# UNCHARTED TERRITORY: THE FAA AND THE REGULATION OF PRIVACY VIA RULEMAKING FOR DOMESTIC DRONES

MELISSA BARBEE*

TABLE OF CONTENTS



* J.D. Candidate, 2015, American University Washington College of Law; M.P.A., 2012, Northeastern University; B.A. Political Science & International Affairs, Northeastern University. I am grateful to the dedicated staff of the *Administrative Law Review* for their insightful suggestions, advice, and support.

## INTRODUCTION

The Federal Aviation Administration (FAA or Agency) has traditionally been tasked with regulating safety in the United States' national airspace.[1] However, the role of this vitally important federal agency may be shifting in order to keep up with the rapidly emerging use of private and public drone technology. Drones are unmanned aircraft that are piloted remotely and are equipped with surveillance equipment such as powerful cameras.[2] While their use is typically associated with military operations overseas,[3] drones are increasingly being used in the skies over the United States.[4] Unbeknownst to much of the public, local and federal law enforcement agencies, border patrol agents, firefighters, and public universities conducting research all use drones domestically.[5] Thus far, the FAA has tightly controlled the public use of domestic drones.[6] However, their use is expected to increase dramatically as drone technology continues to advance, the technology becomes more accessible and affordable, and the U.S. regulatory schemes are adapted to keep up with and support emerging technology.[7] As a result, the FAA has estimated that by 2030, more than 30,000 unmanned aircraft systems (UASs) will fly in the skies over the United States.[8] With nearly limitless possibilities for the uses of UASs,

1. *See* Fed. Aviation Admin., *Mission*, FAA.GOV, http://www.faa.gov/about/mission (last visited May 9, 2014) [hereinafter FAA, *Mission*] (stating that the mission of the Federal Aviation Administration (FAA) "is to provide the safest, most efficient aerospace system in the world").

2. *See* FAA, *Unmanned Aircraft (UAS) Questions and Answers*, FAA.GOV, http://www.faa.gov/about/initiatives/uas/uas_faq/#Qn1 (last updated July 26, 2013) [hereinafter FAA, *UAS Q & A*].

3. *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R42701, DRONES IN DOMESTIC SURVEILLANCE OPERATIONS: FOURTH AMENDMENT IMPLICATIONS AND LEGISLATIVE RESPONSES 2 (2013) (observing that the public most commonly associates drones with their military utility, typically in tracking and targeting suspected terrorists overseas).

4. *See* Chris Francescani, *From Hollywood to Kansas, Drones are Flying Under the Radar*, REUTERS, Mar. 3, 2013, http://www.reuters.com/article/2013/03/03/us-usa-drones-domestic-idUSBRE92206M20130303 (detailing the various current applications for drones, including filming movies and sporting events, tracking wildfires, surveying crops, monitoring weather and wildlife patterns, and detecting illegal drugs and people crossing the nation's borders).

5. *See* FAA, *Fact Sheet—Unmanned Aircraft Systems (UAS)*, FAA.GOV, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153 (last updated Jan. 6, 2014) [hereinafter FAA, *Fact Sheet*].

6. *See id.*

7. *See* FED. AVIATION ADMIN., FAA AEROSPACE FORECAST: FISCAL YEARS 2010–2030 48 (2010), *available at* http://www.faa.gov/data_research/aviation/aerospace_forecasts/2010-2030/media/2010%20Forecast%20Doc.pdf [hereinafter FAA, *Forecast*].

8. *See id.*

domestic drones are expected to become a part of the everyday lives of Americans in the near future. However, the addition of such an enormous number of unmanned aircraft flying alongside and sharing airspace with manned aircraft will require complex modifications to the regulatory structure of the national airspace system (NAS).[9]

Because UASs will be operating in national airspace, the FAA is responsible for formulating regulations and policies on their safe integration and use.[10] To keep ahead of this emerging phenomenon and in anticipation of the regulatory challenges it will present, Congress has directed the FAA to develop a comprehensive plan for the safe and efficient integration of both public and private UASs into the national airspace through the FAA Modernization and Reform Act of 2012 (FMRA).[11] The all-inclusive regulation of UASs will present many unique challenges for the FAA. One of the foremost concerns is how the FAA can ensure that citizens' fundamental privacy rights will not be infringed upon once the nation's skies are teeming with UASs capable of sophisticated and intrusive surveillance.[12] Another concern is whether the FAA, which has rarely, if ever, implemented rules concerning the protection of fundamental privacy rights before, is adequately equipped to take on the role of privacy policy enforcer.[13] Taking on a new role concerned with adjudicating privacy rights has the potential to interfere with the most important responsibility of the FAA—ensuring that American airspace remains the safest airspace system in the world.[14]

This Comment argues that the FAA, which traditionally has the structure in place to focus solely on safety and security in the national airspace, is not the appropriate agency to regulate privacy policy and ensure that individual privacy rights are protected. Part I of this Comment provides an overview of UASs. Part II discusses the FAA's traditional and transforming regulatory role in the wake of increasing UAS use in the national airspace. This discussion includes an examination of the relevant provisions of the FMRA and the progress the FAA has made in developing a comprehensive plan for regulating UASs. Part III examines the FAA's stance on its responsibility to protect privacy rights, as well as the current resistance UAS integration is facing at local, state, and federal levels

9. *See* FAA, *Fact Sheet*, *supra* note 5.

10. *See* FAA, *Safety: The Foundation of Everything We Do*, FAA.GOV, http://www.faa.gov/about/safety_efficiency/ (last updated Feb. 1, 2013) [hereinafter FAA, *Safety*].

11. FAA Modernization and Reform Act of 2012 (FMRA), Pub. L. No. 112-95, § 332, 126 Stat. 11, 73–75 (2012) (codified at 49 U.S.C. § 40101).

12. *See* THOMPSON, *supra* note 3, at 1.

13. *Id.* at Summary.

14. *See* FAA, *Mission*, *supra* note 1.

because of the lingering privacy questions that have gone unanswered. Part IV considers the practicality of the FAA regulating privacy policy and argues that Congress is the more appropriate body for formulating and enforcing privacy policy. The Comment concludes with recommendations for the FAA as it moves forward with the integration of UASs, as well as recommendations for Congress if and when it decides to take on the issue of UAS privacy safeguards.

## I. OVERVIEW OF UNMANNED AIRCRAFT SYSTEMS

UASs are aerial aircraft that are controlled remotely by a pilot on the ground or independently by an on-board computer with pre-programmed routes.[15] UASs serve a variety of surveillance and wartime functions, and come in diverse shapes and sizes,[16] ranging from the size of a passenger jet to a hummingbird.[17] UASs, more commonly known as drones, have traditionally been technology exclusively reserved for military use in overseas operations.[18] UASs were originally developed by the U.S. military, contained very expensive technology, and were composed of generally classified materials.[19] However, in the past decade, with the explosion of the commercial availability of many military-developed technologies such as Global Positioning Systems (GPS), drone technology has become more affordable, user friendly, and accessible to even the most

15. *See* FAA, *UAS Q & A*, *supra* note 2 (defining a unmanned aerial system (UAS) as "the unmanned aircraft (UA) and all of the associated support equipment, control station, data links, telemetry, communications and navigation equipment, etc., necessary to operate the unmanned aircraft. The UA is the flying portion of the system, flown by a pilot via a ground control system, or autonomously through use of an on-board computer, communication links and any additional equipment that is necessary for the UA to operate safely.").

16. *See* FAA, *Fact Sheet*, *supra* note 5.

17. *See* Editorial, *The Dawning of Domestic Drones*, N.Y. TIMES, Dec. 25, 2012, http://www.nytimes.com/2012/12/26/opinion/the-dawning-of-domestic-drones.html?_r=0 (describing the "Nano Hummingbird" drone that has the capability to hover and take pictures, while weighing only 19 grams).

