NOTE

Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat Through Interagency Coordination

*Patrice Hendriksen**

ABSTRACT

Unmanned aircraft systems ("UASs"), popularly known as "drones," are an evolving technology that provides a tempting alternative to more traditional law enforcement surveillance methods. Their presence in the national airspace is a quickly approaching reality. The Federal Aviation Administration ("FAA") is the primary agency regulating UAS use, but its reach extends to safety, not privacy. The FAA must integrate UASs into the national airspace by 2015. UAS technology and its market are also changing. Models are becoming smaller, faster, and less expensive to build and operate. There will likely be 30,000 UASs in our skies by 2030, with law enforcement agencies representing their most significant future users.

Domestic UAS surveillance operations implicate the Fourth Amendment right to freedom from unreasonable searches and other privacy interests. UASs have great potential to violate citizens' "reasonable expectations of privacy" as explained by the Supreme Court in aerial surveillance and sense-enhancing technology cases because the technology lacks certain practical boundaries that formerly constrained traditional surveillance.

This Note proposes that Congress amend the FAA Modernization and Reform Act to mandate interagency coordination among UAS federal stake-

* J.D., expected May 2014, The George Washington University Law School; B.S., 2011, University of Delaware. I would like to thank Kerry McGrath for her insights and assistance with this Note, as well as the staff of *The George Washington Law Review*, particularly Vinny Cirilli, Jake Steele, Becca Wernicke, and Courtney Murtha, for their fantastic editorial work.

holders. Congress should require these stakeholders to create a Memorandum of Understanding that clarifies responsibilities, recommends permissible use guidelines, and creates accountability for the privacy implications of UAS integration. Such an amendment will effectively address the complexity of UAS operations and close the privacy gap that exists under the law today.

TABLE OF CONTENTS

INTRODUCTION

Attorney Bruce Quick condemned the June 2011 arrest of his client, Rodney Brossart, as laden with "guerrilla-like police tactics" that "smack[ed] of big brother."[1] What about Brossart's arrest did Quick find unusually violative? It marked the first drone-assisted arrest of an American citizen.[2]

When six cows strayed onto Brossart's 3000-acre Lakota, North Dakota farm, he refused to surrender them.[3] Instead, he and his family, armed with rifles and threatening to kill officers who came onto his property, engaged the police in a sixteen-hour standoff.[4] The Grand Forks Police Department SWAT team brought in a Predator drone, borrowed from the Department of Homeland Security.[5] A Predator is a large unmanned aircraft marketed as "the most combat-proven" drone in the world,[6] and has been deployed in the Balkans, Afghanistan, Iraq,[7] and now, North Dakota.

Grand Forks police explained that they dispatched the Predator only after obtaining arrest warrants, did not use it to determine whether a crime had been committed, and that no caselaw bars drone use.[8] The Predator surveilled the property to ensure that the Bros-

1 Jason Koebler, *Attorney: 'Guerilla-Like Police Tactics' Used in First American Drone Arrest*, U.S. NEWS & WORLD REP., May 3, 2012, http://www.usnews.com/news/articles/2012/05/03/attorney-guerilla-like-police-tactics-used-in-first-american-drone-arrest [hereinafter Koebler, *'Guerilla-Like Police Tactics'*].

2 *Id.*

3 Jason Koebler, *Court Upholds Domestic Drone Use in Arrest of American Citizen*, U.S. NEWS, Aug. 2, 2012, http://www.usnews.com/news/articles/2012/08/02/court-upholds-domestic-drone-use-in-arrest-of-american-citizen.

4 Koebler, *'Guerilla-Like Police Tactics*,' *supra* note 1.

5 *Id.* See Matthew L. Burow, Note, *The Sentinel Clouds Above the Nameless Crowd: Protecting Anonymity from Domestic Drones*, 39 NEW ENG. J. ON CRIM. & CIV. CONFINEMENT 427, 428, 452–54 (2013), for a discussion of how the Brossart arrest exposes a loophole in existing law whereby local police can access military-funded UASs so long as the operator is an executive agency, permitting their "unfettered access" to UASs.

6 *Predator UAS*, GEN. ATOMICS AERONAUTICAL, http://www.ga-asi.com/products/aircraft/predator.php (last visited Dec. 26, 2013).

7 Press Release, Gen. Atomics Aeronautical, Predator 107 Soars Past 20,000 Flight Hours (June 28, 2013), *available at* http://www.ga-asi.com/news_events/index.php?read=1&id=420.

8 State's Response to Defendants' Combined Motion to Dismiss at 12, State v. Brossart, Nos. 32-2011-CR-00049, 00071, 32-201-CR-00074, 32-2011-CR-00050, 00076, 32-2011-CR-00046, 32-2011-CR-00048, 32-2011-CR-00047 (N.D. Dist. Ct. Apr. 23, 2012).

sarts were unarmed during the arresting raid.[9] Brossart's motion to dismiss described the Predator as an "aerial spy plane"[10] and a "military-like aircraft,"[11] arguing that the warrantless operation justified dismissal of all charges or suppression of all subsequently seized evidence.[12] District Judge Joel Medd rejected that contention, determining that police did not improperly use the drone and that its use had no bearing on the contested charges.[13]

Public familiarity with unmanned aircrafts, popularly known as "drones," comes largely from their use in military operations abroad.[14] Unmanned aircrafts are aircrafts "operated without the possibility of direct human intervention from within or on the aircraft."[15] The preferred term, used by the Federal Aviation Administration ("FAA") and the international community, is "unmanned aircraft system" ("UAS").[16] "UAS" refers to the airframe as well as the associated communication links and control station.[17]

Contrasted with their manned counterparts, UASs may fly longer, slower, above, in, or below piloted aircraft zones and either

---

9 *See* Koebler, *'Guerilla-Like Police Tactics,' supra* note 1.

10 Brief in Support of Motion to Dismiss at 5, State v. Brossart, Nos. 32-2011-CR-00049, 00071, 32-201-CR-00074, 32-2011-CR-00050, 00076, 32-2011-CR-00046, 32-2011-CR-00048, 32-2011-CR-00047 (N.D. Dist. Ct. Apr. 10, 2012).

11 *Id.* at 19.

12 *Id.* at 19–22.

13 Memorandum Decision and Order Denying Motion to Dismiss at 12, State v. Brossart, Nos. 32-2011-CR-00049, 00071, 32-201-CR-00074, 32-2011-CR-00050, 00076, 32-2011-CR-00046, 32-2011-CR-00048, 32-2011-CR-00047 (N.D. Dist. Ct. Aug. 1, 2012).

14 JAY STANLEY & CATHERINE CRUMP, ACLU, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT 1 (2011); *see also* MONMOUTH UNIV. POLLING INST., U.S. SUPPORTS SOME DOMESTIC DRONE USE 1 (2012), *available at* http://www.monmouth.edu/assets/0/84/159/2147483694/3b904214-b247-4c28-a5a7-cf3ee1f0261c.pdf (reporting that "[a] majority of Americans have heard either a great deal (27%) or some (29%) news about the use of unmanned surveillance drones by the U.S. Military"). Much of the recent media attention on these aircrafts relates to President Obama's drone strike policy. *See, e.g.*, Michael Isikoff, *Justice Department Memo Reveals Legal Case for Drone Strikes on Americans*, NBC NEWS, Feb. 4, 2013, http://openchannel.nbcnews.com/_news/2013/02/04/16843014-justice-department-memo-reveals-legal-case-for-drone-strikes-on-americans?lite (credited with leaking the Department of Justice white paper discussing the legality of drone strikes abroad).

15 FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 331(8), 126 Stat. 11, 72.

16 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-08-511, UNMANNED AIRCRAFT SYSTEMS: FEDERAL ACTIONS NEEDED TO ENSURE SAFETY AND EXPAND THEIR POTENTIAL USES WITHIN THE NATIONAL AIRSPACE SYSTEM 6 (2008) [hereinafter FEDERAL ACTIONS NEEDED TO ENSURE SAFETY], *available at* http://www.gao.gov/assets/280/275328.pdf.

17 FAA Modernization and Reform Act § 331(9), 126 Stat. at 72. For a conceptual diagram of the primary UAS components, see FEDERAL ACTIONS NEEDED TO ENSURE SAFETY, *supra* note 16, at 7.

autonomously on a preprogrammed path or by responding to commands from a pilot-operated ground station.[18] A UAS can also be built and operated more cheaply than traditional aircrafts.[19] Imaging sensors of varying sophistication are "mounted to the underbellies" of UASs for data collection.[20]

Existing UAS models range dramatically in characteristics and capabilities. As one commentator explains, UASs "are evolving faster than Americans' ability to understand how, legally and ethically, to use them."[21] He describes the experience of operating this "radically new and deeply strange technology" as surreal:

> A drone isn't just a tool; when you use it you see and act through it—you inhabit it. It expands the reach of your body and senses in much the same way that the Internet expands your mind. The Net extends our virtual presence; drones extend our physical presence.[22]

Legislators,[23] public interest groups,[24] and the public[25] alike are resistant to the integration of this new, strange technology. They fear privacy violations, and with good reason.[26] UASs lack the "natural limits" that constrain traditional manned aircrafts.[27] They are capable of a "swarming, persistent presence, low-level but ubiquitous and

---

18 *See* FEDERAL ACTIONS NEEDED TO ENSURE SAFETY, *supra* note 16, at 7.

19 *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R42701, DRONES IN DOMESTIC SURVEILLANCE OPERATIONS: FOURTH AMENDMENT IMPLICATIONS AND LEGISLATIVE RESPONSES 15 (2013); BART ELIAS, CONG. RESEARCH SERV., R42718, PILOTLESS DRONES: BACKGROUND AND CONSIDERATIONS FOR CONGRESS REGARDING UNMANNED AIRCRAFT OPERATIONS IN THE NATIONAL AIRSPACE SYSTEM 11 (2012).

20 ELIAS, *supra* note 19, at 17.

21 Lev Grossman, *Game of Drones*, TIME, Feb. 11, 2013, at 28, 30.

22 *Id.* at 28.

23 Federal and state legislation has been proposed that would severely limit UAS use in the interest of privacy. *See, e.g.*, H.R. 6199, 112th Cong. (2012); Assemb. 3157, 215th Leg., Reg. Sess. (N.J. 2012).

24 *See, e.g.*, STANLEY & CRUMP, *supra* note 14, at 1; *Surveillance Drones*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/surveillance-drones (last visited Dec. 26, 2013).

25 A June 2013 report found that sixty-seven percent of those surveyed were somewhat or very concerned about the potential for UAS monitoring outside homes and in public spaces. INST. FOR HOMELAND SEC. SOLUTIONS, UNMANNED AIRCRAFT AND THE HUMAN ELEMENT: PUBLIC PERCEPTIONS AND FIRST RESPONDER CONCERNS 3 (2013), *available at* http://sites.duke.edu/ihss/files/2013/06/UAS-Research-Brief.pdf.

26 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 14, 29–32 (2012) [hereinafter MEASURING PROGRESS], for an assessment of other threats posed by UAS integration, including safety and national security.

27 *See* STANLEY & CRUMP, *supra* note 14, at 1.

above all anonymous."[28] As Brossart's arrest illustrates, domestic UAS operations are not a hypothetical threat. Although the Grand Forks Predator operation was narrow in scope, the appealingly lower cost and higher sophistication of UASs foretell their increased use in coming years.

This Note argues that domestic UAS surveillance operations implicate the Fourth Amendment right to freedom from unreasonable searches, as well as other privacy interests. Regulation of UAS operations is necessary to safeguard the rights of U.S. citizens. The FAA is presently the primary agency regulating UAS activity, but its reach extends primarily to UAS safety.[29] Other federal agencies are potentially valuable stakeholders in UAS integration.[30] This Note proposes that Congress mandate interagency communication through a Memorandum of Understanding ("MOU"), charging major federal agency stakeholders with clarifying responsibilities, recommending permissible use guidelines, and creating accountability for the privacy implications of UAS integration.

