, e.g.,* Joe Coscarelli, "Drones Not Welcome Over Serena Williams at the U.S. Open," *New York Magazine* (Sept. 4, 2014).

10 *See* "President Barack Obama to Issue Executive Order on Drone Privacy," *Politico* (July 23, 2014).

11 I am especially indebted—generally and in the précis of state liability rules set forth in this section—to two pieces surveying the laws regulating civilian drones and privacy. One was authored by John Villasenor and is entitled *Observations From Above: Unmanned Aircraft Systems and Privacy*, 36 Harv. J. L. & Pub. Pol'y 458, 498-508 (2013); the other is Margot Kaminski's *Drone Federalism: Civilian Drones and the Things They Carry,* 4 Cal. L. Rev. 57 (2014). Only the latter specifically calls for a qualified form of "drone federalism."

With respect to federal law, I have in mind chiefly the Electronic Communications Privacy Act ("ECPA"). The statute is obviously implicated by many forms of surveillance, including, at least theoretically, that conducted from the air by private parties. But owing to its one-party consent defense, and its insistence that a plaintiff's "reasonable expectation of privacy" be offended by any unwelcome recording, "ECPA's application to private parties is unlikely to be a central concern of drone regulation." Kaminski, *Drone Federalism* at 58.

12 *See* Villasenor at 499-500 (among other things, citing Ariz. Rev. Stat. § 13-1501 and Or. Rev. Stat. § 164.205(3)(a), and discussing discrepancies between Arizona and Oregon criminal trespassing statutes.)

13 *Id*. It remains to be seen just how permissive or restrictive the courts will be, in cases alleging aerial trespass by drone over private real property. *See United States v. Causby,* 328 U.S. 256, 264 (1946) (asserting that if a landowner is to have full enjoyment of the land, "he must have exclusive control of the immediate reaches of the enveloping atmosphere."); Troy A. Rule, *Airspace in an Age of Drones* at 16-17 (forthcoming 2015) (noting uncertainty regarding precisely how far landowners may go, in seeking to exclude aerial trespassers).

14 Kaminski, *Civilian Drones* at 65 & n. 46 (citing William L. Prosser, *Privacy*, 48 Cal. L. Rev. 383, 391-92 (1960)).

15 *Id.; see also* Villasenor at 501-06.

16 *Id*. at 68 (citing, among other things, Cal. Civ. Code § 1708.8(b) (2011)).

17 *See* Villasenor at 499 ("If paparazzi are willing to engage in high speed freeway chases to capture images of a celebrity, it would be optimistic to the point of naïveté to expect them to always operate UAS in a manner respectful of privacy considerations and in compliance with FAA safety regulations.")

18 Tenn. Stat. Ann. § 70-4-302(a)(6).

19 *Id* §§ 39-13-903, 904.

20 Wisc. Stat. Ann. § 942.10.

21 *See* Kaminski, *Civilian Drones* at 66 ("Eventually, state civilian drone laws may converge into a floor that other states can each build on, with the more successful statutes—the ones that survive First Amendment scrutiny in courts— serving as the blueprint for eventual federal legislation. For now, however, we truly do not have a uniform idea of how to balance privacy against speech rights in gathering information.")

22 As noted above, the FAA purports to ban all drone operation for commercial purposes; hobbyists, though, can pilot "model aircraft" for recreation. An administrative law judge recently invalidated a fine the FAA had levied against Raphael Pirker, for having taken photographs for hire from his drone, somewhere near the University of Virginia. *See generally* Decisional Order, *Huerta v. Pirker*, Docket CP-217 (Mar. 6, 2014). The agency then had (and still has) yet to issue a mandatory rule governing small unmanned aircraft. Instead, aviation rules only exist right now for "aircraft," meaning the manned kind. And, as Pirker subsequently argued, with respect to "model aircraft," the FAA only has put forth an advisory circular, which itself urges voluntary compliance with FAA safety standards. *Id*. at 4. The administrative law judge reasoned that the model aircraft policy was just that—a policy—and that absent a validly enacted rule for *unmanned* aircraft like Pirker's, the agency lacked the power to slap him with a $10,000 civil penalty arising from a regulatory infraction. *Id*. at 7-8.

23 *See* Villasenor at 499; Kaminski, *Civilian Drones* at 61-64.

24 *See* Kaminski, *Civilian Drones* at 61-64.

25 *Id.* at 68 ("state legislation permits experimentation with these regulations, subject to crucial feedback from courts on First-Amendment boundaries. Congress should therefore wait to enact regulation of civilian use of drones for information-gathering until more data emerges out of state experimentation.").