18. *See* THOMPSON, *supra* note 3, at 2 (stating that drones are most commonly associated with their military function, specifically in the Middle East where they are used to target and kill suspected Al Qaeda members and other members of terrorist organizations); *see also* Jefferson Morley, *Drones for "Urban Warfare"*, SALON (Apr. 24, 2012, 7:37 AM), http://www.salon.com/2012/04/24/drones_for_urban_warfare/ (observing that aerial surveillance technology was first developed in the "battle space" of America's war operations in the Middle East).

19. *See* Ben Popper, *Drones Over U.S. Soil: the Calm Before the Swarm*, THE VERGE (Mar. 13, 2013, 1:00 PM), http://www.theverge.com/2013/3/19/4120548/calm-before-the-swarm-domestic-drones-are-here.

amateur hobbyist.[20] One can now go on the Internet and purchase a highly-sophisticated UAS, equipped with GPS, the capability to affix a high-resolution camera, and capable of reaching speeds up to twenty-two miles per hour at an altitude of one thousand feet, for less than five hundred dollars.[21] The technology has advanced so much that some drones have even been developed to have the capability to crack Wi-Fi networks and intercept e-mails, cell phone conversations, and text messages.[22] Although this sophisticated technology has the potential to be used for good in the furtherance of the public interest, it could just as easily be misused.

UASs represent the fastest growing sector in the aviation industry.[23] According to FAA estimates, worldwide annual spending on research and development for all UASs will increase from $6.6 billion in 2013 to $11.4 billion in 2022.[24] To profit from this boom in the drone industry, at least fifty companies are in the process of developing over 150 different types of UASs.[25] With sales projections slated to reach $6 billion by the year 2016 in the United States alone, drone manufacturing companies have recognized the pattern of increased UAS use in the United States and have targeted American law enforcement and public safety agencies as potential customers.[26]

Because of the growing accessibility and ease of use of UASs, the FAA has estimated that there will be 30,000 UASs flying in the skies above America by the year 2030.[27] This use will be both public and private, as UASs have the potential to perform a number of useful, as well as

20. *Id.* (quoting Chris Anderson as describing how once-rare components used in military UAS technology, such as accelerometers, magnetometers, gyroscopes, and Global Positioning Systems (GPS) trackers, are now affordable and commercially available with the surge of mobile devices).

21. *See, e.g.*, DJI PHANTOM AERIAL UAV DRONE QUADCOPTER FOR GOPRO, AMAZON.COM, http://www.amazon.com/DJI-Phantom-Aerial-Drone-Quadcopter/dp/B00AGOSQI8 (last visited May 9, 2014); *see also* Popper, *supra* note 19 (describing DJI Innovations' Quadcopter Phantom and its sophisticated capabilities).

22. *See* Andy Greenberg, *Flying Drone Can Crack Wi-Fi Networks, Snoop on Cell Phones*, FORBES, (July 28, 2011), http://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/.

23. *See* FED. AVIATION ADMIN., FAA AEROSPACE FORECAST: FISCAL YEARS 2013–2033 65 (2013), *available at* http://www.faa.gov/about/office_org/headquarters_offices/apl/aviation_forecasts/aerospace_forecasts/2013-2033/media/2013_Forecast.pdf.

24. *See id.*

25. Morley, *supra* note 18; *see also* FAA, *Forecast*, *supra* note 7, at 48 (explaining that there are currently 100 private manufacturers, universities, and government organizations in the process of designing over 300 different types of UASs).

26. Morley, *supra* note 18.

27. FAA, *Forecast*, *supra* note 7, at 48.

questionable, applications domestically.[28] UASs are already used on a limited basis by government agencies, federal and local law enforcement agencies, research institutions, and other public entities for furthering the public interest. For example, UASs are used for firefighting, locating missing persons, monitoring weather, providing disaster relief, patrolling the border, and military training.[29] The Department of Homeland Security (DHS) regularly uses predator drones to patrol the U.S. border and survey for people, arms, and drugs crossing the border illegally.[30] In 2012, DHS assisted local law enforcement in North Dakota by using one of its predator drones for the first time to locate and aid in the capture of a wanted suspect.[31] DHS has also lent its drones to assist the Federal Bureau of Investigation (FBI), the Secret Service, the United States Forest Service, the Texas Rangers, and other local law enforcement agencies to conduct various operations.[32] It was recently revealed through a Freedom of Information Act request that DHS has considered the possibility of arming their UASs with non-lethal weapons to immobilize targets.[33]

Due to rapidly advancing technology, increased accessibility, and lower costs for cutting-edge surveillance equipment, commercially available UASs can now be equipped with super high-resolution cameras[34] and thermal infrared cameras capable of detecting individuals through walls and at great distances.[35] Furthermore, some UASs are capable of flying and surveying

28. *Id.*

29. *Id.*

30. THOMPSON, *supra* note 3, at 3.

31. Jason Koebler, *First Man Arrested With Drone Evidence Vows to Fight Case*, U.S. NEWS & WORLD REP., Apr. 9, 2012, http://www.usnews.com/news/articles/2012/04/09/first-man-arrested-with-drone-evidence-vows-to-fight-case.

32. DEP'T OF HOMELAND SEC. OFFICE OF INSPECTOR GEN., OIG-12-85, CBP'S USE OF UNMANNED AIRCRAFT SYSTEMS IN THE NATION'S BORDER SECURITY 6 (2012), *available at* http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-85_May12.pdf.

33. DEP'T OF HOMELAND SEC., CONCEPT OF OPERATIONS FOR CBP'S PREDATOR B UNMANNED AIRCRAFT SYSTEM: FISCAL YEAR 2010 REPORT TO CONGRESS 63 (2010), *available at* https://www.eff.org/files/filenode/cbp_uas_concept_of_operations.pdf.

34. Ryan Gallagher, *Could the Pentagon's 1.8 Gigapixel Drone Camera Be Used for Domestic Surveillance?*, SLATE (Feb. 6, 2013), http://www.slate.com/blogs/future_tense/2013/02/06/argus_is_could_the_pentagon_s_1_8_gigapixel_drone_camera_be_used_for_domestic.html (describing the world's highest resolution camera, a 1.8 gigapixel camera developed by the U.S. military for use on drones. The camera is capable of seeing a six-inch small object at 17,000 feet in the air; it is the "equivalent of having 100 Predator drones look at an area the size of a medium city at once.").

35. Barry Neild, *Not Just for Military Use, Drones Turn Civilian*, CNN, June 12, 2013, http://www.cnn.com/2012/07/12/world/europe/civilian-drones-farnborough; *see also* Brian Bennett, *Police Employ Predator Drone Spy Planes on Home Front*, L.A. TIMES, Dec. 10, 2011, http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211.

for up to fifty-four hours nonstop.[36] Due to the increasingly sophisticated and complex nature of commercially available surveillance equipment, many civil liberties groups are growing concerned over the potential for misuse of UASs by both public and private entities, and the prospect that such misuse will infringe upon individuals' privacy rights.[37]

Despite the authorized use of UASs by some public entities, the profit-making, commercial use of drones is currently illegal[38] and other civilian use is severely restricted.[39] However, one can imagine the day when a company such as Google will use a UAS for its aerial maps feature or a media outlet will use drones to capture breaking news in real time.[40] For example, the online retailer Amazon recently announced that it is in the process of developing a package delivery system using unmanned drones.[41]

Many other countries are already allowing domestic drones to be used for commercial purposes, with businesses finding innovative ways to integrate drones into their delivery methods. Organizers of a music festival in South Africa recently used a small drone to deliver beer via parachute to patrons who had placed their orders using a smartphone app.[42] Domino's Pizza recently tested its own drone, called the "DomiCopter," which

36. Neild, *supra* note 35 (explaining that the "Penguin B" drone, which is privately manufactured by UAV Factory at a cost of over $50,000, is capable of fifty-four-and-one-half hours of continuous flying).