Part I provides the factual and legal background for this analysis, setting forth the current and projected status of domestic UAS use. Part II discusses relevant aspects of Fourth Amendment jurisprudence. Part III analyzes UAS surveillance under the Fourth Amendment, predicting that there will be insufficient limitations on this technology. Part IV proposes that Congress amend the FAA Modernization and Reform Act to direct interagency coordination on the privacy threat posed by UAS technology. Lastly, Part V identifies legislative and single-agency counterproposals, highlighting their inadequacies in constraining complex, developing UAS surveillance.

I. Approaching UAS Integration in Both Law and Practice

Domestic UAS presence is now a reality due to legal and technological changes in recent years. The FAA Modernization and Reform Act of 2012[31] charges the FAA with achieving safe UAS integration by 2015.[32] Simultaneously, UAS technology and its consumer market continue to develop.

---

28 Grossman, *supra* note 21, at 31; *see also* Stanley & Crump, *supra* note 14, at 1 (explaining that UASs may "eradicate existing practical limits on aerial monitoring," leading to "pervasive surveillance [and] police fishing expeditions").

29 *See infra* Part I.A.

30 *See infra* Part IV.A.

31 FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 11.

32 *Id.* §§ 332(a)(3), 334(b).

A. *The Legal Landscape: Congressionally Mandated Integration by 2015*

In 2012, Congress, dissatisfied with the pace of UAS integration, set an aggressive timeline to incorporate UASs into the national airspace system.[33] The FAA Modernization and Reform Act of 2012 charges the Secretary of Transportation with developing comprehensive plans for the safe and accelerated integration of civil and public UASs into the national airspace system.[34] Most of the Act's objectives must be satisfied by December 2015.[35] The FAA hopes to achieve "routine [UAS] access to the national airspace system after 2020."[36]

The FAA has made progress on several of the Act's mandates. It achieved its first milestone in March 2012, when it streamlined the authorization process for public agencies to fly UASs.[37] Presently, public agencies must apply to the FAA for a Certificate of Waiver or Authorization ("COA") to approve their specific flight operation.[38] Applicants complete an online form that inquires about the identity of the proponent; descriptions of the operation, UAS model, and its surveillance and detection capabilities; flight plan; aircrew certifications; and any special circumstances, among other details.[39] The FAA then assesses the safety of the proposed operation.[40] Under the streamlined process, the FAA responds to nonemergency requests in less than sixty days.[41] The FAA has issued an increasing number of COAs since 2009, with 327 COAs active as of February 15, 2013.[42]

---

33 MEASURING PROGRESS, *supra* note 26, at 23–24.

34 FAA Modernization and Reform Act §§ 332(a), 334(a), 126 Stat. at 73, 75–76.

35 *Id.* § 334(b); *see also* MEASURING PROGRESS, *supra* note *26, at 24–25.*

36 MEASURING PROGRESS, *supra* note 26, at 24.

37 *FAA Makes Progress with UAS Integration*, FED. AVIATION ADMIN., http://www.faa.gov/news/updates/?newsId=68004 (last modified May 14, 2012, 3:09 PM).

38 *Fact Sheet—Unmanned Aircraft Systems (UAS)*, FED. AVIATION ADMIN. (Feb. 19, 2013), http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153 [hereinafter *Fact Sheet*]; *see also* FAA Modernization and Reform Act § 331(2), 126 Stat. at 63 (defining COA).

39 To view a sample COA application, see FED. AVIATION ADMIN., SAMPLE COA APPLICATION (2008), *available at* http://www.faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/media/COA%20Sample%20Application%20v%201-1.pdf.

40 *Fact Sheet*, *supra* note 38.

41 *Id.*

42 *Id.* One hundred forty-six COAs were issued in 2009, 298 in 2010, 313 in 2011, and 257 in 2012. *Id.* Note that the number of COAs issued does not directly reflect the number of UASs in use; multiple missions may be conducted under one COA and a single agency may hold more than one COA. *See* MEASURING PROGRESS, *supra* note 26, at 7–8.

The FAA has also made progress regarding plans for the integration of civil UASs, as required by the Act.[43] In September 2013, the FAA's Joint Planning and Development Office ("JPDO") published its *Unmanned Aircraft Systems Comprehensive Plan*, a document setting forth interagency goals and objectives for the safe and efficient integration of UAS into the national airspace.[44] In November 2013, the FAA also released its five-year roadmap for civil UAS integration.[45]

Finally, the FAA anticipates selecting six test sites by the end of 2013, from which the agency will collect information to inform future rulemaking and policy decisions.[46] Although the FAA maintains that its mission is safety and not privacy, it will require site operators to comply with its final privacy requirements.[47] Rather than comply with a uniform FAA-defined privacy policy, operators will be required to create their own publicly available privacy policies, to be reviewed annually and updated as necessary to remain operationally current and effective.[48] Operators must also comply with applicable privacy laws and have a data retention policy.[49] Test site privacy policies are not to predetermine the regulatory framework that will apply when UASs are fully integrated, but may "inform the dialogue" when that framework is developed.[50]

B. The Practical Landscape: Continued Development and Diversity in Technology and the UAS Market

An understanding of the diversity and developments in UAS technology is necessary to assess their potential impact on citizens' privacy interests. A wide range of UAS models exist and can be outfitted with an equally diverse array of sense-enhancing technology.

---

43 FAA Modernization and Reform Act § 332(a)(1), (5), 126 Stat. at 73, 74 (requiring the Secretary of Transportation to develop a comprehensive plan and a five-year roadmap for the introduction of civil UASs into the national airspace system).

44 JOINT PLANNING & DEV. OFFICE, UNMANNED AIRCRAFT SYSTEMS (UAS) COMPREHENSIVE PLAN 3 (2013) [*hereinafter* COMPREHENSIVE PLAN].

45 *See* FED. AVIATION ADMIN., INTEGRATION OF CIVIL UNMANNED AIRCRAFT SYSTEMS (UAS) IN THE NATIONAL AIRSPACE SYSTEM (NAS) ROADMAP (2013).

46 COMPREHENSIVE PLAN, supra note 44, at 15.

47 Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 68,360, 68,361 (Nov. 14, 2013) ("The FAA's mission . . . does not include regulating privacy."); *see also infra* notes 174–82 and accompanying text.

48 Unmanned Aircraft System Test Site Program, 78 Fed. Reg. at 68,364.

49 *Id.*

50 COMPREHENSIVE PLAN, supra note 44, at 4.

As a result, UASs are well-suited to many types of missions, including use by law enforcement agencies.

1. Diversity of UAS Models

Existing UAS models and their payloads[51] vary immensely. Models are often divided into two broad categories by size. Small UASs weigh less than fifty-five pounds.[52] They typically "fly below 400 feet above ground level, can stay airborne for several hours, and can be used for reconnaissance, inspection, and surveillance."[53] Large UASs weigh more than fifty-five pounds.[54] They may "fly at altitudes up to or greater than 60,000 feet, some can remain airborne for multiple days, and are generally used for the purposes of surveillance, data gathering, and communications relay."[55]

This two-category division obscures the true diversity of UAS characteristics.[56] Consider the following Table, illustrating the range in weight, launch mechanism, wingspan, maximum speed, maximum altitude, and mission duration among various models:

---

51 "Payload" refers to the equipment or devices with which a UAS is outfitted. *See UAS Components*, UNMANNED AERIAL VEHICLE SYS. ASS'N, http://www.uavs.org/index.php?page=uas_components (last visited Dec. 26, 2013).

52 FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 331(6), 126 Stat. 11, 72. *But see Types of Lower Cost Aircraft*, NAT'L INST. OF JUST. (Feb. 19, 2013), http://nij.gov/topics/law-enforcement/operations/aviation/Pages/types-of-aircraft.aspx [hereinafter *Types of Aircraft*] ("A [small UAS] typically refers to an unmanned aircraft weighing less than 25 pounds . . . .").

53 MEASURING PROGRESS, *supra* note 26, at 5. The majority of UASs that will operate in the national airspace system will likely be small UASs. *Id.* at 5 n.8.

54 *See id.* at 5.

55 *Id.*

56 *See id.*; *see also* STANLEY & CRUMP, *supra* note 14, at 2–3 (dividing UASs into more categories descriptive of UAS specifications, including large fixed-wing aircrafts, small fixed-wing aircrafts, backpack crafts, hummingbirds, and blimps). The American Civil Liberties Union ("ACLU") apparently named its "hummingbird" category after the AeroVironment Nano Hummingbird, created for the Defense Advanced Research Projects Agency ("DARPA"). *Id.* The Nano Hummingbird weighs less than one ounce, including batteries and video camera, and has a wingspan of six and a half inches when outfitted with a removable bird-shaped body; it can hover or fly for about eight minutes and travel at eleven miles per hour. Press Release, AeroVironment, Inc., AeroVironment Develops World's First Fully Operational Life-Size Hummingbird-Like Unmanned Aircraft for DARPA (Feb. 17, 2011), *available at* http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird.

TABLE. SPECIFICATIONS OF VARIOUS UAS MODELS[57]

Model	SkySeer	Aerosonde	ScanEagle	Fire Scout	Predator B
Weight	4 lbs.	33.5 lbs.	38 lbs.	3150 lbs.	10,000 lbs.
Launch Mechanism	Hand launch	Catapult or from roof of fast-moving vehicle	Catapult	Vertical	Runway
Wingspan	N/A	9.5 ft.	10.2 ft.	27.5 ft.	66 ft.
Max. Speed	24 knots	60 knots	70 knots	125 knots	≥ 220 knots
Max. Altitude	11,000 ft.	15,000 ft.	16,400 ft.	20,000 ft.	50,000 ft.
Mission Duration	50 min.	≤ 30 hrs.	20 hrs.	≤ 8 hrs.	30 hrs.

2. *Sophistication of UAS Payloads*

The payloads affixed to UASs vary in type and sophistication. Common payloads include cameras and electro-optical imagers, infrared sensors, synthetic aperture radar, and other specialized sensors.[58] Cameras may range from off-the-shelf still or video cameras to sophisticated, high-resolution cameras.[59] Infrared sensors capture images that the naked eye or a regular camera cannot; these are used, for example, for nighttime or other conditions of poor visibility.[60] Payloads vary by mission—for example, the National Oceanic and Atmospheric Administration equipped UASs with instruments to gather and analyze air samples,[61] whereas law enforcement agencies may employ high-powered cameras, thermal imaging devices, and laser radar.[62] Law enforcement agencies may currently use UAS sensors to "identify individuals by location, clothing, and even some biological features like skin and hair color," but cannot yet "identify faces, weapons, license plates or other fine detail."[63] They may in the future, however, develop UAS sensors with the ability to both recognize and track such fine detail.[64]

---

57 Adapted from FEDERAL ACTIONS NEEDED TO ENSURE SAFETY, *supra* note 16, at 8.

58 ELIAS, *supra* note 19, at 17–19.

59 *Id.* at 17.

60 *Id.* at 17–18.

61 *Id.* at 19.

62 THOMPSON, *supra* note 19, at 3.

63 *Types of Aircraft*, *supra* note 52.

