MERCATUS CENTER
George Mason University
Bridging the gap between academic ideas and real-world problems

PUBLIC INTEREST COMMENT

FEDERAL AVIATION ADMINISTRATION
Unmanned Aircraft System Test Site Program
Docket No: FAA-2013-0061

By Jerry Brito, Eli Dourado, and Adam Thierer

In the FAA Modernization and Reform Act of 2012 (FMRA),[1] Congress tasked the Federal Aviation Administration (FAA) with integrating unmanned aircraft systems (UASs), sometimes referred to as unmanned aerial vehicles or drones, into the National Airspace System by September 2015. As part of that effort, Congress directed the FAA to establish six test ranges to serve as integration pilot projects.[2] On February 22, 2013, the FAA issued a notice in the Federal Register announcing the process for selection of the sites and a request for public comment on its "proposed approach for addressing the privacy questions raised by the public and Congress with regard to the operation of unmanned aircraft systems within the test site program."[3]

The Technology Policy Program (TPP) of the Mercatus Center at George Mason University is dedicated to advancing knowledge of the impact of regulation on society. As part of its mission, TPP conducts careful and independent analyses employing contemporary economic scholarship to assess rulemaking proposals from the perspective of the public interest. Therefore, this comment on the FAA's Notice of Availability and Request for Comments does not represent the views of any particular affected party or special interest group, but is designed to assist the administration as it carries out Congress's mandate to safely integrate UASs into the National Airspace System.

CONCEIVING OF AIRSPACE AS A PLATFORM FOR INNOVATION

In analyzing the proposed policies being developed to carry out Congress's mandate, it is important to remember that the purpose of the mandate is to open America's skies to commercial UAS use in order to reap the social benefits that such use will bring.[4] The commercial use of UASs is an important step toward the efficient utilization of airspace. When an important national resource like airspace arbitrarily excludes commercial uses, the social costs of such exclusion may not always be immediately evident. For example, until 1989, commercial use of the

1. FAA Modernization and Reform Act of 2012, Pub L. No. 112-95, 126 Stat. 11 (hereinafter "FMRA").
2. Id., § 332(c).
3. Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 12259 (Feb. 22, 2013) (hereinafter, "FAA Notice"). It should be noted that, as will be shown below, Congress has raised no such privacy questions and has clearly omitted privacy considerations in its mandate to the FAA.
4. Jerry Brito, "Domestic Drones Are Coming Your Way," *Reason.com*, March 11, 2013, http://reason.com/archives/2013/03/11/domestic-drones-are-coming-your-way. Chris Anderson, "Why We Shouldn't Fear Personal Drones," *Time*, January 31, 2013, http://ideas.time.com/2013/01/31/why-we-shouldnt-fear-personal-drones.

For more information, contact:
Robin Bowen, (703) 993-8582, rbowen@mercatus.gmu.edu
Mercatus Center at George Mason University
3351 Fairfax Drive, 4th Floor, Arlington, VA 22201

Internet was prohibited. As a 1982 MIT handbook for the use of ARPAnet, the progenitor of what would become the Internet, warned students:

> It is considered illegal to use the ARPAnet for anything which is not in direct support of government business...Sending electronic mail over the ARPAnet for commercial profit or political purposes is both anti-social and illegal. By sending such messages, you can offend many people, and it is possible to get MIT in serious trouble with the government agencies which manage the ARPAnet.[5]

Undoubtedly, these commercial restrictions were put in place with the best of intentions. Had rulemakers understood the nature of the revolution that they were forestalling, they probably would never have imposed restrictions on commercial use of the Internet. They were simply unable to imagine the enormous benefits that would be generated by allowing the Internet to become an open platform for social and commercial innovation.

Vint Cerf, one of the "fathers of the Internet," credits "permissionless innovation" for the economic benefits that the Internet has generated.[6] As an open platform, the Internet allows entrepreneurs to try new business models and offer new services without seeking the approval of regulators beforehand.

Like the Internet, airspace is a platform for commercial and social innovation. We cannot accurately predict to what uses it will be put when restrictions on commercial use of UASs are lifted. Nevertheless, experience shows that it is vital that innovation and entrepreneurship be allowed to proceed without ex ante barriers imposed by regulators.[7] We therefore urge the FAA not to impose *any* prospective restrictions on the use of commercial UASs without clear evidence of actual, not merely hypothesized, harm.

PRIVACY AND COMMERCIAL UASS

The FAA's proposed privacy requirements for test range operators address concerns about hypothesized impositions on individual privacy. In view of the importance of "permissionless innovation" for the development of airspace as a platform for commercial and social entrepreneurship, we believe that the FAA should not impose any additional privacy rules for UAS Test Sites, for four reasons.