37. *See, e.g.*, AM. CIVIL LIBERTIES UNION, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT 1 (2011), *available at* http://www.aclu.org/files/assets/protectingprivacyfromaerial surveillance.pdf [hereinafter ACLU, RECOMMENDATIONS] (recommending mechanisms to protect civil liberties with the increased prevalence of surveillance).

38. 14 C.F.R. § 91.319(a)(2) (2013); *see also* Matthew L. Wald, *Current Laws May Offer Little Shield Against Drones, Senators Are Told*, N.Y. TIMES, Mar. 20, 2013, http://www.nytimes.com/2013/03/21/us/politics/senate-panel-weighs-privacy-concerns-over-use-of-drones.html.

39. 14 C.F.R. § 91.319; *see also* FAA, *Fact Sheet*, *supra* note 5 (describing how commercial use of drones is prohibited, while civilian use is currently only available to universities and drone manufacturers for research and development purposes, and flight and sales demonstrations).

40. Greg McNeal, *A Primer on Domestic Drones: Legal, Policy, and Privacy Implications*, FORBES (Apr. 10, 2012), http://www.forbes.com/sites/gregorymcneal/2012/04/10/a-primer-on-domestic-drones-and-privacy-implications/.

41. The delivery service, called Amazon Prime Air, will be able to deliver packages to customers within thirty minutes of placing the order online. Joanna Stern, *Amazon Prime Air: Delivery by Drones Could Arrive as Early as 2015*, ABC NEWS, Dec. 1, 2013, http://abcnews.go.com/Technology/amazon-prime-air-delivery-drones-arrive-early-2015/story?id=21064960.

42. Rianne Houghton, *Drone Drops Beer at South African Music Festival*, DIGITAL SPY (Aug. 9, 2013), http://www.digitalspy.com/odd/news/a505460/drone-drops-beer-at-south-african-music-festival.html.

successfully delivered two pepperoni pizzas to a suburb of London.[43] The FMRA mandates a regulatory structure to enable the private and commercial use of UASs in the United States.[44] The FAA has estimated that as many as 7,500 civil and commercial UASs may be in use in the national airspace by 2018.[45]

## II. THE FAA'S STATUTORY AUTHORITY AND CURRENT REGULATORY FRAMEWORK

The FAA's foremost mission is to ensure safety in the nation's airspace.[46] To this end, the Agency is responsible for regulating the domestic use of UASs.[47] Safeguarding the nation's airspace has been the FAA's mission since its inception in 1958 with the passage of the Federal Aviation Act.[48] Congress believed it was important to have an independent agency tasked solely with providing and overseeing a safe and efficient NAS.[49] Although the FAA became an organization within the Department of Transportation in the 1960s, it retained its exclusive authority over regulating all civil aviation operations in the NAS.[50]

Congress grants the FAA authority to make and enforce rules to aid in the implementation of laws it passes.[51] The enabling legislation governing the FAA grants the administrator the authority to regulate the NAS by adopting regulations through rulemaking to ensure the safety of aircraft and the efficient use of airspace.[52] With the passage of the FMRA, Congress granted the FAA the authority to pass the appropriate regulations to

43. Nidhi Subbaraman, *Domino's 'DomiCopter' Drone Can Deliver Two Large Pepperonis*, NBCNEWS.COM (June 3, 2013), http://www.nbcnews.com/technology/dominos-domicopter-drone-can-deliver-two-large-pepperonis-6C10182466.

44. FMRA, Pub. L. No. 112-95, § 332, 126 Stat. 11, 73–75 (2012) (codified at 49 U.S.C. § 40101).

45. FAA AEROSPACE FORECAST, *supra* note 23, at 66.

46. *See* FAA, *Mission*, *supra* note 1.

47. *See* FMRA § 332.

48. Federal Aviation Act of 1958, Pub. L. No. 85-726, 72 Stat. 731 (1958).

49. At that time, it was called the "Federal Aviation Agency." *See id.*; *see also* FAA, *A Brief History of the FAA*, FAA.GOV, https://www.faa.gov/about/history/brief_history/#origins (last modified Feb. 1, 2010) [hereinafter FAA, *Brief History*].

50. At which time the Agency became the Federal Aviation Administration. *See* FAA, *Brief History*, *supra* note 49; *see also* Federal Aviation Act of 1958, *supra* note 48, at § 301(a).

51. *See* OFFICE OF INFORMATION AND REGULATORY AFFAIRS, FAQS/RESOURCES, REGINFO.GOV, http://www.reginfo.gov/public/jsp/Utilities/faq.jsp (last visited May 9, 2014).

52. 49 U.S.C. § 40103(b)(1) (2006); *see also* Administrative Procedure Act, 5 U.S.C. § 553 (2012) (describing the process of rulemaking in which an agency drafts and publishes a proposed rule in the Federal Register, receives and responds to public comments, and publishes a final, binding rule in the Federal Register).

facilitate the implementation and enforcement of UASs into the NAS.[53]

### *A. FAA Regulation of UASs in the NAS*

The FAA's current policy toward the regulation of UASs in the NAS depends on the classification of the UAS as either public or civil.[54] A public UAS is an aircraft owned and operated by a local, state, or federal government entity, including the armed forces and law enforcement agencies, and put to public use.[55] A civil UAS is an aircraft owned and operated by any entity other than a public entity,[56] such as private individuals and private companies for commercial purposes. Regardless of its classification, any entity wanting to access the NAS must first be granted authorization from the FAA.[57]

The first authorization for an unmanned aircraft was granted in 1990.[58] Since then, the FAA has only authorized UASs for very limited purposes on a case-by-case basis, mainly for carrying out operations in the public interest.[59] Obtaining FAA authorization to fly a UAS in national airspace is quite difficult. Public entities such as government and law enforcement agencies that want to fly UASs in the national airspace must first apply for a Certificate of Waiver or Authorization (COA).[60] Once issued, public entities are heavily restricted in their permitted scope of activity.[61] The COA defines the parameters under which the operator is allowed to fly the UAS, including the permitted block of airspace, the time of day, and the length of time the entity is allowed to fly the UAS.[62] As a testament to the

53. FMRA, Pub. L. No. 112-95, § 332, 126 Stat. 11, 73–75 (2012) (codified at 49 U.S.C. § 40101).

54. *See* Unmanned Aircraft Operations in the National Airspace System, 72 Fed. Reg. 6689 (Feb. 13, 2007) (codified at 14 C.F.R. pt. 91).

55. 14 C.F.R. § 1.1 (2013); *see also* Unmanned Aircraft Operations in the National Airspace System, 72 Fed. Reg. at 6689 (describing some public uses for UASs: military and law enforcement surveillance, customs and border control, and first responder reports on weather, natural disasters, or other catastrophes).

56. 14 C.F.R. § 1.1.

57. Unmanned Aircraft Operations in the National Airspace System, 72 Fed. Reg. 6689.

58. FAA, *Fact Sheet*, *supra* note 5.

59. *Id.* (giving examples of public interest missions, which include: firefighting, disaster relief, search and rescue, law enforcement, border and port surveillance, military training, scientific research, and environmental and weather monitoring).

60. Unmanned Aircraft Operations in the National Airspace System, 72 Fed. Reg. 6689.

61. *Id.*

62. *See id.*; s*ee also* FAA, *Fact Sheet*, *supra* note 5 (explaining that public UAS operators are also required to coordinate with the appropriate air traffic control facility, and must be able to ensure that it can maintain visual contact with the UAS at all times when it is in airspace

increasing role drones are playing in domestic surveillance, the FAA has been increasing the number of COAs it authorizes annually to public entities.[63] In 2009, only 146 COAs were issued; yet as of October 2013, the FAA had already issued 373 COAs to public entities.[64] Authorized UASs are heavily restricted on where they are allowed to fly in the national airspace; for instance, they are not allowed to fly in Class B airspace, which includes densely-populated urban areas and in high-traffic areas of manned aircraft, such as near airports.[65]

Currently, the only way for civil or private UAS operators to obtain authorization to fly their drones is to apply for a special airworthiness certificate, in the experimental category.[66] These experimental certificates are only issued to operators such as private drone manufacturers and universities to carry out research and development, training, and flight and sales demonstrations.[67] Obtaining one of these experimental certificates is quite rare and difficult,[68] making it virtually impossible for private companies or individual drone hobbyists to obtain FAA authorization for their UASs. Furthermore, commercial use of UASs is still strictly prohibited.[69]

### *B. The FAA Modernization and Reform Act of 2012*

Despite the strong interest by government and law enforcement agencies in utilizing UAS technology to assist in domestic surveillance, so far the FAA has tightly controlled UAS use in the national airspace.[70] Consequently, laws meant to regulate the use of UASs have been far

shared by other aircraft).