26 *Id*. at 67 (qualifying proposal for state-based regulations for privacy and civilian drones on the Federal Aviation Administration's use of "its licensing programs to solve perhaps the biggest puzzle of drone regulation: how to provide notice or at least transparency to those being observed so they can determine whether they have been subjected to a privacy violation.")

27 *See* FMRA §§ 332(a)(1), 332(3).

28 FMRA touched on privacy matters only in a few stray places. One rather remote part of the statute, for example, deals with privacy protections for air passengers; another concerns oversight and audit powers conferred on the Comptroller General of the United States. *Id*. §§ 836, 1004. But as noted above, neither these nor any other of FMRA's privacy rules concern the broader integration of drones into U.S. airspace.

29 *See id*. § 332(c)(1) (commanding the Federal Aviation Administration to "establish … a program to integrate unmanned aircraft systems into the national airspace system at 6 test ranges."); Fact Sheet—FAA UAS Test Site Program (Dec. 30, 2013), *available at* http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=15575 ("[D]ata and other information related to the operation of UAS that is generated by the six test site operators will help the FAA answer key research questions such as solutions for "sense and avoid," command and control, ground control station standards and human factors, airworthiness, lost link procedures and the interface with the air traffic control system.")

30 Letter from Michael Toscano, President and CEO, Association for Unmanned Vehicle Systems International ("AUVSI"), to the Hon. Ray LaHood, Secretary of Transportation (Aug. 20, 2012). Both the Government Accountability Office and Congressional Research Service agreed with Toscano that the FAA had failed to meet a FMRA milestone, by not identifying any test sites in early August. *See, e.g.,* 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."); Government Accountability Office, "Unmanned Aircraft Systems: Measuring Progress and Addressing Potential Privacy Concerns Would Facilitate Integration into the National Airspace System" at 27 (Sept. 14, 2012) ("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.") (emphasis added).

31 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).

32 The University of Alaska, the State of Nevada, New York's Griffiss International Airport, the North Dakota Department of Commerce, Texas A&M University, and Virginia Tech all won the right to run experimental drone hubs. This list obscured a key practical point: the FAA's award of an operating authorization, to an institution located in one state, did not in fact obligate that institution to conduct drone flights there. Instead, an operator in location X might opt to hold its experimental flights in location Y or Z. *See* "F.A.A. Picks Diverse Sites to Carry Out Drone Tests," *N.Y. Times* (Dec. 30, 2013) (observing that Griffiss International Airport, in New York, "will fly some tests from Cape Cod in Massachusetts;" that Virginia Tech "will fly in Virginia [but] has an agreement with Rutgers University in New Jersey for testing there as well;" and that the University of Alaska "plans to test in Hawaii and Oregon as well as Alaska.")

33 "Fact Sheet—FAA UAS Test Site Program " (Dec. 30, 2013), *available at* http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=15575

34 *See generally* 78 Fed. Reg. 220 at 68360-64 (2013) (to be codified at 14 C.F.R. Part 91) ("Unmanned Aircraft System Test Site Program"); *see also, e.g.,* UAS Test Site Privacy Policy, Mid Atlantic Aviation Partnership, *available at* http://www.maap.ictas.vt.edu/wp-content/uploads/2014/06/FINAL-PRIVACY-POLICY.pdf (implementing final privacy rules, and among other things prohibiting "intentional data collection on individuals except when prior consent has been obtained."); "Nevada UAS Test Site Privacy Policy," *available at* http://www.nias-uas.com/sites/default/files/NevadaUASTestsiteprivacypolicy.pdf (implementing final privacy rules, and among other things proclaiming that if a drone flight "is conducted in a 'sensitive' area, steps will be taken to ensure sensors are not operated during that

time while over such area, including removing power from the sensor or confirming that the sensor is gimbaled in such a manner that data is not collected.")

35 Between the issuance of draft and final rules, some objected that "The FAA should focus on its safety mission [and] not engage in regulating privacy." 78 Fed. Reg. 220 at 68361. By way of response, the agency agreed that privacy regulation was not part of its statutory mission, but nevertheless recognized that there is substantial debate and difference of opinion among policy makers, advocacy groups, and members of the public as to whether [drone] operations at the Test Sites will raise novel privacy issues that are not addressed by existing legal frameworks. *Id.*

36 FMRA § 332(c) (1) ("The [test site] program shall terminate 5 years after the date of enactment of this Act.")

37 The contracts impose obligations on test site operators, rather than on the operators of drones that make use of the test sites. "Fact Sheet—FAA UAS Test Site Program " (Dec. 30, 2013), *available at* http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=15575

38 78 Fed. Reg. 220 at 68362-64 (2013) (emphasis added).