64 THOMPSON, *supra* note 19, at 3–4.

3. *Expansion of UAS Operations*

Given the range in capabilities, public users may find diverse applications for UASs. They are considered ideal for "dirty, dull, or dangerous" missions.[65] As of September 2012, domestic UAS missions were "limited" and consisted of "law enforcement, search and rescue, forensic photography, monitoring or fighting forest fires, border security, weather research, and scientific data collection."[66] Potential future uses include "commercial . . . pipeline, utility, and farm fence inspections; vehicular traffic monitoring; real-estate and construction-site photography; relaying telecommunications signals; fishery protection and monitoring; and crop dusting."[67]

Growing interest in domestic UAS use may be attributed to several factors: military application has shown UAS technology to be successful to date; the UAS industry is expanding; and, as trained UAS operators return from overseas military operations, their availability increases domestically.[68] Ultimately, forecasts predict that there may be 15,000 UASs in the domestic airspace by 2020, doubling to 30,000 by 2030.[69]

Most pertinent to citizens' privacy interests are UAS missions by law enforcement agencies. In January 2008, only about a dozen law enforcement agencies had contacted the FAA to discuss UAS use.[70] By July 2012, about 100 agencies had expressed an interest in using UASs to the Department of Justice,[71] and the FAA granted COAs to twelve state and local law enforcement agencies.[72] At least two law enforcement entities use UASs consistently.[73] Looking forward, state and local law enforcement agencies are the greatest potential users of small UASs because the vehicles offer a simple, cost-effective solution for the agencies' airborne activities.[74] Small UASs may cost a police department between $30,000 and $50,000—roughly equivalent to a pa-

---

65 ELIAS, *supra* note 19, at 2.

66 MEASURING PROGRESS, *supra* note 26, at 10.

67 *Id.*

68 FEDERAL ACTIONS NEEDED TO ENSURE SAFETY, *supra* note 16, at 3.

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

70 FEDERAL ACTIONS NEEDED TO ENSURE SAFETY, *supra* note 16, at 14.

71 MEASURING PROGRESS, *supra* note 26, at 27.

72 *Id.*

73 GERALD L. DILLINGHAM, U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-889T, UNMANNED AIRCRAFT SYSTEMS: USE IN THE NATIONAL AIRSPACE SYSTEM AND THE ROLE OF THE DEPARTMENT OF HOMELAND SECURITY 4–5 (2012).

74 MEASURING PROGRESS, *supra* note 26, at 11.

trol car.[75] An industry forecast predicts that local law enforcement agencies' interest in operating UASs will increase as 2017 approaches.[76] The lower cost is a driving factor behind UASs' threat to privacy: as UASs increase in affordability, law enforcement agencies may find it easier to use and possibly abuse the technology.

Neither the legal nor technological status of UASs will remain stagnant in coming years. The FAA aims to bring about the rapid, safe integration of UASs into the national airspace system. Technological improvements render UASs suitable for an increasing variety of operations, particularly by local and state law enforcement. An expanded UAS presence creates privacy concerns for potential targets of powerful, pervasive governmental surveillance.

II. UNDERSTANDING FOURTH AMENDMENT PROTECTIONS FROM UNREASONABLE SEARCHES

Governmental UAS surveillance and investigation implicate the Fourth Amendment, which constrains such operations. As explained by the American Civil Liberties Union ("ACLU"), the "potential for pervasive use [of UASs] in ordinary law enforcement operations and capacity for revealing far more than the naked eye" pose a worrying threat to citizens' constitutional rights.[77]

The Fourth Amendment protects "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures."[78] As a threshold matter, the Fourth Amendment limits only governmental action, and only action in the nature of an unreasonable search or a seizure.[79] This Part considers

---

75 *Id.* For example, Ben Miller, director of the Mesa County Sheriff's Office UAS program, explains that the Office's use of two UASs is due to cost—the UASs are less expensive than manned helicopters. Grossman, *supra* note 21, at 31. *But see* Ben Yount, *Drone On: Illinois Has New Regulations on Eyes in the Sky*, QUINCY J., Sept. 1, 2013, http://quincyjournal.com/above-the-fold/2013/09/01/drone-on-illinois-has-new-regulations-on-eyes-in-the-sky/ (explaining that budgetary constraints may constrain Illinois state police departments' UAS use more than new regulations).

76 FEDERAL ACTIONS NEEDED TO ENSURE SAFETY, *supra* note 16, at 14 (citing TEAL GROUP CORP., WORLD UNMANNED AERIAL VEHICLE SYSTEMS (2008)).

77 STANLEY & CRUMP, *supra* note 14, at 14.

78 U.S. CONST. amend. IV.

79 United States v. Jacobsen, 466 U.S. 109, 113–15 (1984) (holding that federal agents did not violate the Fourth Amendment when they removed and tested a white substance concealed within a package without a warrant, because employees of a private freight carrier had already independently opened and examined the package). A "search" and a "seizure" implicate different interests. "A 'search' occurs when an expectation of privacy that society is prepared to consider reasonable is infringed." *Id.* at 113. A "seizure" may be of property, which occurs when there is meaningful interference with one's possessory interests in that property, *id.*, or of a

predominant Fourth Amendment tests, and their application to developing technologies, in turn.

A. Limitations on "Searches" in General

Governmental UAS use will be subject to the same Fourth Amendment doctrine that constrains other searches. Courts apply one of two tests to determine whether a search has occurred: the reasonable expectation of privacy test announced in *Katz v. United States*[80] and the trespassory test revived in *United States v. Jones*.[81] The inquiry can be further informed by considering whether the place searched is one afforded special constitutional protections, such as the interior of the home.

1. The Reasonable Expectation of Privacy and Trespassory Tests

Today, as at the adoption of the Fourth Amendment, "to search mean[s] to look over or through for the purpose of finding something; to explore; to examine by inspection."[82] Early Fourth Amendment search cases turned on the occurrence or nonoccurrence of common law trespass.[83] In 1967, however, the Supreme Court moved away from this approach in *Katz v. United States*.[84]

In *Katz*, Federal Bureau of Investigation ("FBI") agents attached an electronic listening device to the outside of a public telephone booth without a warrant, listening to and recording Katz's conversation within.[85] The Court rejected both parties' formulation of the question presented as whether the telephone booth was a "constitutionally protected area," stating that "the Fourth Amendment protects people, not places."[86] Reasoning that the Fourth Amendment cannot turn merely on physical intrusion, the Court held that what a person "seeks to preserve as private . . . may be constitutionally protected"

---

person, which occurs when there is meaningful inference with an individual's freedom of movement, *id.* at 113 n.5.

80 Katz v. United States, 389 U.S. 347, 351 (1967).

81 United States v. Jones, 132 S. Ct. 945, 949–50 (2012).

82 Kyllo v. United States, 533 U.S. 27, 32 n.1 (2001) (internal quotation marks omitted).

83 *See, e.g.*, Olmstead v. United States, 277 U.S. 438, 464 (1928) (holding that wiretaps attached to telephone wires on the street did not constitute a Fourth Amendment search because there was no physical entry of the defendants' property); *see also Jones*, 132 S. Ct. at 949–50 (2012) ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass, at least until the latter half of the 20th century.").

84 *Katz*, 389 U.S. at 351.

85 *Id.* at 348.

86 *Id.* at 351.

even in the absence of a physical trespass.[87] The often-cited two-prong test for such nontrespassory searches was articulated by Justice Harlan in concurrence: "[F]irst that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.'"[88]

The Court held that the agents conducted an unreasonable search.[89] Katz exhibited a subjective expectation of privacy when he entered the booth, closed the door, and paid the toll;[90] in doing so, he was reasonably "entitled to assume that the words he utter[ed] into the mouthpiece [would] not be broadcast to the world."[91] The government violated the privacy on which he justifiably relied when it electronically listened to and recorded his conversation, offending the Fourth Amendment.[92]

Although the *Katz* test remains good law, the Court's most recent Fourth Amendment decisions have revived the early "property-based approach."[93] In *United States v. Jones*, FBI agents attached a global positioning system ("GPS") device to the undercarriage of Jones's Jeep without a warrant and tracked its movements over the next twenty-eight days.[94] The majority found this to be an unreasonable search because the agents physically occupied Jones's private property to obtain information.[95] Similarly, in *Florida v. Jardines*,[96] the Court held that officers violated the Fourth Amendment when they intruded upon the curtilage of Jardines's home to conduct a dog sniff for drugs.[97] Relying on the physical intrusion principle resurrected in

87 *Id.* at 351–53.

88 *Id.* at 361 (Harlan, J., concurring). This test has subsequently been described as the "lodestar," Smith v. Maryland, 442 U.S. 735, 739 (1979), and "touchstone," California v. Ciraolo, 476 U.S. 207, 211 (1986), of the Fourth Amendment analysis. The Court has at times, however, acknowledged the fallibility of the *Katz* test. *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) (noting that the *Katz* test has been criticized as circular); *Smith*, 442 U.S. at 740 n.5 (suggesting that the *Katz* test could prove inadequate if, for example, the government made a nationwide announcement that all homes would be subject to warrantless entry, thereby destroying citizens' subjective privacy expectations); *see also Jones*, 132 S. Ct. at 950–51 (stating that Jones's Fourth Amendment rights were not dependent on the *Katz* formulation).

89 *Katz*, 389 U.S. at 353.

90 *Id.* at 352.

91 *Id.*

92 *Id.* at 361 (Harlan, J., concurring).

93 *See* Florida v. Jardines, 133 S. Ct. 1409, 1414 (2013); *Jones*, 132 S. Ct. at 950.

94 *Jones*, 132 S. Ct. at 948.

95 *Id.* at 949. Justice Alito reached the same result in his concurrence by applying the *Katz* test, finding a "search" because the long-term monitoring of the vehicle's movements violated the respondent's reasonable expectation of privacy. *Id.* at 957–58, 964 (Alito, J., concurring).

96 Florida v. Jardines, 133 S. Ct. 1409 (2013).

97 *Id.* at 1417–18.

Jones, the Court found that a search occurred when the officers exceeded their implied license to enter Jardines's property when they approached his home for the sole purpose of conducting a drug sniff.[98] After *Jardines*, the government "undoubtedly" conducts a search when it "obtains information by physically intruding on persons, houses, papers, or effects."[99]

Where does this leave the *Katz* test? The *Jones* majority clarified that its decision does not mandate exclusive application of a trespassory test.[100] Rather, the Fourth Amendment guarantees, at a minimum, protection from government trespass; the *Katz* reasonable expectation of privacy test remains applicable in situations without physical trespass.[101]

2. The Continued Relevance of Constitutionally Protected Areas

Despite the Court's rejection of the "constitutionally protected areas" argument in *Katz*, subsequent decisions demonstrate the continuing relevance of this concept.[102] Commonly considered areas include the home, curtilage, and "open fields."

At one end of the spectrum, courts afford the interior of the home the greatest protection.[103] Under the *Katz* test, an individual expects to remain free from governmental intrusion within the interior of his home and society recognizes this expectation as reasonable.[104] Absent exigent circumstances, any warrantless search of a private residence is presumptively unreasonable.[105] Additionally, occupants have a reasonable and accepted expectation of privacy in the curtilage, or the area immediately surrounding the home.[106] This reasonable ex-

98 *Id.* at 1415–17.

99 *Id.* at 1414.

100 *Jones*, 132 S. Ct. at 953.

101 *Id.*; *see also Jardines*, 133 S. Ct. at 1414 (explaining that *Katz* adds to, but does not subtract from, the Fourth Amendment's baseline protections).

102 *See Jones*, 132 S. Ct. at 951 (citing United States v. Knotts, 460 U.S. 276, 286 (1983) (Brennan, J., concurring)) (explaining that the *Katz* test remained in force but did not erode the pre-*Katz* principle that governmental intrusion of a constitutionally protected area may constitute a Fourth Amendment violation).

103 Weeks v. United States, 232 U.S. 383, 390 (1914) (explaining that the Fourth Amendment is the fundamental law that "a man's house [is] his castle and [is] not to be invaded by any general authority to search").

104 *See* United States v. Karo, 468 U.S. 705, 714 (1984) (holding that warrantless monitoring of an electronic tracking device in a private residence not open to visual surveillance was a "search").

105 *Id.* at 714–15.