63. *See* FAA, *Fact Sheet*, *supra* note 5.

64. *See id.* (demonstrating that the number of Certificates of Wavier or Authorization (COAs) issued by the FAA has steadily increased every year, with the exception of 2012: 146 in 2009, 298 in 2010, 313 in 2011, 257 in 2012, and 373 as of October 31, 2013).

65. *Id.*

66. 14 C.F.R. §§ 21.191, 193, 195 (2013); *see also* 14 C.F.R. § 91.319 (2013).

67. Fed. Aviation Admin. Order No. 8130.34B Establishing Procedures for Issuing Special Airworthiness Certificates for Unmanned Aircraft Systems § 2 (Nov. 28, 2011), http://www.faa.gov/documentLibrary/media/Order/8130.34B.pdf; FAA, *Fact Sheet*, *supra* note 5.

68. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-981, UNMANNED AIRCRAFT SYSTEMS: MEASURING PROGRESS AND ADDRESSING POTENTIAL PRIVACY CONCERNS WOULD FACILITATE INTEGRATION INTO THE NATIONAL AIRSPACE SYSTEM 7 (2012) (demonstrating the rarity of experimental airworthiness certificates; between January 1, 2012 and July 13, 2012, the FAA only issued eight special airworthiness certificates for experimental use to four UAS manufacturers).

69. 14 C.F.R. § 91.319(a)(2); *see also* FAA, *Fact Sheet*, *supra* note 5.

70. ACLU, RECOMMENDATIONS, *supra* note 37, at 8.

outpaced by the rapid development of drone technology.[71] However, Congress, the powerful UAS industry lobby, and law enforcement agencies began to pressure the FAA to loosen its restrictions on UASs in anticipation of the rapid influx of UASs in the skies over the United States in coming years.[72] To stay abreast of the unique challenges this will present, Congress directed the FAA to begin the integration of both public and private UASs into the NAS in the FMRA.[73] In only seven pages of the three-hundred page FMRA, Congress stipulates that the FAA meet a number of deadlines for developing a comprehensive plan of rules, standards, and regulations to safely and efficiently integrate both public and private UASs into the national airspace.[74] The final deadline for fully implementing the comprehensive plan for UAS integration is ambitiously set for September 30, 2015.[75] To assist in streamlining the integration process and developing a uniform and efficient procedure for issuing both civil and public COAs, the FAA has since created the Unmanned Aircraft Systems Integration Office.[76]

The Act first mandates the FAA to develop a simpler, more streamlined process for public and private entities to apply for and receive COAs.[77] The provision directs the FAA to now allow both public and government agencies carrying out public safety operations to operate UASs without going through the COA process as long as the aircraft meets the following criteria: less than 4.4 pounds, operated within the line of sight of the operator, less than four hundred feet above the ground, flown during daylight hours, and at least five miles away from airports and other locations with aviation activities.[78]

The Act also mandates that the FAA establish a program to integrate UASs into the NAS at six test ranges in coordination with the National Aeronautics and Space Administration (NASA) and the Department of

71. Popper, *supra* note 19.

72. M. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29, 31 (2011).

73. FMRA, Pub. L. No. 112-95, § 332(4), 126 Stat. 11, 73 (codified at 49 U.S.C. § 40101).

74. *Id.* §§ 331–36.

75. *Id.* § 332(a)(3).

76. FAA, *Fact Sheet*, *supra* note 5.

77. *See* FMRA § 334(a)–(c).

78. *See id.* § 334(c)(2). *See generally* ASS'N FOR UNMANNED VEHICLE SYS. INT'L, 2011 ANNUAL REPORT, *available at* http://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807 f9a4e95d1ef1/UploadedImages/2011_AnnualReport.pdf (detailing how the Association for Unmanned Vehicle Systems International, a UAS lobbying group, was largely responsible for the language in the 2012 FMRA, specifically the immediate access of public safety agencies with drones less than 4.4 pounds, and the creation of test sites).

Defense.[79] The FAA will use the designated test sites to test all aspects of the safe and effective full integration of UASs into the national airspace, such as determining how UASs can be safely designated to share airspace with manned aircraft, how UASs will operate with air traffic control systems, ensuring that UASs will integrate properly with the Next Generation Air Transportation System,[80] and testing the safety and navigation systems of various UAS models.[81] The FMRA set a deadline of August 10, 2012 for the FAA to establish these six test sites,[82] but the FAA missed the deadline,[83] citing emerging privacy concerns.[84] The FAA did not even initiate a public comment period to collect questions and concerns about the proposed test ranges until February 2013, after which it began taking applications from state and local governments, universities, and other public entities to develop the six testing sites around the country.[85] The FAA finally selected the applicants to operate the six testing sites in December 2013.[86]

79. FMRA § 332(c)(3).

80. The Next Generation Air Transportation System (NexGen) is the new satellite-based system of air traffic management being implemented by the FAA, which will replace the traditional ground-based system of air traffic control of manned aircraft. *See* FAA, *What is NexGen?*, FAA.GOV, http://www.faa.gov/nextgen/why_nextgen_matters/what/ (last modified May 13, 2013).

81. FAA, *Fact Sheet*, *supra* note 5.

82. *See* FMRA § 332(c)(1).

83. *See* Saurabh Anand, *Hovering on the Horizon: Civilian Unmanned Aircraft*, 26 THE AIR & SPACE LAW. 18 (2013), *available at* http://www.americanbar.org/content/dam/aba/publications/air_space_lawyer/ASL_V26N1_anand.authcheckdam.pdf.

84. Michael P. Huerta, in a letter to Representative McKeon, explained the FAA's delay:

> Our target was to have the six test sites named by the end of 2012. However, increasing the use of UAS in our airspace also raises privacy issues, and these issues will need to be addressed as unmanned aircraft are safely integrated. We are working to move forward with the proposals for the six test sites as we evaluate options with our interagency partners to appropriately address privacy concerns regarding the expanded use of UAS.

Letter from Michael P. Huerta, Acting Adm'r, FAA, to Rep. McKeon (Nov. 1, 2012), available at http://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedFiles/FAA%20Response%20to%20Congressional%20Unmanned%20Systems%20Caucus%20on%20Test%20Site%20Delay%20-%20112812.pdf.

85. *See* JOINT PLANNING & DEVELOPMENT OFFICE (JPDO), UNMANNED AIRCRAFT SYSTEMS (UAS) COMPREHENSIVE PLAN: A REPORT ON THE NATION'S UAS PATH FORWARD, DEP'T OF TRANSP. 15 (Sept. 2013), *available at* http://www.faa.gov/about/office_org/headquarters_offices/agi/reports/media/UAS_Comprehensive_Plan.pdf.

