




2013

Watching the Watchmen: Drone Privacy and the Need for Oversight

Ben Jenkins
University of Kentucky

Follow this and additional works at: <https://uknowledge.uky.edu/klj>

 Part of the [Air and Space Law Commons](#), and the [Science and Technology Law Commons](#)
Right click to open a feedback form in a new tab to let us know how this document benefits you.

Recommended Citation

Jenkins, Ben (2013) "Watching the Watchmen: Drone Privacy and the Need for Oversight," *Kentucky Law Journal*: Vol. 102 : Iss. 1 , Article 8.
Available at: <https://uknowledge.uky.edu/klj/vol102/iss1/8>

This Note is brought to you for free and open access by the Law Journals at UKnowledge. It has been accepted for inclusion in Kentucky Law Journal by an authorized editor of UKnowledge. For more information, please contact UKnowledge@lsv.uky.edu.

NOTES

Watching the Watchmen: Drone Privacy and the Need for Oversight

*Ben Jenkins*¹

“The question we confront today is what limits are upon this power of technology to shrink the realm of guaranteed privacy.”

—*Kyllo v. United States*

INTRODUCTION

To those who enjoy the popular war simulation video game franchise *Call of Duty*, the phrase “our UAV is online” is a thing of beauty.² They signal that the locations of all enemy combatants are now conveniently showcased on an in-game map.³ To protect themselves from being seen, the enemy must deploy a UAV jammer to scramble the electronics of the drone.⁴ But drones are not just fun and games: to privacy enthusiasts, the idea of these words used in connection with domestic drone use might be harrowing. Citizens lack UAV jammers, and currently the Constitution is their only protection from the government’s all-seeing eye.

Drones are rarely used in U.S. airspace today; however, as a result of a recent congressional push, the Federal Aviation Administration (FAA) has predicted that 30,000 drones could be flying in U.S. skies in less than twenty years.⁵ Coupled with cutting-edge technology such as thermal imaging devices, high-powered cameras, and facial recognition technology, current law may not be prepared to adapt fast enough to address the privacy concerns raised by mass domestic drone usage. Some action should be taken to protect citizens’ privacy; however, in doing so, care must be taken to not smother a kindling industry

¹ J.D. expected May 2014, University of Kentucky College of Law.

² See *Our UAV is Online*, URBAN DICTIONARY, <http://www.urbandictionary.com/define.php?term=OUR+UAV+IS+ONLINE&defid=3246529> (last visited Oct. 19, 2013).

³ See *id.*

⁴ Jammers interrupt communication systems so that the information being transmitted is indiscernible; the effect is similar to turning up your radio louder than everyone else’s so they cannot hear their own radios. *UAV Jammer*, CALL OF DUTY WIKI, http://callofduty.wikia.com/wiki/UAV_Jammer (last visited Mar. 17, 2013).

⁵ FED. AVIATION ADMIN., FAA AEROSPACE FORECAST: FISCAL YEARS 2010–2030, at 48 (2010), available at http://faa.gov/data_research/aviation/aerospace_forecasts/2010–2030/media/2010%20Forecast%20Doc.pdf.

that could bring great technological advancement and economic growth to America's economy. The industry "hopes that there will be 100,000 people with drone-related jobs by 2025,"⁶ and envisions a world in which parents will soon be able to slap a high-tech sticker on their child's soccer ball that will allow a drone to follow and record the action of the game in high quality video.⁷

This note argues that in order to safeguard Americans' privacy against government drone surveillance in an actively growing field, Congress should implement legislation that provides a framework for protection while allowing for industry growth and innovation. Although several bills are pending, it is uncertain if or when those bills will pass. While it would be a large step towards ensuring privacy protection from drone surveillance if the proposed bills pass, there is still room for improvement. Even the most promising bill, the Drone Aircraft Privacy and Transparency Act of 2013 (DAPTA),⁸ fails to provide a process for ongoing oversight of drone operators to ensure transparency and continued compliance with the Act's privacy protections. DAPTA and other pending legislation should be amended to charge a single agency with responsibility for drone privacy oversight, including audits to make sure drone operators comply with privacy regulations. Operators should be required to submit ongoing reports of their data collection, retention, and disposal procedures to the agency, and these reports should be gathered and submitted to Congress annually.

Proper legislative action would ensure that the constitutional right to privacy is not overrun by rapidly growing technologies, diminishing privacy norms, and heightened security interests. With proper privacy protections in place, society could be more receptive to increased use, development, and application of drones in daily life. Part I of this Note provides background on drones: their nature, use, technology, and the current Fourth Amendment jurisprudence relevant to such. Part II explains why drones present a unique threat to privacy and addresses current shortfalls in Fourth Amendment jurisprudence and in legislative efforts to address privacy concerns connected with their widespread use. Part III suggests amendments to proposed legislation to address shortfalls therein, concluding that proper anticipatory action and ongoing oversight are necessary to ensure that police technology does not erode the minimum expectations of privacy guaranteed by the Fourth Amendment.⁹

6 Victor Luckerson, *Where Will the Drone Jobs Go? States Balance Economic Opportunity with Privacy Concerns*, TIME (May 1, 2013), <http://business.time.com/2013/05/01/where-will-the-drone-jobs-go-states-balance-economic-opportunity-with-privacy-concerns/>.