39 *Id.*

40 "Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS)" at 11 (Nov. 7, 2013) ("Road Map") ("Although the FAA's mission does not include developing or enforcing policies pertaining to privacy or civil liberties, experience with the UAS test sites will present an opportunity to inform the dialogue in the IPC and other interagency forums concerning the use of UAS technologies and the areas of privacy and civil liberties.")

41 *See* Explanatory Statement, Consolidated Appropriations Act of 2014, H.R. 3547, 113th Cong., Division L at 6 (Jan. 14, 2014).

42 *Id.*

43 Even a voluntary privacy measure may imply mandatory federal enforcement. Suppose Jeff Bezos soon realizes Amazon's fever dream of on-demand drone delivery. Suppose further that he pairs the realization with a corporate pledge of fealty to NTIA principles regarding commercial drone use, but then employs Amazon's delivery fleet to gather personal data in a manner contrary to the NTIA's guidance. In such a case, Amazon could theoretically face an action by the Federal Trade Commission. It has settled authority to punish material misrepresentations to consumers, including false promises to adhere to voluntary codes of corporate conduct. *See* 15 U.S.C. 45(a)(1) (declaring unlawful the use of deceptive acts or practices in or affecting interstate commerce); Complaint, *In the Matter of Myspace LLC*, No. C-4369 ¶¶ 14-16, 21-28 (Aug. 30, 2012) (alleging that company acted deceptively, by first pledging to adhere to voluntary international standards for data collection and retention, and then routinely flouting those standards).

44 Pilots of manned aircraft often must meet training and education requirements before getting the FAA's blessing to fly; the agency likely will take a similar approach for would-be pilots of at least some unmanned aircraft within the agency's purview. *See generally* 14 C.F.R. Part 61 (establishing minimal training and other criteria for operators of manned aircraft, including recreational, private and commercial pilots); "Unmanned Aircraft Systems (UAS) Comprehensive Plan: A Report on the Nation's UAS Path Forward" at 10 (Sept. 2012) (describing as a "national objective" the need to "Develop and propose regulatory changes, as required, to define licensing (certification) and training requirements for pilots/crew members, other … operational personnel[.]")

45 There is precedent here—though the policy proposals in question would go considerably further than this Essay, in extending the federal government's oversight of drones and privacy. As noted above, Professor Margot Kaminski has called upon the FAA to use its licensing mechanism, in order to ensure that affected persons learn of unlawful surveillance from unmanned aircraft. In that vein, Senator Ed Markey would expand the FAA's privacy jurisdiction by requiring drone operators to submit detailed data collection statements in advance of any drone surveillance—or risk revocation of operating credentials, or civil enforcement by the Federal Trade Commission or state attorneys general, or lawsuits from private parties. *See* Kaminski, *Civilian Drones* at 67 (citing Drone Aircraft Privacy and Transparency Act of 2013, H.R. 6676, 112th Cong. (2012)).

46 FMRA § 336 (barring agency rulemaking for "model aircraft," provided operators heed certain statutory commands; but not limiting the FAA Administrator's authority to "to pursue enforcement action against persons operating model aircraft who endanger the safety of the national airspace system.").

47 A "small" unmanned aircraft system means one weighing less than fifty-five pounds. *See id*. § 331(5), (6).

48 Federal privacy regulation is almost taken as a given in other sectors, ones no more important or privacy-sensitive than unmanned aerial surveillance. By way of example, the White House, privacy advocates, and industry all agree that, so far as consumer data privacy is concerned, broad-brush federal reforms are necessary. *See generally Consumer Data Privacy In a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Feb. 23, 2012) (establishing "Consumer Bill of Rights" and calling for related federal legislation). All three support the Obama Administration's plan for federal enforcement of voluntary codes of conduct, for online businesses that collect significant volumes of personal data from their customers. *Id*. at 23-24. It would seem odd to insist on rigorous federal privacy enforcement, when a company stores its customers' identifying data in an insecure manner; but to recoil from even minimal federal involvement, when images of home life are scooped up by a drone's camera or sensor in violation of state law.

49 One oft-cited example: a minimum altitude requirement can protect safety, by separating aircraft from people and property on the ground; but also privacy, by requiring surveillance to be conducted from at least a certain distance. *See* John Villasenor, "How Drone Safety Rules Can Also Help Protect Privacy," *Slate* (May 2, 2013). It remains to be seen how such knock-on effects will play out—for example, whether and to what extent divergent state approaches to drone privacy will bolster or frustrate the FAA's ability to enforce uniform safety standards.

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

Editors
Christine Jacobs
Beth Stone

Production & Layout
Beth Stone

EMAIL YOUR COMMENTS TO GSCOMMENTS@BROOKINGS.EDU