86. There are six applicants to operate testing sites: the University of Alaska, the State of Nevada, New York's Griffiss International Airport, North Dakota Department of Commerce, Texas A&M University Corpus Cristi, and Virginia Polytechnic Institute and

## III. UASS AND PRIVACY RIGHTS

The current use of drones by domestic law enforcement agencies, coupled with the anticipated influx of private and public UASs in the national airspace, has drawn the attention of privacy and civil liberties advocates.[87] Many members of Congress, who themselves are responsible for prompting the speedy integration of UASs through the passage of the FMRA, and the public are concerned that the current regulatory system lacks sufficient safeguards that would ensure drones are not used to improperly spy on Americans.[88]

There is no express right to privacy in the United States Constitution; however, both the Supreme Court and Congress have recognized privacy as a fundamental right. For purposes relevant to the drone-privacy debate, the Fourth Amendment, which guards against unreasonable and warrantless searches and seizures,[89] is the most pertinent to a discussion of an individual's expectation of privacy. The rise of the use of drone technology in the United States is certain to raise a number of questions concerning an individual's expectation of privacy. With the proliferation of UASs, a number of invasive surveillance scenarios could potentially occur. Government entities and law enforcement agencies could spy on unsuspecting citizens and perform warrantless searches of their property; corporations could collect data on the private lives and movements of individuals to amass information for market research purposes or to sell customer lists to other corporations; private citizens could simply spy on one another; or criminals could use invasive imagery acquired from UASs to carry out illegal activities.

Privacy advocates fear that the constant presence of UASs in our everyday lives may become commonplace and will be allowed to further infringe on our rights as UASs are embraced by law enforcement for more controversial uses.[90] Furthermore, as UASs infiltrate every part of our

State University. FAA, FACT SHEET—FAA UAS TEST SITE PROGRAM, FAA.GOV, http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=15575 (last visited May 9, 2014).

87. *See* ACLU, RECOMMENDATIONS, *supra* note 37; *see also* ELECTRONIC FRONTIER FOUNDATION (EFF), PUBLIC COMMENTS OF THE EFF REGARDING PROPOSED PRIVACY REQUIREMENTS FOR THE UNMANNED AIRCRAFT SYSTEM TEST SITE PROGRAM (Apr. 23, 2013), *available at* https://www.eff.org/document/effs-comments-faa.

88. *See* THOMPSON, *supra* note 3, at Summary.

89. U.S. CONST. amend. IV ("The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.").

90. This occurrence is referred to as "mission creep." ACLU, RECOMMENDATIONS,

public lives, new uses for surveillance UASs will slowly expand.[91] Drones could potentially be equipped with non–lethal weapons (e.g. rubber bullets, tear gas, tasers) for crowd control and dispersal purposes, or even eventually be armed with lethal weapons for law enforcement purposes.[92] Although a seemingly far-fetched scenario, civil liberties advocates believe that it is a slippery slope once we allow UASs to carry out surveillance and law enforcement purposes.[93]

### *A. The FAA's Stance on Privacy*

The FAA has indicated that it intends to take privacy concerns into account.[94] The privacy policy currently espoused in the FAA's proposed regulations includes the provision that the test site operator must "operate in accordance with Federal, state, and other laws regarding the protection of an individual's right to privacy."[95] Although vague, these proposed rules suggest that the FAA has taken some privacy concerns seriously in its mandate to fully integrate UASs into the national airspace. However, the FAA has only mentioned the issue of privacy as it pertains to its UAS test site program, largely ignoring privacy as it relates to the bigger picture of full UAS integration.[96] The FAA acknowledged that its test site privacy requirements do not suggest it will adopt a long-term privacy regulatory framework for UAS use—only that it may help inform future policymakers and privacy advocates in the privacy debate.[97]

### *B. Current State and Federal Legislation Concerning Domestic Drones and Privacy*

With lingering concerns as to whether the FAA is the appropriate body to be taking on privacy policymaking and enforcement,[98] and unwilling to wait for the courts to decide the issue, several state and federal lawmakers

*supra* note 37, at 11.

91. *Id.*

92. *Id.*

93. *Id.* at 10–11 (explaining that "current trends" surrounding UAS usage suggest a "looming threat").

94. *See* Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 12,259, 12,260 (Feb. 22, 2013) (to be codified at 14 C.F.R. pt. 91).

95. *Id.*

96. *See* JPDO, *supra* note 85, at 7.

97. *See* Unmanned Aircraft System Test Site Program, 78 Fed. Reg. at 12,260.

98. *See* Matthew L. Wald, *Current Laws May Offer Little Shield Against Drones, Senators are Told*, N.Y. TIMES, Mar. 20, 2013, http://www.nytimes.com/2013/03/21/us/politics/senate-panel-weighs-privacy-concerns-over-use-of-drones.html (remarking that Rep. Barton and Rep. Markey have said that the FAA "had no jurisdiction in privacy, nor much expertise in the area").

have crafted legislation in anticipation of having to curb "big brother" style surveillance by the government and other entities.[99] Altogether, forty-three states have proposed legislation to place restrictions on the use of domestic drones for surveillance, with nine states having enacted legislation in 2013.[100] Moreover, the mayor of Seattle recently ordered the police department to abandon its plans to utilize two drones, which were obtained through a federal grant, its surveillance operations after residents and privacy advocates protested the drone program.[101] The support for restricting the use of UASs by privacy advocates and state and local lawmakers is indicative of the widespread concern for protecting civil liberties; however, these pieces of legislation, once enacted, are largely symbolic since the FAA has ultimate control over the NAS and federal law supersedes state law and local ordinances.[102]

The small town of Deer Trail, Colorado wants to have open-season on UASs flying over the town.[103] Town officials and residents are considering an ordinance that would allow hunters to apply for a license to shoot down drones in exchange for a cash reward.[104] Originally scheduled to take place in November 2013, the vote on the ordinance has been postponed while a district court rules on the ordinance's legality.[105] The FAA issued a warning in response to the proposed ordinance, reminding the public that the FAA is the sole authority in charge of regulating airspace.[106] The FAA also warned that it is illegal to shoot at an unmanned aircraft and such an act would result in civil or criminal liability, just as would firing at a

99. *See* Brian Montopoli, *Lawmakers Move to Limit Domestic Drones*, CBSNEWS.COM (May 16, 2013, 4:28 PM), http://www.cbsnews.com/8301-201_162-57584695/lawmakers-move-to-limit-domestic-drones/; *see also* Allie Bohm, *Status of Domestic Drone Legislation in the States*, AMERICAN CIVIL LIBERTIES UNION (Feb. 15, 2014), http://www.aclu.org/blog/technology-and-liberty/status-domestic-drone-legislation-states.

100. *See* Bohm, *supra* note 99.

101. *See* Laura L. Myers, *Seattle Mayor Grounds Police Drone Program*, REUTERS, Feb. 8, 2013, http://www.reuters.com/article/2013/02/08/us-usa-drones-seattle-idUSBRE91704H20130208.

102. *See* U.S. CONST. art. VI (The Supremacy Clause establishes that the Constitution and federal law takes precedence over state law, and if there is a conflict between the two, federal law prevails).

103. *See* Ben Wolfgang, *Drone-hunting Permits on Hold—Colorado Town to let Voters Decide in November*, WASH. TIMES, Aug. 7, 2013, http://www.washingtontimes.com/news/ drone-hunting-permits-hold-colorado-town-let-voter/.

104. *See id.*

105. *See* Ana Cabrera, *Colorado Town's Vote on Drone Ordinance Postponed*, CNN.COM (Dec. 10, 2013, 9:44 AM), http://www.cnn.com/2013/12/10/us/colorado-town-drone-ordinance/.

106. *See* Joan Lowy, *FAA Warns Against Shooting Guns at Drones*, HUFFINGTON POST, July 19, 2013, http://www.huffingtonpost.com/2013/07/19/faa-guns-drones_n_3624940.html.

manned aircraft.[107] Although the town of Deer Trail concedes that the drone hunting license would be more of a symbolic gesture than anything else—since nobody has actually witnessed a drone hovering above the town—Deer Trail represents the cross section of Americans who fear that widespread UAS use will result in the legitimization of government spying and surveillance on its citizens.[108]

In a further show of concern for protecting fundamental privacy rights, members of Congress have proposed three bills that would restrict the use of UASs for domestic surveillance.[109] The House and Senate Judiciary Committees have each held hearings on the issue of the domestic use of UASs.[110] The Preserving American Privacy Act of 2013, proposed by Representatives Zoe Lofgren and Ted Poe would require a public entity, either government or law enforcement, operating a UAS to minimize its collection of personally identifying information.[111] The bill also would ban the use of data obtained by a UAS without a warrant against a suspect in a criminal investigation,[112] and further calls for an outright ban on weaponized drones in national airspace.[113] A second bill, the Preserving Freedom from Unwarranted Surveillance Act of 2013, proposed by Senator Rand Paul, would prevent public officials from using UASs to collect evidence in criminal cases.[114] Representative Ed Markey introduced the Drone Aircraft Privacy and Transparency Act of 2013. This bill would amend the FMRA to mandate the Department of Transportation to conduct a study on the privacy risks posed by the integration of UASs into

107. *See id.*

108. *See* Wolfgang, *supra* note 103 (calling the ordinance a "pre-emptive strike" against drones).