First, the FAA does not have the authority to impose such requirements. A plain reading of Subtitle B of the

5. L. Gordon Crovitz. "WeHelpedBuildThat.com," *Wall Street Journal,* July 29, 2012. http://online.wsj.com/article/SB10000872396390443931404577555073157895692.html

6. Vinton Cerf. "Keep the Internet Open," *New York Times*, May 24, 2012. http://www.nytimes.com/2012/05/25/opinion/keep-the-internet-open.html

7. As Brookings Institution senior fellow John Villasenor has recently explained,

> When considering potential new statutory UAS privacy protections, it is helpful to keep in mind what has occurred with the Internet and mobile telephones, two technologies that are associated with privacy threats that are in some respects much more significant than those that will arise from unmanned aircraft. Both the Internet and mobile phones grew as fast as their underlying technologies enabled. As a result, the public and legislative dialogue regarding how best to address the privacy issues they raise has been conducted with a strong appreciation of their benefits. By contrast, while the privacy concerns associated with domestic UAS are real and deserving of attention, they are getting significant focus long before the potential benefits of the technology are widely recognized. . . .
>
> If, in 1995, comprehensive legislation to protect Internet privacy had been enacted, it would have utterly failed to anticipate the complexities that arose after the turn of the century with the growth of social networking and location-based wireless services. The Internet has proven useful and valuable in ways that were difficult to imagine over a decade and a half ago, and it has created privacy challenges that were equally difficult to imagine. Legislative initiatives in the mid-1990s to heavily regulate the Internet in the name of privacy would likely have impeded its growth while also failing to address the more complex privacy issues that arose years later.

John Villasenor, "Observations from Above: Unmanned Aircraft Systems and Privacy," *Harvard Journal of Law & Public Policy* 36, no. 2 (2013): 517.

FMRA (the relevant section that covers UASs) reveals that Congress's charge to the FAA is simply to ensure the safe integration of UASs into the national airspace.[8] There are over 20 references to safety in the section, but not one reference to privacy or related concerns.[9] Additionally, the specific section mandating the establishment of test ranges lists six requirements that the administrator must meet in doing so.[10] These requirements exclude privacy considerations, suggesting that Congress did not intend to give the FAA any authority to include privacy consideration in its requirements. This view is buttressed by the fact that Congress is now considering the Drone Aircraft Privacy and Transparency Act of 2013, which would amend FMRA to require the FAA to develop privacy regulations in conjunction with the Federal Trade Commission and the Departments of Commerce and Homeland Security.[11] The implication is that at least some in Congress do not believe the FAA now has a privacy mandate. These facts comport with the FAA's history as a safety regulator. Indeed, the FAA's mission is "to provide the safest, most efficient aerospace system in the world,"[12] not to regulate for privacy.

Second, there is no evidence of a materialized harm that calls out for the proposed privacy requirements for test range operators. Prospective regulation at this juncture necessarily involves hypothesizing about the privacy violations that might arise. Since many of these harms may never materialize, forward-looking regulation is likely to overprotect privacy at the expense of innovation.

Third, as the proposed privacy requirements make clear, there already exist "federal, state, and other laws regarding the protection of an individual's right to privacy."[13] If harms due to privacy violations can be shown in court, damages will be awarded to the victims of those violations. Property law already governs trespass, and new court rulings may well expand the body of such law to encompass trespass by commercial UASs by focusing on actual cases and controversies, not merely imaginary hypotheticals. In particular, state "peeping Tom" laws already prohibit spying into individual homes.[14] Privacy torts—including the tort of intrusion upon seclusion—may also evolve in response to technological change and provide more avenues of recourse to plaintiffs seeking to protect their privacy rights.[15]

Fourth, adequate time should be afforded for the development of nongovernmental privacy protection mechanisms, ranging from market-based solutions to voluntary codes of conduct to individual self-help. The UAS industry has already developed a set of industry best practices, which include respect for the privacy of individuals.[16] These guidelines will likely be refined over time to meet new challenges and concerns. Industry norms and practices will also be influenced by pressure from media, activists, and consumers. Such less-restrictive solutions can greatly reduce the need for administrative intervention and can therefore increase the "permissionlessness" of airspace as a platform for innovation.

SOCIAL ADAPTATION

Patience is also wise here not only because it provides breathing space for future innovation, but also because it provides an opportunity to observe both the evolution of societal attitudes toward this new technology and how citizens adapt to it. It is possible that citizen attitudes about UASs will follow a familiar cycle we have seen play out in other contexts of initial *resistance*, gradual *adaptation*, and then eventual *assimilation* of that new technology

8. FMRA §§ 331–336.
9. Id.
10. FMRA § 332(c)(2)(A)–(F).
11. H.R. 1262, 113th Cong. 1st Sess. (1st Sess. 2013).
12. "Mission," Federal Aviation Administration, last modified April 23, 2010, http://www.faa.gov/about/mission/.
13. FAA Notice at 12260.
14. For example, see Va. Code Ann. § 18.2–130, Peeping or spying into dwelling or enclosure.
15. Restatement (Second) of Torts §§ 652B (1977).
16. "Unmanned Aircraft System Operations Industry 'Code of Conduct,'" Association for Unmanned Vehicle Systems International, accessed April 19, 2013, http://www.auvsi.org/conduct.

into society.[17] As technology author Larry Downes has observed, "after the initial panic, we almost always embrace the service that once violated our visceral sense of privacy."[18]

The introduction and evolution of the camera and photography provides a useful comparison in this regard. The camera was initially viewed as a highly disruptive force when photography became more widespread in the late 1800s. Indeed, the most important essay ever written on privacy law, Samuel D. Warren and Louis D. Brandeis's famous 1890 *Harvard Law Review* essay on "The Right to Privacy," decried the spread of the device.[19] The authors lamented that "instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life" and claimed that "numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.'"[20]

Similar fears often animate criticisms of UASs today. But just as personal norms and cultural attitudes toward cameras and public photography evolved quite rapidly over a century ago, attitudes about UASs may evolve in coming years. Just as cameras and photography became an ingrained part of the human experience, UASs might, as well. And just as social norms and etiquette evolved to address those who would use cameras in inappropriate, privacy-invasive ways, the same could happen for UASs.