106 Dow Chem. Co. v. United States, 476 U.S. 227, 235 (1986). To determine whether an area is within the curtilage, courts consider: (1) proximity of the area to the home, (2) whether

pectation of privacy does not extend, however, to activities within the curtilage that any member of the public could observe.[107] Conversely, an "open field" fails to warrant similar protections.[108] The "open fields" doctrine encompasses more than areas that are literally "open" or "fields."[109] Rather, the doctrine covers any unoccupied land beyond the curtilage that does not provide a setting for the types of intimate activities that occur within the home.[110]

A comparison of two electronic tracking device cases considered by the Court in the 1980s best demonstrates the relevance of constitutionally protected areas. *United States v. Knotts*[111] and *United States v. Karo*[112] involved similar facts. In both cases, government agents installed a tracking device in a canister that the respondent would transfer.[113] The agents in *Knotts* tracked the device along public highways to its destination, the respondent's cabin.[114] No Fourth Amendment search occurred because everything the officers learned was observable to the naked eye.[115] The agents in *Karo*, however, continued to monitor the device after the respondent transported the canister off the public highway and into his private residence.[116] There, the Supreme Court found that a search occurred when the agents obtained critical facts about the interior of a private residence not open to visual surveillance.[117]

---

the area lies within an enclosure surrounding the home, (3) what the area is used for, and (4) any steps taken by the resident to conceal the area from observation. United States v. Dunn, 480 U.S. 294, 301 (1987). *Compare Dunn*, 480 U.S. at 301–02 (finding a barn located fifty yards from a house and outside the boundary of the fence surrounding the house was not within the curtilage), *with* Florida v. Riley, 488 U.S. 445, 448, 450 (1989) (finding a greenhouse located ten to twenty feet from a mobile home and enclosed within the fence surrounding the house was within the curtilage).

107 *See* California v. Ciraolo, 476 U.S. 207, 213 (1986) ("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares. Nor does the mere fact that an individual has taken measures to restrict some views of his activities preclude an officer's observations from a public vantage point where he has a right to be and which renders the activities clearly visible.").

108 United States v. Jones, 132 S. Ct. 945, 953 (2012); *see also Dow Chem. Co.*, 476 U.S. at 235–37 (contrasting the curtilage and open fields doctrines).

109 Oliver v. United States, 466 U.S. 170, 180 n.11 (1984).

110 *Id.* at 179.

111 United States v. Knotts, 460 U.S. 276 (1983).

112 United States v. Karo, 468 U.S. 705 (1984).

113 *Karo*, 468 U.S. at 709–10; *Knotts*, 460 U.S. at 277, 281.

114 *Knotts*, 460 U.S. at 277, 281.

115 *Id.* at 285.

116 *Karo*, 468 U.S. at 709–10.

117 *Id.* at 714–15.

B. *Limitations on "Searches" Conducted Using Developing Technologies*

UAS technology represents a significant expansion of the government's surveillance capabilities.[118] To predict how UAS surveillance will fare under the Fourth Amendment, it is useful to look at how the Court has responded to increasingly sophisticated methods of governmental surveillance in the past.[119]

The Court has struggled to apply the Fourth Amendment to technological advances, cautioning that they may push up against or exceed the Amendment's outer bounds.[120] Justice Alito's concurrence in *Jones* most recently explored these difficulties: "[T]he *Katz* test rests on the assumption that this hypothetical reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations."[121] The Court's resolution of this issue with manned aerial surveillance and sense-enhancing technology, considered below, provides some insight into how UAS technology will fare under the Fourth Amendment.

1. *Manned Aerial Surveillance*

Constitutional limits imposed on manned aerial surveillance will inform the limits to be imposed on *unmanned* aerial surveillance. On three occasions, the Supreme Court has considered whether manned aerial surveillance constitutes a search in violation of the Fourth Amendment.[122] The Court concluded each time that no search occurred.

Both *California v. Ciraolo*[123] and *Florida v. Riley*[124] concerned police officers' naked-eye observations of marijuana growing in the cur-

---

118 *See supra* Part I.B.

119 The cases described in Part II.B occurred between the *Katz* and *Jones* decisions, discussed in Part II.A, *supra*. They were decided under the *Katz* test and largely without reference to the trespassory concerns emphasized in *Jones*. Because these cases do not turn on physical trespass, however, *Jones* does not affect their holdings.

120 *See, e.g.*, Kyllo v. United States, 533 U.S. 27, 34 (2001) ("The question we confront today is what limits there are upon this power of technology to shrink the realm of guaranteed privacy.").

121 United States v. Jones, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring). Specifically, Justice Alito noted the likelihood that people confronted with developing technology will find the tradeoff between convenience and privacy justified, or, if not justified, inevitable. *Id.*

122 Florida v. Riley, 488 U.S. 445 (1989); Dow Chem. Co. v. United States, 476 U.S. 227 (1986); California v. Ciraolo, 476 U.S. 207 (1986).

123 California v. Ciraolo, 476 U.S. 207 (1986).

124 Florida v. Riley, 488 U.S. 445 (1989).

tilage of respondents' homes.[125] Both respondents satisfied the first prong of the *Katz* test by manifesting a subjective expectation of privacy.[126] However, in both cases, the second prong of *Katz* proved fatal. In an age where overhead flight is common, "[a]ny member of the public flying in this airspace who glanced down could have seen everything that these officers observed."[127] Consequently, neither case involved an unreasonable search in violation of the Fourth Amendment.[128]

Worth noting is a point of contention in *Riley* between the majority opinion and Justice O'Connor's concurring opinion. The majority noted that its search analysis might have been different had the officers flown their helicopter where it had no legal right to be.[129] In her concurrence, Justice O'Connor criticized the majority's reliance on compliance with FAA regulation.[130] Instead, she emphasized whether the flight was sufficiently rare or routine.[131]

In the third aerial surveillance case, *Dow Chemical Co. v. United States*,[132] Environmental Protection Agency agents photographed an outdoor industrial complex from an aircraft flying at altitudes ranging between 1200 and 12,000 feet.[133] This case differs from *Ciraolo* and *Riley* in two major respects. First, the alleged search was of an industrial rather than residential area.[134] The Court noted that when inspecting commercial property, agents have greater latitude because of the lower privacy expectations.[135] Second, the agents photographed their observations with a precision aerial mapping camera.[136] The

---

125 *Riley*, 488 U.S. at 449 (officers observing marijuana growing in a greenhouse within the respondent's backyard, through a gap in the greenhouse roof, from a helicopter); *Ciraolo*, 476 U.S. at 210 (officers observing marijuana growing within the respondent's backyard from a fixed-wing airplane).

126 Riley, 488 U.S. at 448 (respondent enclosed two sides of the greenhouse, obscured the other two, and partially covered the top with roofing panels); *Ciraolo*, 476 U.S. at 209 (respondent erected a ten-foot fence around his backyard).

127 *Ciraolo*, 476 U.S. at 213–14; *see also Riley*, 488 U.S. at 451 ("Any member of the public could legally have been flying over Riley's property in a helicopter at an altitude of 400 feet and could have observed Riley's greenhouse.").

128 *See Riley*, 488 U.S. at 452; *Ciraolo*, 476 U.S. at 214–15.

129 *Riley*, 488 U.S. at 451.

130 *Id.* at 452 (O'Connor, J., concurring).

131 *Id.* at 453.

132 Dow Chem. Co. v. United States, 476 U.S. 227 (1986).

133 *Id.* at 229.

134 *See id.*

135 *Id.* at 237–38 (quoting Donovan v. Dewey, 452 U.S. 594, 598–99 (1981)).

136 *Id.* at 231 (explaining that the photographs taken were like those used in mapmaking and could be replicated by "[a]ny person with an airplane and an aerial camera").

Court recognized that there might be cases in which surveillance of private property by highly sophisticated equipment constitutes an unreasonable search, but found that the photography here did not rise to the level of a constitutional violation.[137] Again, the Court found no Fourth Amendment violation.[138]

In each aerial surveillance case, the Court considered the area searched, the nature and altitude of the flight, and the surveillance equipment used. It remains unclear whether, as raised in *Riley*, the question of the nature and altitude of the flight should be informed by compliance with FAA regulations or the rarity of air traffic in a given area.[139] This analysis will be further complicated by the inevitable use of sophisticated sense-enhancing technology on UASs.

2. Sense-Enhancing Technology

A defining characteristic of UASs is the necessity of attaching a sense-enhancing payload to obtain information.[140] Although ordinary visual surveillance has long been permissible under the Fourth Amendment,[141] and apparently remains so when visual observations are captured with relatively unsophisticated photography,[142] the Court has recognized that other sense-enhancing technology may be different.

Most notably, in *Kyllo v. United States*,[143] a police officer on a public street aimed a thermal imaging device[144] at a private residence to detect relative amounts of heat within.[145] The officer saw, in shades of gray depicting varying degrees of warmth, that areas of the petitioner's garage were substantially warmer than the rest of the home.[146] He concluded from this information that the petitioner was using halide lights to grow marijuana in his home.[147]

---

137 *Id.* at 238.

138 *Id.* at 239.

139 *See supra* notes 129–32 and accompanying text.

140 *See supra* Part I.B.2.

141 Kyllo v. United States, 533 U.S. 27, 31–32 (2001) ("[T]he lawfulness of warrantless visual surveillance of a home has still been preserved.").

142 *Dow Chem. Co.*, 476 U.S. at 238. The agents' photography in that case enhanced human vision but did not reveal intimate details, and was of a commercial rather than a residential area. *Id.*

143 Kyllo v. United States, 533 U.S. 27 (2001).

144 Thermal imagers detect infrared radiation, emitted by virtually all objects, and convert the radiation into images based on relative warmth. *Id.* at 29.

145 *Id.*

146 *Id.* at 30.

147 *Id.*

The government argued that there was a difference between "off-the-wall" and "through-the-wall" observations.[148] Taking up this argument, the dissent in *Kyllo* compared a thermal imager that captures heat emanating from a house with a microphone that picks up sound or a satellite that picks up light.[149] The Court rejected this contention, holding that when the government uses a sense-enhancing device that is not in general public use to access intimate details within a private home, otherwise undiscoverable without physical trespass, an unreasonable search occurs.[150]

Kyllo reaffirms the sentiment expressed in *Dow Chemical Co.* that sense-enhancing technology not in general public use can offend the Fourth Amendment. While *Dow Chemical Co.* raised the idea hypothetically,[151] *Kyllo* addressed the question specifically and established a bright line that sense-enhancing technology may not cross.

As evidenced by the manned aerial surveillance and sense-enhancing technology cases, unresolved questions remain when the Fourth Amendment is applied to an alleged technological search. These questions will result in similar uncertainties when courts address the constitutionality of UAS surveillance.

III. Applying the Fourth Amendment to UAS Surveillance Yields Uncertain & Insufficient Limitations

Government UAS surveillance missions, whether conducted by federal, state, or local law enforcement agencies, implicate the Fourth Amendment.[152] As Justice Alito's concurrence in *Jones* counsels, when new technology lacks practical or statutory limits, "[t]he best that [the Court] can do . . . is to apply existing Fourth Amendment doctrine."[153] Accordingly, UAS missions will be subject to both the trespassory test, as revived in *Jones*, and *Katz*'s reasonable expecta-

148 *Id.* at 35.

149 *Id.*

150 *Id.* at 40.

151 Dow Chem. Co. v. United States, 476 U.S. 227, 238 (1986) (suggesting that this line *might* be reached by some sophisticated technology such as satellite technology).

152 *See, e.g.*, Travis Dunlap, Comment, *We've Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search*, 51 S. Tex. L. Rev. 173, 204 (2009) (concluding that under existing jurisprudence, warrantless UAS surveillance would not likely be an unconstitutional search under all circumstances); Paul McBride, Comment, *Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations*, 74 J. Air L. & Com. 627, 661–662 (2009) (concluding that under existing jurisprudence, warrantless UAS surveillance of the curtilage of the home is an unconstitutional search within the meaning of the Fourth Amendment but conceding that this prediction is speculative).