109. *See* Preserving American Privacy Act of 2013, H.R. 637, 113th Cong. (2013); Preserving Freedom from Unwarranted Surveillance Act of 2013, S. 1016, 113th Cong. (2013); Drone Aircraft Privacy and Transparency Act of 2013, H.R. 2868, 113th Cong. (2013).

110. *See Eyes in the Sky: The Domestic Use of Unmanned Aerial Systems: Hearing Before the Subcomm. on Crime, Terrorism, Homeland Sec., and Investigations of the H. Comm. on the Judiciary*, 113th Cong. (2013); *see also Operating Unmanned Aircraft Systems in the National Airspace System: Assessing Research and Development Efforts to Ensure Safety: Hearing Before the Subcomm. on Oversight of the H. Comm. on Sci., Space, & Tech.*, 113th Cong. 1 (2013) [hereinafter *Hearing: Operating Unmanned Aircraft Systems*]; *The Future of Drones in America: Law Enforcement and Privacy Concerns*: *Hearing Before the S. Comm. on the Judiciary*, 113th Cong. (2013) [hereinafter *Hearing: Future of Drones*].

111. *See* Preserving American Privacy Act of 2013, H.R. 637, 113th Cong. § 3119b (2013).

112. *See* H.R. 637 § 3119(c).

113. *See id.* § 3119(h).

114. *See* Preserving Freedom from Unwarranted Surveillance Act of 2013, S. 1016, 113th Cong. § 10 (2013).

the national airspace.[115] However, despite these efforts by a handful of members of Congress to take action on protecting privacy rights, none of the three bills have moved past committee.[116]

### *C. The Divisive Debate Over the Appropriate Entity*

It could be years before the Supreme Court clarifies case law on the issue of whether data collected during an unmanned aerial surveillance operation constitutes a Fourth Amendment search. Furthermore, a persistently divisive Congress makes substantive federal privacy policy legislation regarding UAS use unlikely any time soon. Local policymakers and state legislatures have attempted to fill the privacy vacuum left by gaps in the legal framework, but those efforts are largely symbolic as these institutions may actually have little authority to regulate drone policy in national airspace. Because of the uncertainty over which entity has the authority to regulate privacy issues for UASs, there is no correct answer for who exactly has the responsibility to formulate domestic drone privacy policy.

The seemingly simple answer is the FAA. With the Congressional mandate encompassed in the FMRA, the FAA is the agency tasked with integrating UASs into the national airspace.[117] Some stakeholders claim that by extension, this mandate includes the FAA assuming the responsibility for formulating and implementing privacy regulations because it is a fundamental part of the integration process.[118] However, there is nothing expressly written into the FMRA mandate that requires the FAA to create privacy law protections as part of that integration.[119] The

115. *See* Drone Aircraft Privacy and Transparency Act of 2013, H.R. 2868, 113th Cong. § 2 (2013).

116. *See* Preserving American Privacy Act of 2013, H.R. 637, GOVTRACK.US, http://www.govtrack.us/congress/bills/113/hr637 (last visited May 9, 2014); Preserving Freedom from Unwarranted Surveillance Act of 2013, S. 1016, GOVTRACK.US, http://www.govtrack.us/congress/bills/113/s1016 (last visited May 9, 2014); Drone Aircraft Privacy and Transparency Act of 2013, H.R. 2868, GOVTRACK.US, http://www.govtrack.us/congress/bills/113/hr2868 (last visited May 9, 2014).

117. *See* FMRA Pub. L. No. 112-95, § 332, 126 Stat. 11, 73–75 (codified at 49 U.S.C. § 40101).

118. *See* ACLU, RECOMMENDATIONS, *supra* note 37, at 2 (arguing that the FAA's mandate extends to "protecting individuals . . . on the ground" and therefore has the obligation to protect individuals' fundamental right to privacy); *see also,* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 68, at 35–36.

119. *See* Harley Geiger, *How Congress Should Tackle the Drone Privacy Problem*, CTR. FOR DEMOCRACY & TECH. (Mar. 27, 2012), *available at* https://www.cdt.org/blogs/harley-geiger/2703how-congress-should-tackle-drone-privacy-problem (suggesting the FAA need not develop privacy rules).

FAA may not even have the legal authority to create broad privacy protections without being delegated that authority by Congress.[120] While the FAA has promised to consider the issue of privacy in its regulations, it has also acknowledged that it may not actually have the legal authority to enforce rules and regulations with regard to privacy.[121] Furthermore, FAA officials have suggested that the agency is ill-equipped to take on regulating privacy issues that do not affect safety since doing so would be outside of the FAA's mission.[122] Because of this uncertainty, there are stakeholders who believe that Congress should take the additional step of instructing the FAA to take privacy policy formulation into account as part of the FMRA mandate.[123]

Congress having left the FMRA mandate quite open-ended,[124] when privacy policy is undoubtedly one of the foremost concerns associated with UAS use, is perhaps indicative of its intention to let the FAA fill the void left in drone privacy law.[125] On the other hand, the language of the FMRA seems to specifically focus on safety in the integration of UASs, while the absence of any mention of privacy issues is glaring.[126] One could argue this is evidence that Congress's actual intention was for the FAA to focus on what it does best—safety—rather than privacy.[127]

Although it serves as the final authority on all aircraft operations in the NAS and can preempt local and state law, the FAA itself has suggested that, in the absence of widespread federal privacy law, existing state laws that protect individual privacy rights could potentially be applied in

120. *See* ALISSA M. DOLAN & RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R42940, INTEGRATION OF DRONES INTO DOMESTIC AIRSPACE: SELECTED LEGAL ISSUES 22 (2013) (arguing that federal agencies do not have "inherent power"—Congress must assign specific powers).

121. *The Future of Unmanned Aviation in the U.S. Economy: Safety and Privacy Concerns: Hearing Before the S. Comm. on Commerce, Sci., and Transp.,* 113th Cong. 2 (2014) [hereinafter *Hearing: Future of Unmanned Aviation*] (statement of Michael P. Huerta, Adm'r, Fed. Aviation Admin.) (testifying that the FAA's role is limited to the "safety and operational efficiency" of the national airspace system (NAS), and therefore, issues outside of that scope are beyond the FAA's authority).

122. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 68, at 36.

123. *Hearing: Future of Drones*, *supra* note 110 (statement of Ryan Calo, Assistant Professor, Univ. of Washington School of Law).

124. Under the law, the FAA has been broadly tasked with developing "a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system." *See* FMRA, Pub. L. No. 112-95, § 332, 126 Stat. 11, 73–75 (codified at 49 U.S.C. § 40101).

125. *See* DOLAN & THOMPSON, *supra* note 120, at 27.