Toward that end, just as we did not preemptively foreclose photographic innovation in the late 1800s, we should not foreclose UAS innovation today with overly prescriptive privacy regulations. Let innovation continue, and address tangible harms as they develop, if they do.

APPLICATION TO THE PROPOSED PRIVACY REQUIREMENTS

In light of these arguments, section (1) of the proposed privacy rules is inappropriate for the current stage of experimentation with commercial UASs. The requirement that site operators develop privacy policies that are informed by Fair Information Practice Principles is quite onerous for commercial operators of UASs, and its cost will likely outweigh any hypothetical benefits.

Consider, for example, a real estate agent that uses an UAS to create a detailed, three-dimensional photograph of the exterior of a property that is for sale. In doing so, the UAS inadvertently captures images of passersby in the street adjacent the property. According to so-called Fair Information Practice Principles,[21] must the UAS operator treat the passersby as potential victims of privacy violation? If so, then would the following requirements apply?

- To give all passersby notice of data collection before any photos are taken.
- To publicly identify the real estate agent before any photos are taken.
- To ensure that passersby understand that pictures of their faces and information about their whereabouts may be used on a real estate listing website.
- To give passersby a choice to opt-in or opt-out of such photography.
- To ensure that all inadvertently photographed passersby are given access to all photographs,

17. Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Minnesota Journal of Law, Science & Technology* 14, no. 1 (2013): 309–386.
18. Larry Downes, "A Rational Response to the Privacy 'Crisis,'" *Cato Institute Policy Analysis* no. 716 (Jan. 7, 2013): 10.
19. Samuel D. Warren & Louis D. Brandeis, "The Right to Privacy," *Harvard Law Review* 4 (1890): 193.
20. Id., at 195.
21. White House, *Consumer Data Privacy in a Networked World: A Framework for Protecting Privacy and Promoting Innovation in the Global Digital Economy* (Washington, DC, February 2012), 1, http://www.whitehouse.gov/sites/default/files/privacy-final.pdf. (listing as FIPPs: Transparency, Individual Control, Respect for Context, Security, Access, Accuracy, Focused Collection, and Accountability.)

including ones that are not used on the real estate listing website.

- To take expensive security measures to protect photos that were taken in a public place.

If adhered to strictly, Fair Information Practice Principles could make it prohibitively costly to use commercial UASs in applications as benign as taking photographs near public spaces. It is not clear that they could comply, in this context or any other, with Executive Order 13563, which requires that any regulation promulgated by an executive agency be cost-beneficial. It should also be noted that Fair Information Practice Principles are law nowhere else in the federal government.

CONCLUSION

While the FAA makes clear in its Notice that the privacy requirements it proposes are only applicable to the test site operators and "are not intended to pre-determine the long-term policy and regulatory framework under which commercial UASs would operate,"[22] it would be unreasonable to believe that the precedent set in this proceeding will not affect future deliberations. Indeed, the actions the FAA takes in this proceeding will begin to set the baseline for future UAS regulation.

The FAA further notes that the purpose of the privacy requirements are simply to "assure maximum transparency of privacy policies associated with UAS test site operations in order to engage all stakeholders in discussion about which privacy issues are raised by UAS operations and how law, public policy, and the industry practices should respond to those issues in the long run."[23] Unfortunately, by mandating that test site operators issue privacy policies and that those policies be informed by Fair Information Practice Principles, the FAA would be excluding an important possible alternative from the discussion: some operators might choose not to issue a privacy policy or adopt a non-FIPPs-compliant policy. If the true purpose of the pilot programs is "to develop a body of data and operational experiences to inform integration and the safe operation of these aircraft in the National Airspace System," then the FAA should seek not just geographic and climatic diversity, but policy diversity as well.

We therefore urge the FAA to strike section (1) of its proposed privacy regulations and rely exclusively on existing law and other mechanisms to protect individuals' privacy rights. We believe that such an approach would have the virtue of protecting individual rights, fostering the use of airspace as a platform for innovation, and allowing the scope of any necessary future privacy laws to be narrowly tailored by actual cases and controversies that emerge. To the extent that it remains the subject of public concern, the FAA should recognize its lack of authority on the matter, leaving further deliberations about the privacy implications of UASs to Congress, where elected officials can consider these concerns while weighing the benefits and costs of potential regulation.

22. FAA Notice, 12260.
23. Id., 12259.