153 United States v. Jones, 132 S. Ct. 945, 964 (2012) (Alito, J., concurring).

tion of privacy test.[154] A warrantless mission would be an unreasonable search if a UAS either trespassed onto private property, or in the more likely case, violated an individual's reasonable expectation of privacy.[155] Whether a warrantless UAS mission violates the *Katz* test will likely depend on several contextual factors, most importantly the location and behavior of the aircraft and the image-capturing or sense-enhancing technology used.[156]

Questions about UAS location and flight behavior are best informed by the aerial surveillance cases.[157] It is reasonable to predict that UAS surveillance revealing the intimate details of the interior of a home will be considered an unreasonable search, but that UAS surveillance revealing that which is visible to the naked eye in public places will not constitute an unreasonable search. The most difficult cases will likely involve the curtilage. UAS surveillance may force courts to confront the tension raised in *Riley*: whether the reasonableness of a search depends on compliance with FAA regulations or the frequency of similar aircraft activity.[158] FAA rules would inform the former; the popularity of civil and public UAS flights, and the public's reception thereof,[159] would inform the latter.

---

154 See *supra* Part II.A.1.

155 It seems likely that the *Katz* test will prove more relevant to UASs than the trespassory test. Particularly with micro-UASs, however, the trespassory test may find application. For example, a demonstration of the AeroVironment Nano Hummingbird, *see supra* note 56, shows the bird-like aircraft flying through an open door into a building, and transmitting a video feed of the building's interior. *See* theworacle, *AeroVironment/DARPA Nano Hummingbird UAV Flying*, YOUTUBE (Feb. 17, 2011), http://www.youtube.com/watch?v=a8ZbtZqH6Io. Governmental use of a UAS in this manner would presumably violate the trespassory test, as well as the *Katz* test.

156 *See* THOMPSON, *supra* note 19, at 12. Additionally, the Congressional Research Service predicts that reviewing courts may find it helpful to consider cases regarding privacy in the home, privacy in public spaces, location tracking, and the national border. *See* THOMPSON, *supra* note 19, at 5.

157 See *supra* Part II.B.1.

158 Florida v. Riley, 488 U.S. 445, 455 (1989).

159 Public acceptance is extremely hard to predict at this point. In 2008, the Government Accountability Office ("GAO") explained:

> Because UASs have never routinely operated in the national airspace system, the level of public acceptance is unknown. One researcher observed that as UASs expand into the non-defense sector, there will inevitably be public debate over the need for and motives behind such proliferation. One expert we surveyed commented that some individuals may raise privacy concerns about a small aircraft that is "spying" on them, whether operated by law enforcement officials or by private organizations . . . . On the other hand, a study . . . noted that if UASs were increasingly used to produce public benefits in large-scale emergency response efforts, public acceptance could grow as the public notes the benefits that UASs can provide.

The sense-enhancing technology cases discussed above will likely inform courts analyzing the Fourth Amendment implications of government use of various UAS payloads.[160] Drawing from the factors weighed in *Dow Chemical Co.* and *Kyllo*, courts will likely consider the relative sophistication of the payload, the technology's acceptance by or availability to the public, and the area searched.

As one commentator frames the issue, "[t]he crucial question, then, is whether [UASs] have the potential to be significantly more invasive than traditional surveillance technologies . . . that have been upheld in previous cases."[161] The "sheer sophistication" of UASs, however, makes it difficult, if not impossible, to apply the existing Fourth Amendment framework.[162] Many of the practical boundaries of manned aircrafts—flight altitude, duration, and location—informed existing case law. These boundaries are eroded in UAS operations. As such, it is easy to predict situations in which UASs will push against and exceed Fourth Amendment safeguards.[163] Ultimately, any limitations that courts will impose on UAS technology under the Fourth Amendment cannot be predicted with sufficient confidence or timeliness to give UAS manufacturers and government users meaningful guidance on the issue.

IV. Proposal for a Mandatory Interagency MOU Between Federal UAS Stakeholders

As smaller, cheaper, and smarter public UASs assimilate into the domestic airspace,[164] the threat to citizens' privacy interests grows stronger. Yet, UAS privacy issues remain unresolved. This Note proposes that Congress revise the FAA Modernization and Reform Act of 2012 to mandate coordination between the FAA and other major stakeholders in UAS privacy issues, identified below.[165] Congress should amend the Act to require these agencies to generate an MOU:

Federal Actions Needed to Ensure Safety, *supra* note 16, at 24. Both trends identified by the GAO still appear relevant. *See* Inst. for Homeland Sec. Solutions, *supra* note 25, at 3 (reporting high levels of public support for UAS use in homeland security, fighting crime, and search and rescue, but also high levels of public concern with UAS monitoring outside homes and in public).

160 See *supra* Part II.B.2.

161 Thompson, *supra* note 19, at 15.

162 *Id.* at 21.

163 Measuring Progress, *supra* note 26, at 36. The *Jones* decision buttresses this point—the difficulties of applying the *Katz* test to GPS technology seem to have informed the Court's application of the trespassory test instead.

164 *See supra* Part I.

165 *See infra* Part IV.A.

(1) outlining each agency's interest, (2) recommending guidelines for acceptable UAS use, and (3) establishing a timeline for revision of the MOU and guidelines. Additionally, the Act should mandate that the FAA consider the MOU and apply its guidelines in the Agency's COA approval process.

A. The Insufficiency of the Status Quo

The proposed statutory amendment is necessary because neither existing case law nor the current statutory regime places adequate limitations on domestic UAS surveillance by law enforcement. Courts have not yet applied the Fourth Amendment to UAS surveillance,[166] and when they do, the degree to which UAS use will be circumscribed is difficult to predict.[167] Moreover, even if the courts that ultimately confront this issue do provide meaningful protections from UAS abuse, those protections will come too late, after UASs have become more prevalent. UAS stakeholders agree that developing usage guidelines before UASs become more popular may prevent abuses by law enforcement and a negative public perception of UASs.[168] Waiting for courts to speak on the issue opens the door for such abuses to occur in the meantime.

Legislative guidance is also lacking. As Justice Alito suggested in *Jones*, legislative or regulatory action may better safeguard privacy interests from new technology than courts of law.[169] Legislatures can respond to public attitudes, draw appropriately detailed lines, and balance comprehensive public interests.[170] Congress has not yet spoken

---

166 Excluding the North Dakota Nelson County District Court apparently, although the UAS there was not used for surveillance preceding an arrest and Brossart advanced no meaningful Fourth Amendment argument. *See supra* notes 1–13 and accompanying text.

167 *See supra* Part III.

168 *See* DILLINGHAM, *supra* note 73, at 11. In July 2012, Congressman Ted Poe echoed the need for regulation before full integration when he introduced House Bill 6199: "Now is the time for Congress to act, not in 2015. . . . Congress has to be proactive in controlling drone use to law enforcement . . . ." 158 CONG. REC. H5133 (daily ed. Jul. 24, 2012) (statement of Rep. Poe).

169 United States v. Jones, 132 S. Ct. 945, 962–64 (2012) (Alito, J., concurring).

170 *Id.* In the past, Congress has provided greater regulation over government surveillance with respect to wiretapping, e-mails, bank records, and health records. THOMPSON, *supra* note 19, at 18. For example, the Right to Financial Privacy Act, 12 U.S.C. §§ 3401–3422 (2012), was passed in response to the Court's decision in *United States v. Miller*, 425 U.S. 435, 443 (1976) (holding that the defendant had no reasonable expectations of privacy in his bank records because he had disclosed them to a third party, the bank), creating a statutory protection for such records. *See also* THOMPSON, *supra* note 19, at 2 n.9. Similarly, Congress passed the Omnibus Crime Control and Safe Streets Act of 1968, 18 U.S.C. §§ 2510–2522 (2006), to regulate wiretapping after the issue was raised in the courts by *Katz*, and wiretapping has since been governed by statute rather than caselaw. *See Jones*, 132 S. Ct. at 962–64 (Alito, J., concurring). But see *infra*

directly on UAS privacy issues. Under the current statutory regime, the FAA apparently has the greatest authority over UASs due to its general responsibility to regulate the national airspace, and its specific charge to facilitate the safe integration of UASs into the airspace under the FAA Modernization and Reform Act of 2012.[171] Some UAS stakeholders have already urged the FAA to incorporate privacy concerns into its UAS rulemaking procedures.[172] FAA officials have rejected the call to address privacy, explaining that it is outside the FAA's mission of aviation safety.[173] Despite the FAA's earlier protest, however, in November 2013, the agency released Final Privacy Requirements for its six UAS test sites.[174] Rather than prescribing substantive privacy policies for test site operators, the requirements mandate that operators develop their own privacy and data retention policies and comply with applicable privacy law.[175]

Commentators disagree on the implications of this move by the FAA. Professor Ryan Calo called the plan "sensible," explaining that it contains "subtle signals" that the FAA is beginning to consider privacy concerns.[176] Others are less optimistic. For example, Senator Edward Markey described the FAA plan as demonstrating a "disregard for the need for strong and comprehensive privacy safeguards."[177] Whatever subtle signals this plan conveys, the FAA sent an unambiguous message that its "mission is to provide the safest, most efficient aerospace system in the world and does not include regulating privacy."[178]

Part V for a discussion of why the UAS legislation proposed thus far provides an inadequate solution to the problem.

171 *See* DILLINGHAM, *supra* note 73, at 10–11.

172 *Id.* at 11.

173 *Id.*

174 Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 68,360, 68,364 (Nov. 14, 2013).

175 *Id.*

176 Ryan Calo, *The FAA's Drone Privacy Plan: Actually Pretty Sensible*, FORBES (Nov. 9, 2013, 6:38 PM), http://www.forbes.com/sites/ryancalo/2013/11/09/the-faas-drone-privacy-plan-actually-pretty-sensible/.

177 Keith Laing, *Markey: FAA Drone Plan 'Falls Far Short*,' HILL (Nov. 7, 2013, 3:11 PM), http://thehill.com/blogs/transportation-report/aviation/189603-markey-faa-drone-plan-falls-far-short (internal quotation marks omitted).

178 Unmanned Aircraft System Test Site Program, 78 Fed. Reg. at 68,361.

B. *Identifying Federal Agencies Implicated by the UAS Privacy Threat*

Currently, though the FAA stands at the forefront of UAS integration,[179] Congress has not directed a single agency to regulate UAS privacy matters.[180] Indeed, a number of other federal entity stakeholders are invested in UAS integration and may be qualified to contribute to the resolution of related privacy issues.[181]

The Department of Defense ("DOD") provides the FAA with UAS operational and safety data, and is a UAS user itself.[182] The National Aeronautics and Space Administration ("NASA") provides research and development and testing on UAS integration efforts.[183] Within the Department of Homeland Security ("DHS"), both the Transportation Security Administration ("TSA") and Customs and Border Patrol ("CBP") are implicated.[184] The Government Accountability Office ("GAO") has recommended that TSA examine the security implications of nonmilitary UAS operations, pursuant to TSA's authority to regulate the security of all transportation modes and establish relevant safeguards.[185] CBP provides flight demonstrations to the FAA and also uses UASs for border patrol and security.[186] Moreover, DHS established a working group to examine the privacy and civil liberties policy and legal issues implicated by governmental UAS use, and to support and improve DHS and DHS-funded UAS missions.[187]

Additionally, the Department of Justice ("DOJ") is partially responsible for addressing the technological needs of state, local, and tribal law enforcement agencies—including UASs.[188] DOJ's National Institute of Justice ("NIJ") has evaluated small UASs in the context of

---

179 *See supra* Part I.A.

180 MEASURING PROGRESS, *supra* note 26, at 35.

181 *Id.* at 11–12; *see also* DILLINGHAM, *supra* note 73, at 2.

182 MEASURING PROGRESS, *supra* note 26, at 12 tbl.1.

183 *Id.*

184 *Id.* at 11–12.