126. FMRA § 332(a).

127. DOLAN & THOMPSON, *supra* note 120, at 27.

situations of UAS use infringing on fundamental rights.[128] Although the FAA's enabling statute proclaims the federal government "has exclusive sovereignty of airspace of the United States,"[129] and courts have long-held that the federal government preempts all attempts by the states to regulate aircraft safety,[130] numerous state legislatures have still attempted to pass their own regulations over UAS operations.[131] Arguments can be made for using state privacy regulatory structures already in place to protect infringements of privacy; however, if state laws attempt to regulate the use of UASs in any way and are challenged under the principle of federal preemption, it is likely most courts would find the laws to be unenforceable.[132]

There seems to be no definitive answer as to which entity is best positioned to take the lead in implementing safeguards to ensure that fundamental privacy rights are not infringed upon by UAS surveillance and usage. Currently, no federal agency has been granted the specific statutory authority by Congress to regulate privacy policy related to the integration and use of UASs in the NAS.[133] A top Government Accountability Office official testified at a congressional hearing that it is currently unknown which entity is responsible for regulating privacy concern issues in the UAS implementation process.[134] Some have suggested that the DHS or the Department of Justice (DOJ) would be better suited to address privacy policy since privacy concerns would most likely stem from those departments' surveillance and law enforcement operations.[135] No matter which legislative body, administrative agency, or group of agencies ends up formulating privacy-protective rules, such federal regulations are necessary to protect the fundamental right to privacy that Americans have come to expect.

128. JPDO, *supra* note 85, at 7.

129. 49 U.S.C. § 40103(a)(1) (2006).

130. *See, e.g.*, Abdullah v. Am. Airlines, Inc., 181 F.3d 363, 371 (3d Cir. 1999) ("Because the legislative history of the FAA and its judicial interpretation indicate that Congress's intent was to federally regulate aviation safety, we find that *any* state or territorial standards of care relating to aviation safety are federally preempted.").

131. *See* Bohm, *supra* note 99.

132. *See* Jol. A. Silversmith, *You Can't Regulate This: State Regulation of the Private Use of Unmanned Aircraft*, 26 AIR & SPACE LAW. 23 (2013), *available at* http://www.zsrlaw.com/images/stories/ASL_V26N3_WINTER13_Silversmith.pdf.

133. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 68, at 35.

134. *Hearing: Operating Unmanned Aircraft Systems*, *supra* note 110, at 63 (2013) (statement of Gerald L. Dillingham, Dir., Civil Aviation Issues, Gov't Accountability Office).

135. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 68, at 36.

## IV. THE PRACTICALITY OF THE FAA REGULATING PRIVACY POLICY

There is considerable debate whether the FAA even has the legal authority to regulate privacy rights.[136] Congress' mandate in the FMRA only directs the FAA to implement two sets of rules.[137] The first requires the FAA to "develop a comprehensive plan to safely accelerate the integration of civil unmanned aircraft systems into the national airspace system"[138] and to publish a final rule by August 14, 2015.[139] The second mandated rulemaking requires the FAA to issue a final rule on integrating "small unmanned aircraft systems that will allow for civil operation of such systems in the national airspace" by June 14, 2014.[140] The FMRA does not explicitly mandate the FAA to regulate privacy, nor does it explicitly provide the FAA with the authority to address privacy concerns in its regulatory rulemaking.[141]

The FAA has traditionally been a largely technical agency tasked with research, engineering, and development of new aviation technologies; operation of air traffic control and navigation systems; and regulating minimum standards for aircraft manufacturing, operation, and maintenance.[142] FAA employees are mostly technical and industrial professionals—air traffic controllers, safety inspectors, engineers, transportation systems specialists—all working toward the common goal of ensuring that the United States maintains the safest and most efficient NAS in the world.[143] A drastic change in mission, from one focused exclusively on safety to one split between safety and privacy, would likely require a substantial reorganization of the agency, starting with personnel. For instance, more bureaucrats and lawyers would be needed at the FAA to ensure that privacy laws are being properly implemented and enforced and that no unconstitutional invasions of privacy are being committed. The FAA, which currently has no constitutional lawyers on staff, would need to

136. *Compare* Dolan & Thompson, *supra* note 120, at 22 (stating that Congress must delegate certain powers to federal agencies), *and Hearing: Future of Unmanned Aviation*, *supra* note 121 (implying that privacy lies outside the scope of the FAA's statutory authority to regulate safety), *with Hearing: Future of Drones*, *supra* note 110, at 28 (testimony of Amie Stepanovich, Dir., Domestic Surveillance Project, Elec. Privacy Information Ctr.) (stating that the FAA should be the "primary regulating source").

137. FMRA § 332(b).

138. *Id.* § 332(a)(1).

139. *Id.* § 332(b)(2).

140. *Id.* § 332(b)(1).

141. *Id.* § 332; *see* DOLAN & THOMPSON, *supra* note 120, at 23.

142. FAA, FAA — WHAT WE DO, FAA.GOV, http://www.faa.gov/ about/mission/ activities/ (last visited May 9, 2014).

143. FAA, FAA—WHO WE ARE, FAA.GOV, http://www.faa.gov/jobs/who_we_are/ (last visited May 9, 2014).

reorganize its legal department in anticipation of these changes, as well as to prepare itself for needing to defend itself in privacy lawsuits.

Although it has carried out important regulatory rulemaking, the FAA has never been tasked with the responsibility to protect fundamental privacy rights, and specifically, the Fourth Amendment's protection against unreasonable and warrantless searches and seizures.[144] The FAA's foremost mission is to keep the national airspace system safe and efficient.[145] It is impractical for the FAA to be the entity in charge of regulating fundamental privacy rights because the FAA has very little, if any, expertise in that area.[146] Likewise, it is unwise to distract the agency from its critically important mission by forcing it to take on the unfamiliar responsibility of privacy rulemaking and enforcement. Instead, the FAA should continue to focus solely on how to safely integrate unmanned aerial systems into national airspace shared with manned aerial systems.[147]

The agency has already faced considerable challenges concerning how to safely integrate UASs into the national airspace, resulting in delays and missed deadlines.[148] Certainly, requiring the FAA to formulate privacy policy will create unique challenges and further add to the delays in implementation of the comprehensive plan.[149] With far more pressing responsibilities, it would be infeasible and a poor use of resources to have the FAA formulate and enforce privacy safeguards concerning UAS use.

## V. MOVING FORWARD

Although the FMRA mandate for the FAA to make rules regarding UASs integration may be read to include the responsibility to regulate privacy policy, because the FAA does not have the expertise or focus to take

144. DOLAN & THOMPSON, *supra* note 120, at 24*; see also* Wald, *supra* note 98.

145. FAA, *Mission*, *supra* note 1.

146. DOLAN & THOMPSON, *supra* note 120, at 23–24; *see Hearing: Future of Drones*, *supra* note 110, at 28 (testimony of Michael Toscano, President, Ass'n for Unmanned Vehicle Sys. Int'l.) (remarking that the FAA has "very limited, if any, expertise" in regulating privacy and that the Agency should stay focused on its mission of safety).

147. *See Hearing: Duture of Drones*, *supra* note 110, at 28 (testimony of Michael Toscano, President, Ass'n for Unmanned Vehicle Sys. Int'l).

148. *See* Letter from Michael P. Huerta, *supra* note 84 (identifying privacy issues as a chief operational challenge to establishing the six testing sites, which was delayed by nearly a year-and-a-half); *see also* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 68, at 27 (citing privacy concerns regarding the collection and use of information gathered by UASs as the cause for delay in the FAA seeking Requests for Proposals from applicants for its six testing sites); *see also* Anand, *supra* note 83, at 2–3.

149. *See* U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 68, at 38 (remarking that no federal agency has stepped forward to proactively address UAS privacy issues and this lack of movement may trigger further delays in implementing UASs into the NAS).

on comprehensive privacy policy, Congress may be the more appropriate body to legislate and enforce protections for fundamental privacy rights. In his concurrence in *United States v. Jones*,[150] Justice Alito wrote, "In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[151] Recognizing that Congress can play a far more effective role than the Judicial or the Executive Branch, Justice Alito called for legislative solutions for privacy law concerns. Overzealous government surveillance is most likely to be executed by the Executive Branch and the federal agencies that operate under the Executive, such as DHS, DOJ, the FBI, and the Drug Enforcement Agency. Moreover, it may be years before the Supreme Court hears a case regarding this issue. With the number of UASs performing a variety of public and law enforcement functions ever-increasing,[152] and with privacy laws lagging behind the advances in technology,[153] it is important for Congress to take the reins and act fast to pass UAS privacy law.