185 *Id.*

186 *Id. See also generally Unmanned Aerial Vehicles Support Border Security*, CUSTOMS & BORDER PROTECTION TODAY, July–Aug. 2004, at 8, *available at* http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml.

187 Memorandum from the Office for Civil Rights and Civil Liberties to the Secretary of the Department of Homeland Security (Sept. 14, 2012), *available at* http://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-s1-information-memorandum-09142012.pdf.

188 MEASURING PROGRESS, *supra* note 26, at 11–12.

police operations.[189] NIJ released a technical bulletin in 2007 advising law enforcement agencies on the COA approval process and the FAA's UAS position at the time.[190] The bulletin additionally stated that the NIJ's Aviation Technology Program would provide a forum for law enforcement agencies' opinions regarding UAS use.[191]

Interagency efforts are not foreign to UAS regulation.[192] Several interagency groups comprised of these and other agencies already exist, aimed at resolving particular UAS issues.[193] For example, the FAA's JPDO consists of representatives from the DOD, DHS, NASA, and FAA, as well as the Department of Commerce, National Oceanic and Atmospheric Administration, White House Office of Science and Technology Policy, and Office of the Director of National Intelligence.[194] One of the JPDO's goals is to fully integrate UASs into the Next Generation Air Transportation System ("NextGen").[195] NextGen is an initiative that leverages existing and new technologies to enhance the safety, speed, efficiency, and demand levels of air transportation.[196] The JPDO authored the September 2013 *Unmanned Aircraft Systems Comprehensive Plan*, setting the interagency goals, objectives, and approach to UAS integration.[197] The plan is a self-described "testament to the collaboration among representatives from the partner agencies and the UAS community."[198] The goals and objectives do not include privacy considerations, though the *Comprehensive Plan* notes that the partner agencies agree on the need to address privacy and civil liberties issues in the future.[199]

Similarly, the National Defense Authorization Act for Fiscal Year 2010[200] formed the UAS Executive Committee ("UAS ExCom"). Se-

---

189 *Types of Aircraft*, *supra* note 52.

190 NAT'L INST. OF JUSTICE, U.S. DEP'T OF JUSTICE, TECHNICAL BULLETIN: LAW ENFORCEMENT USE OF UAS 10/10/2007, at 1–2 (2007), *available at* https://www.justnet.org/pdf/UAS-Technical-Bulletin101007.pdf.

191 *Id.* at 2.

192 *See* MEASURING PROGRESS, *supra* note 26, at 11–12.

193 *See id.*

194 *About Us*, JOINT PLAN. & DEV. OFFICE, http://www.jpdo.gov/About_us.asp (last visited Dec. 27, 2013); *Who's Who*, JOINT PLAN. & DEV. OFFICE, http://www.jpdo.gov/whoswho.asp (last visited Dec. 27, 2013).

195 *About Us*, *supra* note 194; *NextGen Topics*, JOINT PLAN. & DEV. OFFICE, http://www.jpdo.gov/nextgen_topics.asp (last visited Dec. 27, 2013).

196 *About Us*, *supra* note 194.

197 COMPREHENSIVE PLAN, supra note 44.

198 *Id.*

199 *Id.* at 7.

200 National Defense Authorization Act for Fiscal Year 2010, Pub. L. No. 111-84, § 935, 123 Stat. 2436–37.

nior executives from federal agencies including FAA, DOD, NASA, and DHS comprise the UAS ExCom.[201] This group is responsible for discussing and identifying solutions to certain DOD UAS integration problems.[202] Congress charged the UAS ExCom with developing a joint plan for increased DOD UAS access to the national airspace.[203] The UAS ExCom plan must describe communication efforts between the Department of Transportation and DOD; specific milestones; and recommended policies for use of the national airspace, flight standards, and operating procedures.[204] The statute additionally requires that the Secretary of Defense and Secretary of Transportation submit a report containing the plan to certain congressional committees.[205]

Though there is some disagreement about the scope of the various stakeholders' jurisdiction over UAS privacy issues, the GAO has suggested on multiple occasions that one, if not all, of the major stakeholders have jurisdiction to act, but that the agencies' related interests have kept them from taking action.[206] Specifically, the GAO suggests that the FAA, DHS, and DOJ may be particularly suitable to confront UAS privacy concerns.[207] The threat posed by UASs to privacy interests can be better resolved by tapping into the respective expertise and interests of these stakeholders.

C. The Need for Interagency Coordination to Close the UAS Privacy Gap

The aforementioned agencies have related but fragmented interests in UAS privacy issues. Commentators disagree about what, if any, single agency is best situated to take on the UAS privacy issue.[208] No agency has taken proactive steps regarding an overarching privacy policy because they do not believe themselves to have direct authority.[209] Situations in which multiple agencies have overlapping interests in the same issue, as is the case here, often result in redundancy, ineffi-

---

201 MEASURING PROGRESS, *supra* note 26, at 12 tbl.1.

202 *Id.*

203 National Defense Authorization Act for Fiscal Year 2010 § 935.

204 *Id.* § 935(b)(1)–(3).

205 *Id.* § 935(c).

206 *See* MEASURING PROGRESS, *supra* note 26, at 38.

207 *Id.* at 36.

208 *Id.* at 35.

209 *Id.* at 38. The FAA stated that its authority to include the Final Privacy Requirements in agreements with UAS test site operators comes from 49 U.S.C. § 106(*l*)(6), authorizing the Administrator to enter such agreements "on terms and conditions as the Administrator may consider appropriate." 49 U.S.C. § 106(*l*)(6) (2006); Unmanned Aircraft System Test Site Program, 78 Fed. Reg. 68,360, 68,361 (Nov. 14, 2013). The FAA's Final Privacy Requirements for

ciency, and gaps in policy.[210] Required interagency coordination could close the gap currently surrounding the UAS privacy issue and resolve confusion over which agencies have authority to act.

Interagency coordination provides a solution. Interagency coordination is "an arrangement in which a lead agency or officer directs an operation, project, or program among one or more other agencies."[211] Rationales supporting interagency efforts abound and include: (1) reduction in policy fragmentation, (2) increased effectiveness in policy formulation and implementation, (3) increased awareness among agencies of different perspectives, (4) increased efficiency and reduced redundancy, and (5) increased awareness in cross-cutting programs and priorities.[212]

Interagency coordination can be effectively used to resolve the UAS privacy threat through a congressionally mandated MOU that brings major stakeholders together. MOUs are a common form of interagency coordination.[213] Agencies frequently enter into them voluntarily, but as in this Note's proposal, Congress may also require their adoption.[214] An MOU typically "assigns responsibility for specific tasks, establishes procedures, and binds the agencies to fulfill mutual commitments."[215] MOUs commonly delineate jurisdictional lines and call for information sharing.[216] They are "highly valuable because of their relative informality, ease of enactment, and adaptability."[217] They can be used to simplify multiagency processes, reducing transac-

---

UAS test sites are only applicable to those sites and do not create an overarching policy. *See* COMPREHENSIVE PLAN, *supra* note 44, at 4.

210 JODY FREEMAN & JIM ROSSI, IMPROVING COORDINATION OF RELATED AGENCY RESPONSIBILITIES 4 (2012), *available at* http://www.acus.gov/wp-content/uploads/downloads/2012/06/Freeman-Rossi-ACUS-Report-5-30-12-PDF.pdf.

211 FREDERICK M. KAISER, CONG. RESEARCH SERV., R41803, INTERAGENCY COLLABORATIVE ARRANGEMENTS AND ACTIVITIES: TYPES, RATIONALES, CONSIDERATIONS 3 (2011). Contrast coordination with the distinct interagency arrangement of collaboration. Collaboration is "an arrangement which relies, to a substantial degree, on voluntary or discretionary participation among the members, who are relatively equal or at least have parity in such an activity and arrangement." *Id.*

212 *Id.* at 16–18. Though the aforementioned rationales are those primarily implicated by the interagency coordination proposed by this Note, other rationales for interagency coordination in general include the following: mitigating conflict among agencies; changing organizational cultures within agencies; changing bureaucratic and administrative cultures; and streamlining and improving congressional and executive oversight. *Id.*

213 FREEMAN & ROSSI, *supra* note 210, at 25.

214 *Id.* Presumably, the President could require them among executive agencies as well. *Id.*

215 *Id.* at 25.

216 *Id.* at 26.

217 *Id.* at 58.

tion costs and improving the expertise on which agency decisions are made.[218]

Although MOUs can be highly effective, they are not legally enforceable, may be frustrated by uncooperative participating agencies, and are not collected on any single interagency database.[219] These problems can be counteracted to a degree. Member agencies can be made more accountable when the MOU is congressionally required rather than voluntary, and when its contents are available to the public.[220] MOUs can be published in the *Federal Register* and on agency websites, and may be subject to a Freedom of Information Act[221] request.[222] This Note's proposal includes both of these safeguards to increase agency accountability.

The proposed amendment and resulting MOU would fall squarely within the definition of interagency collaboration—the FAA would retain its status as the lead agency, with the authority to direct an interagency program and responsibility to generate interagency accountability. As explained below, this proposal takes advantage of many benefits of interagency coordination while avoiding the potential concerns.

D. Proposed Amendment to the FAA Modernization and Reform Act of 2012

To address the UAS privacy gap, Congress should amend the FAA Modernization and Reform Act of 2012 to require creation of an MOU addressing the privacy issues implicated by rapid UAS integration in the national airspace system. The proposed amendment requires participation of three primary stakeholders—the FAA, DOJ, and DHS—and permits their discretionary consultation with other interested agencies.[223] The FAA is well versed as the primary actor in UAS integration already. Of the remaining interested agencies, the DOJ has the closest connection to the crux of the issue: the use of UASs by law enforcement.[224] DHS has demonstrated a vested interest

---

218 *Id.* at 29.

219 *Id.* at 26, 29–30.

220 *See id.* at 25–26.

221 Freedom of Information Act ("FOIA"), 5 U.S.C. § 552 (2012).

222 FREEMAN & ROSSI, *supra* note 210, at 26 n.114

223 For example, the DOD or NASA, as mentioned in Part IV.B, *supra*. House Bill 2868, H.R. 2868, 113th Cong. (2013), described in Part V.B, *infra*, would also involve the Department of Commerce and Federal Trade Commission in this issue.

224 *See supra* notes 188–91 and accompanying text.

in and developing expertise regarding the privacy implications of government UAS operations.[225]

Interagency coordination preserves the current lead status of the FAA while bringing in additional interested agencies to offer their expertise on the issue. A congressionally mandated MOU provides an appropriate vehicle to accomplish this goal: it is flexible enough to respond to the constantly evolving status of UASs and can be structured to create accountability among involved agencies.

Substantively, the mandated MOU should clarify jurisdictional lines among agencies, require interagency communication, and recommend substantive guidelines for permissible UAS operations. Further, the amendment should call for the MOU's timely revision, defined to reflect the FAA's timeline for integration. Stakeholders agree that developing guidelines for permissible UAS uses ahead of their widespread adoption may preclude abuse.[226] This proposal ensures that privacy constraints develop in step with the problem itself by evolving in response to the FAA's already established integration timeline.[227] Finally, to further promote the accountability of member agencies under this amendment, the agencies should publish the MOU and submit a report of the resulting plan to relevant congressional committees for consideration.

This Note proposes that the following language[228] be added to subtitle B of title II of the FAA Modernization and Reform Act of 2012,[229] comprising new section 337 of the Act:

> (a) In this subsection, "member agencies" shall include the Federal Aviation Administration, Department of Justice, Department of Homeland Security, and any such additional agencies that are consulted as permitted by subsection (c).
>
> (b) The Federal Aviation Administration shall act as the lead agency for purposes of coordinating efforts under this section.

---

225 *See supra* note 187 and accompanying text.

226 DILLINGHAM, *supra* note 73, at 11; MEASURING PROGRESS, *supra* note 26, at 36.

227 *See supra* Part I.A.