However, just because Congress is the body that should take the primary role in addressing domestic drone privacy law and enact legislation to protect civil liberties from being encroached upon by drones, this does not mean that the FAA cannot use its resources to assist in this endeavor. There are steps that the FAA can take, as part of its implementing of the mandates of the FMRA, to ensure that individuals' privacy rights are protected.

### *A. Recommendations for the FAA*

Although the FAA should not be tasked with formulating, implementing, and enforcing privacy right protections, it should still do its part to keep the UAS authorization process as democratic, open, and streamlined as possible to encourage the entities that will be utilizing UASs to respect fundamental privacy rights. Making the process transparent will encourage upholding privacy rights as well as expose those entities, both public and private, that infringe upon these rights. First, the FAA should make the information in the COA granting process publicly available so that the public can view which entities are flying UASs, over what airspace they will be flying, and for what purpose, with the exception of classified missions by

150. 132 S. Ct. 945, 957 (2012) (Alito, J., concurring).

151. *Id.* at 964 (Alito, J., concurring).

152. *See* FAA, *Forecast*, *supra* note 7, at 48.

153. U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-961T, PRIVACY: FEDERAL LAW SHOULD BE UPDATED TO ADDRESS CHANGING TECHNOLOGY LANDSCAPE 8–10 (2012) (Statement of Gregory C. Wilshusen, Dir., Info. Sec. Issues, Gov't Accountability Office).

government and law enforcement entities. All data concerning drone flights should be publicly available because the public remains skeptical of domestic UAS use due to their origins shrouded in secrecy and warfare. The word "drone" immediately calls to mind armed drones killing terrorist targets in distant lands.[154] The more publicly-available information there is, the more open-minded the public will become regarding the societal benefits that can be derived from domestic UAS use.[155]

Furthermore, the FAA should require anyone applying for a COA to operate a UAS to submit a statement of purpose, detailing what it intends to do with the data it collects and a plan for minimizing unnecessary intrusions into the privacy of individuals.[156] This information should be shared with the body or agency that is ultimately in charge of enforcing the UAS surveillance privacy law to ensure that the system is transparent and that information-sharing is efficient to minimize occurrences of infringement on individuals' civil liberties. The FAA should be involved in these steps to preserve civil liberties because, as the agency authorizing and denying COAs to UAS operators, it is the first point of interaction for operators and the ultimate authority on approving UASs in the national airspace. The FAA is in the unique position to require UAS operators to provide a plan for what they intend to do with UASs and the data collected, or the operator will not be issued a COA.

### *B. Recommendations for Congress*

Congress is the most appropriate body for updating existing and out-of-date federal privacy laws in order to meet the unique challenges of future UAS surveillance technology. Rapid technological advances that have taken place in the twenty-first century have made many of the country's privacy laws, some of which have not been updated since the 1970s, obsolete.[157] Since the widespread public and private use of UASs is

154. *See* Popper, *supra* note 19 (describing the public perception problem with UASs: "drones have entered the popular consciousness as robotic killing machines controlled by our government, [and therefore] introducing them to domestic airways as tools for law enforcement would only reinforce the image of them as operatives of Big Brother").

155. *See id.* (stating that the key to changing public perceptions is removing the function of drones as war machines or mediums for intrusive government surveillance in the minds of the public; instead, the public needs to see their utility in agriculture, or in finding missing children).

156. *Hearing: Future of Drones*, *supra* note 110, at 28 (testimony of Annie Stepanovich).

157. U.S. GOV'T ACCOUNTABILITY OFFICE, *supra* note 153, at 5 (describing how technological advances "have rendered some of the provisions of the Privacy Act and the E-Government Act of 2002 inadequate to fully protect all personally identifiable information collected, used, and maintained by the federal government.").

inevitable, it is important for Congress to act quickly so that it is prepared for the rapid influx of UASs in the sky once the FAA implements its comprehensive plan for full integration.[158] To meet its obligations to the American public, Congress needs to implement its own comprehensive plan of privacy standards to meet the privacy challenges ahead.[159]

First, Congress should enact baseline privacy laws for all UAS operators, both public and private, that must be followed as part of its comprehensive privacy policy. This would include full compliance with all safety and privacy regulations and parameters that have been established by the FAA, including any mandatory disclosures and reports required for COA authorization. These reports should describe the region and airspace where the drone will be flown, for what purpose the mission is to be conducted, and what surveillance equipment is onboard the UAS.[160] Congress should also include a provision in the law that mandates full disclosure of all data collected on UAS operations, regardless of whether the operation is for private or public use, or commercial or recreational in nature, as well as establish a procedure for ensuring that all the collected data is used and disposed of in an appropriate manner. Furthermore, all of the reports should be made viewable to the public online to guarantee transparency in the process and gain the public's trust.[161]

Next, Congress should adopt uniform guidelines to be followed by government agencies, law enforcement, and other public safety agencies, including a mandate that personally identifiable images or data gathered either intentionally or inadvertently during an operation should not be retained, unless they are pertinent to an ongoing investigation.[162] Furthermore, it should be unlawful under any circumstance for any public entity to weaponize its UASs.[163] Also, to prevent abuses of power and maintain public accountability, it is imperative for Congress to establish a strict warrant requirement for all drone surveillance used by law enforcement.[164]

Congress should also insist upon industry-wide standards for the UAS manufacturing industry. Congress should outlaw three types of drone activity: 1) arming with either nonlethal or lethal weapons, 2) intercepting

158. *See Hearing: Future of Drones*, *supra* note 110, at 58–59, 67 (written statement of Laura W. Murphy, Dir. of Am. Civil Liberties Union) (describing how it is critical that Congress act quickly since the courts cannot keep pace with rapidly developing drone technology).

159. *See id.* at 89–91.

160. *Id.* at 90.

161. *Id.*

162. ACLU, RECOMMENDATIONS, *supra* note 37, at 15–16.

163. Geiger, *supra* note 119.

164. *Hearing: Future of Drones*, *supra* note 110, at 90 (testimony of Amie Stepanovich).

mobile or internet communications, or 3) saving personally identifiable information, such as data, video, and images, indefinitely.[165] These recommendations, in conjunction with existing statutory law and case law concerning privacy, should ensure that individuals' Fourth Amendment rights are protected against unlawful infringement.

## CONCLUSION

The widespread use of UASs for both public and private entities is inevitable as the uses are nearly limitless. The potential to put drones to use for the public benefit is just too great to reverse the anticipated surge. However, with the eventual omnipresence of UASs in our everyday lives, the potential for misuse is also great. The courts have not yet carved out space in the legal framework for how individual privacy rights will be protected from the leering eyes of super cameras mounted on hovering drones, especially through government and law enforcement surveillance. Likewise, Congress has not taken any action to address the privacy concerns that will surely arise with the imminent integration of UASs into the nation's airspace. Therefore, it seems the responsibility may fall on the FAA as regulator of the nation's airspace.

Even though the FAA was tasked with the job of integrating UASs into the NAS,[166] it is not the appropriate agency for ensuring that fundamental privacy rights are protected with the influx of UASs. Already tasked with the supremely important role of ensuring safety in the national airspace, it would be irresponsible and impractical to distract the agency from this vitally important mission and force it to focus its efforts on an area where it lacks the expertise and infrastructure to enforce such rules. Congress is the entity that is much better equipped to formulate and implement privacy policies that will protect the public's Fourth Amendment rights from being infringed upon by the onslaught of drones in the skies above America. Congress has the expertise, the personnel, and the infrastructure in place to implement substantive privacy policies that will surely impact all Americans.

165. ACLU, RECOMMENDATIONS, *supra* note 37, at 16.

166. *See* FMRA, Pub. L. No. 112-95, § 332, 126 Stat. 11, 72–75 (codified at 49 U.S.C. § 40101).