228 The following proposed language is based in part on the National Defense Authorization Act for Fiscal Year 2010, Pub. L. No. 111-84, § 935, 123 Stat. 2436, and in part on the Energy Policy Act of 2005 § 1221(a), 16 U.S.C. § 824p(h) (2012) (requiring the Department of Energy to act as the lead agency in coordination efforts with other agencies); *see also* FREEMAN & ROSSI, *supra* note 210, at 28 (describing the MOU resulting from the congressionally mandated coordination under the Energy Policy Act).

229 FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, 126 Stat. 13.

(c) To the maximum extent practicable under applicable federal law, the Secretary of Transportation and the Attorney General, after consultation with other federal agencies as they determine is necessary, shall coordinate a plan for addressing citizens' privacy rights implicated by the integration of unmanned aircraft systems into the national airspace system.

(d) The plan shall be described in a Memorandum of Understanding, to be made publicly available by at least one member agency named in subsection (a).

(e) The plan required by subsection (c) shall include the following:

(1) A description of how the member agencies will communicate and cooperate to address citizens' privacy rights implicated by the integration of unmanned aircraft systems into the national airspace system, and member agencies' respective jurisdictional bases for such action.

(2) Specific milestones, taking into account the needs of the Federal Aviation Administration for safe integration of UASs into the national airspace system, for addressing citizens' privacy rights that are implicated by such integration. Such milestones shall include a timeline for future revision of the plan required by subsection (c).

(3) Recommendations for policies with respect to acceptable unmanned aircraft system operations and missions, and data collection practices or other surveillance payload use that should be implemented by the member agencies.

(4) An identification of resources required by the member agencies to execute the plan.

(f) Not later than 180 days after the date of the enactment of this Act, the Secretary of Transportation, Attorney General, and Secretary of Homeland Security shall submit a report containing the plan required by subsection (c) to the following committees:

(1) The Committee on Commerce, Science, and Transportation of the Senate and the Committee on Transportation and Infrastructure of the House of Representatives.

(2) The Committee on the Judiciary of the Senate and the Committee on the Judiciary of the House of Representatives.

> (3) The Committee on Homeland Security and Governmental Affairs of the Senate and the Committee on Homeland Security of the House of Representatives.

Additionally, Congress should amend section 334 of the FAA Modernization and Reform Act, dealing with public use of UASs,[230] to require that the FAA consider the resulting MOU guidelines in its COA approval process. The COA process is the current mechanism by which the FAA approves public UAS missions.[231] The FAA already requires applicants to describe the intended mission and proposed UAS behavior.[232] As such, the FAA stands in the best position to provide added scrutiny on the basis of potential privacy threats.

The proposed amendment creates interagency communication and accountability to close the current gap surrounding privacy issues in UAS integration. Unlike more rigid legislative solutions, the informal nature of MOUs should permit the member agencies to communicate amongst themselves in a cost-effective manner while retaining the ability to respond to the still-changing status of UAS integration. The amendment will additionally clarify the responsibilities of involved agencies and hold them accountable for their participation, correcting the apparent reluctance of agencies to act under the current regime.

V. Legislative and Single-Agency Counterproposals Are Insufficient

Commentators and legislators have proposed state legislation, federal legislation, and single-agency regulation to constrain governmental UAS use, considered in turn below. When contrasted with the amendment proposed in Part IV.D, these solutions ultimately prove inadequate to resolve this complex problem.

A. State Legislation

States have taken up the UAS issue with apparent enthusiasm in the past year. A state-level solution, however, will not be comprehensive enough to resolve the UAS privacy threat in its entirety. As of October 2013, forty-two states had proposed UAS legislation, eight of which actually enacted such legislation.[233] Most proposed state legislation would require a probable cause warrant before permitting law

230 *Id.* § 334, 126 Stat. at 76–77.

231 *See supra* notes 38–42 and accompanying text.

232 *See supra* note 39 and accompanying text.

233 Allie Bohm, *Status of Domestic Drone Legislation in the States*, ACLU, http://www.aclu

enforcement to collect information about someone for use in court.[234] The ACLU described bills in Massachusetts[235] and Rhode Island[236] as leaders in privacy protection, proposing that law enforcement surveil only the target identified by the warrant and barring use of incidentally acquired data in court.[237] Conversely, the ACLU described bills in North Dakota[238] and Arizona[239] as "tak[ing] the low road" with privacy.[240] North Dakota would permit incidentally collected information to be used in court.[241] Arizona's bill would cover United States citizens only and would exempt drug crimes and human smuggling from its warrant requirement.[242]

There are some benefits to a state-level response. First, state legislation can respond to local needs and circumstances. The distinct provisions of the Arizona bill, for example, are likely in response to its proximity to the border. CBP UASs help monitor and protect the United States borders, specifically targeting potential terrorists and illegal cross-border activity.[243] The exceptions built into the Arizona bill seem to reflect UAS activity already in place. Second, as law Professor Ryan Calo stated at a Senate Judiciary Committee hearing on this topic, "[t]here is some benefit of the fact that the states are laboratories of ideas. . . . [Y]ou have some states which say 'look, anything goes here,' and other states that go 'nothing goes here,' and maybe we will learn from that experience."[244] Varying state laws may provide

---

.org/blog/technology-and-liberty/status-domestic-drone-legislation-states (last updated Dec. 17, 2013).

234 Allie Bohm, *Drone Legislation: What's Being Proposed in the States?*, ACLU (Mar. 6, 2013, 3:15 PM), http://www.aclu.org/blog/technology-and-liberty-national-security/drone-legislation-whats-being-proposed-states [hereinafter Bohm, *Drone Legislation*].

235 S. 1664, 188th Leg., Reg. Sess. (Mass. 2013).

236 H. 5780, Gen. Assemb., Jan. Sess. (R.I. 2013).

237 Mass. S. 1664; R.I. H. 5780; Bohm, *Drone Legislation*, *supra* note 234.

238 H.R. 1373, 63rd Legis. Assemb. (N.D. 2013). North Dakota's bill was apparently introduced in response to Rodney Brossart's controversial UAS-assisted arrest. James MacPherson, *North Dakota Bill Sets Rules for Law Enforcement Drone Use*, BISMARK TRIB., Jan. 28, 2013, http://bismarcktribune.com/news/local/govt-and-politics/north-dakota-bill-sets-rules-for-law-enforcement-drone-use/article_bbcad63a-698e-11e2-9e9c-001a4bcf887a.html.

239 H. B. 2574, 51st Leg., 1st Reg. Sess. (Ariz. 2013).

240 Bohm, *Drone Legislation*, *supra* note 234.

241 H.R. 1373, 63rd Legis. Assemb. (N.D. 2013); Bohm, *Drone Legislation*, *supra* note 234.

242 Ariz. H. B. 2574; Bohm, *Drone Legislation*, *supra* note 234.

243 U.S. CUSTOMS & BORDER PROT., FACT SHEET: UNMANNED AIRCRAFT SYSTEM MQ-9 PREDATOR B, at 1 (2009), *available at* http://www.cbp.gov/linkhandler/cgov/newsroom/fact_sheets/marine/uas.ctt/uas.pdf; *see also supra* note 186 and accompanying text.

244 *The Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing Before the S. Comm. on the Judiciary*, 113th Cong. 24 (2013) [hereinafter *Future of Drones in*

better insights into how to most effectively guard citizens' interests from use and abuse of UASs.

State legislation alone, however, will not resolve the UAS privacy threat. UASs represent a national industry, acting within the national airspace and presenting a threat to even Constitutional safeguards.[245] Federal agencies are major UAS users themselves.[246] Additionally, those federal agencies share their UASs with state law enforcement, as shown by the Brossart arrest.[247] The privacy threat crosses state lines. A federal response can provide "nationwide baseline privacy standards" to protect citizens' privacy interests.[248] As such, a federal resolution like the proposed amendment will provide the greatest uniformity and predictability for UAS users and manufacturers.

The amendment proposed in this Note responds to both the benefits of and concerns raised by a state legislative solution. The proposed amendment will result in a federal plan that provides necessary "baseline standards" lacking in state legislation. At the same time, as a primarily regulatory solution with a great deal of flexibility, the door is left open for states to restrict UAS use as they see fit and to the extent that their authority allows.

B. Federal Legislation

At the federal level, both the 112th and 113th Congresses considered bills that would limit government UAS operations for the sake of privacy. Five bills introduced between 2012 and 2013 would impose broad warrant requirements with only limited exceptions for situations such as border patrol, exigent circumstances, or high risk of a terrorist attack.[249] All three introduced in 2012 failed to make it out

---

America Hearing], (statement of Ryan Calo, Assistant Professor, University of Washington School of Law).

245 *See id.* at 23 (statement of Sen. Richard Blumenthal, Member, S. Comm. on the Judiciary).

246 *See supra* notes 182–86 and accompanying text.

247 *See supra* notes 5–7 and accompanying text.

248 *Future of Drones in America Hearing*, *supra* note 244, at 12 (statement of Amie Stepanovich, Dir., Domestic Surveillance Project, Electronic Privacy Information Center).

249 S. 1016, 113th Cong. (2013); H.R. 972, 113th Cong. (2013); H.R. 6199, 112th Cong. (2012); S. 3287, 112th Cong. (2012); H.R. 5925, 112th Cong. (2012).

of committee.[250] The two introduced in 2013, House Bill 972[251] and Senate Bill 1016,[252] remain under consideration.[253]

Two other bills introduced in 2013 differ greatly from these blanket warrant requirements.[254] Republican Ted Poe and Democrat Zoe Lofgren introduced House Bill 637, the Preserving American Privacy Act of 2013,[255] on February 13, 2013. Public entities applying to the FAA for a COA would also submit a data collection statement to the Attorney General.[256] Based on the applicant's data collection statement, the Attorney General could request that the Secretary of Transportation revoke its COA.[257] Additionally, a governmental entity could only collect or disclose detailed information about an individual (1) with a warrant, court order, or the individual's prior written consent;[258] (2) in a border patrol operation;[259] or (3) in an emergency situation.[260] Additionally, information obtained in violation of the Act would be inadmissible in any trial or proceeding.[261]

---

250 *See H.R. 5925 (112th): Preserving Freedom from Unwarranted Surveillance Act of 2012*, GOVTRACK, http://www.govtrack.us/congress/bills/112/hr5925 (last visited Dec. 27, 2013); *H.R. 6199 (112th): Preserving American Privacy Act of 2012*, GOVTRACK, http://www.govtrack.us/congress/bills/112/hr6199 (last visited Dec. 27, 2013); *S. 3287 (112th): Preserving Freedom from Unwarranted Surveillance Act of 2012*, GOVTRACK, http://www.govtrack.us/congress/bills/112/s3287 (last visited Dec. 27, 2013).

251 H.R. 972, 113th Cong. (2013).

252 S. 1016, 113th Cong. (2013).

253 *See H.R. 972 (113th): Preserving Freedom from Unwarranted Surveillance Act of 2013*, GOVTRACK, http://www.govtrack.us/congress/bills/113/hr972 (last visited Dec. 27, 2013); *S. 1016 (113th): Preserving Freedom from Unwarranted Surveillance Act of 2013*, GOVTRACK, http://www.govtrack.us/congress/bills/113/s1016 (last visited Dec. 27, 2013).

254 H.R. 2868, 113th Cong. (2013); H.R. 637, 113th Cong. (2013).

255 H.R. 637; *see also* Keith Laing, *Lawmakers File Bill to Limit U.S. Drones, Citing Privacy Concerns*, HILL (Feb. 14, 2013, 6:14 PM), http://thehill.com/blogs/transportation-report/aviation/283195-lawmakers-file-bill-to-limit-domestic-drone-flights.

256 H.R. 637 § 2 (adding § 3119b(c) to 18 U.S.C.). The required data collection statement would state the purpose and nature of the operation, the UAS's capability to collect detailed information about an individual, and any applicable data minimization and oversight procedures. *Id.* (adding § 3119a(2)(A)–(B) to 18 U.S.C.).

257 *Id.*

258 *Id.* (adding § 3119c(c)(1)–(2), (4) to 18 U.S.C.). The order must be based on reasonable suspicion of criminal activity and a reasonable probability that UAS operation will provide evidence of such criminal activity. *Id.* The order may authorize up to a forty-eight hour operation, renewable at the court's discretion for no more than 30 days. *Id.*

259 *Id.* (adding § 3119c(c)(3) to 18 U.S.C.). This covers operations within twenty-five miles from any external land boundary of the United States for the purpose of patrolling or securing that border. *Id.*

260 *Id.* (adding § 3119c(c)(5) to 18 U.S.C.).

261 *Id.* (adding § 3119c(a) to 18 U.S.C.).

Democrat Peter Welch introduced House Bill 2868,[262] the Drone Aircraft Privacy and Transparency Act of 2013,[263] on July 30, 2013.[264] If passed, this bill would amend the FAA Modernization and Reform Act to require the Department of Transportation, Department of Commerce, Federal Trade Commission, and DHS to study potential threats to privacy protections created by UAS integration, and to submit a report of that study to relevant congressional committees.[265] The bill calls on the Secretary of Transportation, as part of its UAS rulemaking, to establish procedures to ensure UAS integration compliance with privacy principles.[266] Regarding the COA process, House Bill 2868 would create extremely detailed data collection[267] and data minimization[268] statement requirements for COA applicants and mandate public FAA disclosure of approved COAs and the recipients' operations.[269] Further, it imposes a warrant requirement on any protective, law enforcement, or intelligence UAS mission, with a sole exception for exigent circumstances.[270] The bill also establishes a number of remedies for its violation.[271]

The proposed federal legislation does address some of the issues inherent in leaving resolution to the courts[272] or states.[273] Federal leg-

---

262 H.R. 2868, 113th Cong. (2013).

263 *Id.* This bill is almost identical to legislation by the same name introduced in December 2012, H.R. 6676, 112th Cong. (2012), March 2013, H.R. 1262, 113th Cong. (2013), and November 2013, S. 1639, 113th Cong. (2013), by Democrat Edward Markey.

264 *Id.*

265 H.R. 2868 § 2 (adding section 337 to Pub. L. No. 112-95).

266 *Id.*

267 All COA applicants must submit a data collection statement under House Bill 2868. The data collection statement would describe the UAS user, operation location, and operation duration; whether and how information about individuals will be collected, retained, and used; possible impact the UAS operation will have on individuals' privacy and specific steps to mitigate that impact such as implementing security features; contact information that an individual with complaints against the UAS user may use to report his or her complaints and request information; a reasonable process for an individual about whom information has been collected to obtain that information, and process by which the individual may challenge a denial of such a request; and a process by which a person about whom data has been collected may challenge the accuracy of that data. *Id.*

268 Only a law enforcement agency, contractor, or subcontractor must submit a data minimization statement in addition to the data collection statement. The data minimization statement would describe the user's policies to minimize the collection of information unrelated to an authorizing warrant; procedures for destruction of information unrelated to a current investigation or no longer relevant to an investigation; and the user's audit or oversight procedures to ensure compliance with the data collection and data minimization statements. *Id.*

269 *Id.*

270 *Id.*

271 *Id.* § 3.

272 *See supra* Part III.

islation provides uniform and clear limitations for UAS operations. It additionally provides a nationwide solution to the problem, which is already subject to federal regulation,[274] crosses jurisdictional lines,[275] and implicates constitutional concerns.[276]

Yet federal legislation imposing strict limitations is inappropriate for the complex, changing nature of the UAS privacy threat at this time. House Bill 972 and Senate Bill 1016 supply the clearest example—they seek to impose generalized warrant requirements with limited exceptions. Such requirements are simply too rigid to account for the abundance of UAS users and operations. Although House Bills 637 and 2868 impose substantially different constraints on UAS use, they share several weaknesses. First, while both bills call for interagency coordination, they leave out important stakeholders and fail to take full advantage of multiple agencies' areas of expertise. House Bill 637 creates a discretionary concurrence requirement whereby the DOJ *may* request revocation of an offensive COA and the FAA *may* comply with such a request.[277] Stronger mandatory concurrence requirements can raise concerns of a "roving veto power" by one agency,[278] but this arrangement amounts to no power at all. House Bill 2868, on the other hand, charges four agencies with studying privacy problems caused by UAS integration.[279] The amendment leaves out other important stakeholders, specifically the DOJ.[280] Additionally, the bill does not require the study to inform the actions of any named agency. Second, both bills place blanket warrant restrictions on law enforcement's UAS use without regard to the circumstances of the operation, absent a few broad exceptions.[281] Third, both impose potentially costly requirements on the COA process. House Bill 637 distributes the application process across two offices, likely increasing administrative resources needed.[282] House Bill 2868 places extremely detailed reporting requirements on applicants, as well as publication requirements on the FAA.[283]

---

273 *See supra* Part V.A.

274 *See supra* Part I.A.

275 *See, e.g.*, *supra* notes 5–7 and accompanying text.

276 *See supra* Parts II–III.

277 *Id.*

278 *See* FREEMAN & ROSSI, *supra* note 210, at 24–25.

279 H.R. 2868, 113th Cong. § 2 (2013) (adding section 337 to Pub. L. No. 112-95).

280 *See supra* notes 188–91 and accompanying text.

281 H.R. 637, 113th Cong. § 2 (2013) (adding 3119c(c)(1)–(6) to 18 U.S.C.); H.R. Res. 2868 § 2 (adding section 337 to Pub. L. No. 112-95).

282 H.R. 637 § 2 (adding § 3119b(c) to 18 U.S.C.).

283 H.R. 2868 § 2 (adding section 337 to Pub. L. No. 112-95).

One additional difficulty that federal legislative efforts to resolve UAS issues have faced generally is a lack of bipartisan support, with most support coming from Republican members of Congress.[284] House Bill 637 has fared the best thus far. Bipartisan cosponsors introduced the bill, attracting a total of fifteen Republican and seven Democratic cosponsors to date.[285] House Bill 2868 was introduced by a Democrat, and currently has no cosponsors.[286] An earlier version of this bill, House Bill 1262, was also introduced by a Democrat and had one Democratic cosponsor.[287] The solution proposed by this Note is markedly different from previously proposed federal legislation—particularly the legislation introduced in 2012.

In contrast to the previously proposed legislation, this Note's proposed amendment will more effectively confront and resolve the UAS privacy threat. First, it requires participation of the major stakeholders, which includes the FAA, DOJ, and DHS, at a minimum. It leaves open an invitation for additional participants, such as those included in House Bill 2868. Interagency coordination through communication and collective planning permits each agency to tap into the collective expertise in UAS and privacy issues. Second, the substantive guidelines developed under this proposed amendment and the resulting MOU must be revised to ensure that the solution develops in step with the privacy threat itself. The possible flexibility and development of these guidelines stands in contrast to the rigid reporting and warrant requirements imposed by the 2013 House Bills.[288] Finally, preserving the COA process within the FAA may have lower transactional costs than spreading it between two agencies. Similarly, requiring the FAA to consider the results of interagency planning in its COA process allows the member agencies to use its expertise to determine what information should be relevant to the privacy inquiry, rather than deferring to the legislature to make that decision. For

---

284 In 2012, House Bill 5925 had twenty-four Republican cosponsors, *H.R. 5925 (112th): Preserving Freedom from Unwarranted Surveillance Act of 2012*, *supra* note 250, Senate Bill 3287 had two Republican cosponsors, *S. 3287 (112th): Preserving Freedom from Unwarranted Surveillance Act of 2012*, *supra* note 250, and House Bill 6199 had twenty-five Republican cosponsors and one Democrat cosponsor, *H.R. 6199 (112th): Preserving American Privacy Act of 2012*, *supra* note 250.

285 *H.R. 637: Preserving American Privacy Act of 2013*, GOVTRACK, http://www.govtrack.us/congress/bills/113/hr637 (last visited Dec. 27, 2013).

286 *H.R. 2868: Drone Aircraft Privacy and Transparency Act of 2013*, GOVTRACK, http://www.govtrack.us/congress/bills/113/hr2868 (last visited Dec. 27, 2013).

287 *H.R. 1262: Drone Aircraft Privacy and Transparency Act of 2013*, GOVTRACK, http://www.govtrack.us/congress/bills/113/hr1262 (last visited Dec. 27, 2013).

288 *Cf. supra* notes 277–83.

these reasons, the proposed amendment would be more effective than the legislation previously discussed in Congress.

C. Single-Agency Regulation

Another possibility is that Congress could delegate regulatory authority over UAS privacy issues to a single agency. Because the FAA is already deeply involved in UAS regulation, some stakeholders in the UAS debate have pressed for the agency to take on privacy issues as well, specifically in its rulemaking procedures.[289] Professor Calo discussed a single-agency proposal as a possible stopgap measure until Congress contemplates more sweeping changes in privacy law as a whole.[290] He suggested that Congress "instruct the FAA to take privacy into account as part of its mandate to integrate drones into domestic airspace."[291] When pressed on whether the FAA has adequate expertise to regulate the privacy side of integration, Calo noted that although the FAA has historically dealt only in safety, they could certainly acquire expertise in privacy going forward.[292]

The pushback on Calo's proposal highlights a problem inherent in the single-agency solution: generally, advocates are hard pressed to name an ideal agency. The FAA publicly rejected the invitation to voluntarily address privacy because its primary mission is safety, and it does not possess the necessary expertise in privacy issues.[293] While some commentators see the Agency's Final Privacy Requirements for UAS test sites as a step away from this position, the FAA maintains that regulating privacy is not within its purview.[294] Recognizing the FAA's reluctance, the GAO stated that "DHS or DOJ might be better positioned to address UAS privacy issues."[295] Ultimately, it remains unclear what one agency is best suited for this role, and no agency has proactively stepped into it.[296]

The solution proposed in this Note escapes this difficulty by mandating the involvement of the primary interested agencies—FAA,

---

289 DILLINGHAM, *supra* note 73, at 11; *see also* STANLEY & CRUMP, *supra* note 14, at 2 (urging that "the FAA's obligation to protect individuals on the ground should include protecting the privacy that Americans have traditionally enjoyed and rightly expect").

290 *Future of Drones in America Hearing*, *supra* note 244, at 72 (prepared statement of Ryan Calo).

291 *Id.*

292 *Id.* at 29 (statement of Ryan Calo).

293 *See supra* notes 173–78 and accompanying text.

294 *See supra* notes 176–78 and accompanying text.

295 MEASURING PROGRESS, *supra* note 26, at 36.

296 *See id.*

DOJ, and DHS—while permitting others' involvement as well. The MOU itself will reduce each agency's interest and authority to writing, clarifying the current confusion. Additionally, the agencies will be better suited to expand their understanding of the issue by tapping into each other's expertise, rather than struggling to develop such expertise in isolation.

Conclusion

Complete UAS integration into the domestic airspace is a steadily approaching reality. As law enforcement surveillance missions increase, so does the threat to citizens' Fourth Amendment and related privacy rights. However, sophisticated UAS technology can be constrained by neither existing Fourth Amendment jurisprudence nor the current statutory scheme. Additionally, legislative and single-agency solutions fail to address the complex nature of UAS use. Congress should revise the FAA Modernization and Reform Act of 2012 to require coordination between the FAA and other agencies invested in UAS privacy issues though an MOU that clarifies jurisdictional bounds, assigns responsibilities, and creates accountability for the privacy "gap" in UAS integration. Such an amendment would respond to the complex and changing nature of the UAS privacy issue and take the much-needed initial step of assigning responsibility for its resolution.