7 Chris Anderson, *Why We Shouldn't Fear Personal Drones*, TIME (Jan. 31, 2013), <http://ideas.time.com/2013/01/31/why-we-shouldnt-fear-personal-drones/>; Luckerson, *supra* note 5.

8 Drone Aircraft Privacy and Transparency Act of 2013, H.R. 2868, 113th Cong. (2013).

9 See *Kyllo v. United States*, 533 U.S. 27, 34 (2001).

I. OVERVIEW: A SNAPSHOT OF DRONES AND THEIR LEGAL LANDSCAPE

A. Defining Drones

1. *Nature*.—Drones, also known as unmanned aerial vehicles, are aircrafts “operated without the possibility of direct human intervention from within or on the aircraft.”¹⁰ Drones can range in size from a traditional jet¹¹ to an insect.¹² Although current drones have maximum flight times of up to two days,¹³ emerging technology could increase flight times indefinitely.¹⁴

2. *Uses*.—Drones have been used internationally in military surveillance and counterterrorism operations in Iraq, Afghanistan, Pakistan and Yemen.¹⁵ Domestically, UAV technology has been used in border control,¹⁶ search and rescue missions,¹⁷ and surveillance during police standoffs.¹⁸ In response to the recent push to integrate drones in the national airspace system, drone use and application is expected to skyrocket in the near future to include surveilling real estate developments,¹⁹ detecting and surveilling forest fires,²⁰ monitoring

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

11 For example, Northrup Grumman’s RQ–4A Global Hawk has a 116-foot wingspan. *Flight of the Drones: Why the Future of Air Power Belongs to Unmanned Systems*, ECONOMIST, Oct. 8, 2011, available at <http://economist.com/node/21531433>.

12 *US Military Surveillance Future: Drones Now Come in Swarms?*, RT (June 20, 2012, 7:47 PM), <http://rt.com/news/us-drones-swarms-274/>. The smallest commercial drones currently cost as little as \$300. *Parrot AR.Drone 2.0 Quadricopter*, AMAZON, <http://www.amazon.com/Parrot-AR-Drone-Quadricopter-Controlled-Android/dp/B007HZLLOK> (last visited Oct 19, 2013).

13 See David Axe, *Upgrades to Killer Drone Could Make it Fly for Two Days Straight*, WIRED (Apr. 19, 2012, 2:09 PM), <http://www.wired.com/dangerroom/2012/04/killer-drone-upgrade/>.

14 Richard Whittle, *How it Works: Laser Beaming Recharges UAV in Flight*, POPULAR MECHANICS (July 28, 2012), <http://www.popularmechanics.com/technology/aviation/news/how-it-works-laser-beaming-recharges-uav-in-flight-11091133>.

15 Peter Finn, *Rise of the Drone: From Calif. Garage to Multibillion-dollar Defense Industry*, THE WASHINGTON POST, Dec. 23, 2011, available at http://articles.washingtonpost.com/2011-12-23/national/35287608_1_mini-drones-engineer-military-doctrine.

16 Drones have been used at the border to prevent terrorism, drug and weapons trading, and illegal immigration. See CHAD C. HADDAL & JEREMIAH GERTLER, CONG. RESEARCH SERV., RS21698, *HOMELAND SECURITY: UNMANNED AERIAL VEHICLES AND BORDER SURVEILLANCE 6* (2010), available at <http://www.fas.org/sgp/crs/homesecc/RS21698.pdf>.

17 Charlie Ban, *Drones Assist County Sheriffs’ Search and Rescue Missions*, NACO.ORG (May 21, 2012), <http://www.naco.org/newsroom/countynews/Current%20Issue/5-21-2012/Pages/Dronesassistcountysheriffs%E2%80%99searchandrescuemissions.aspx>.

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

19 Troy Roberts, *On the Radar: Government Unmanned Aerial Vehicles and Their Effect on Public Privacy Interests from Fourth Amendment Jurisprudence and Legislative Policy Perspectives*, 49 JURIMETRICS J. 491, 492 (2009).

20 Brian Skoloff & Tracie Cone, *Predator Drone Now Part of Calif. Wildfire Battle*, ABC

hostage situations,²¹ observing livestock and oil pipelines,²² and even tracking FedEx package delivery.²³

3. *Technology*.—Currently, drones can be outfitted with high-powered cameras,²⁴ thermal imaging devices,²⁵ and license plate readers.²⁶ In the near future, law enforcement organizations might seek to outfit drones with facial recognition capabilities, which can recognize and track individuals based on height, weight, age, gender, and skin color.²⁷ The sophistication of drone technology might influence a court's decision on whether domestic drone use is lawful under the Fourth Amendment. This is a question that remains largely unanswered by current Fourth Amendment jurisprudence, suggesting the need for legislative action to ensure privacy protection from government searches.

B. Current Fourth Amendment Jurisprudence

Modern day Fourth Amendment jurisprudence has evolved as the Supreme Court has interpreted the Constitution in light of emerging technologies. But the law has struggled to keep up with technology's rapid growth, leaving many questions unanswered concerning the applicability of Fourth Amendment protections to government drone surveillance.

News (Aug. 28, 2013), <http://abcnews.go.com/US/wireStory/calif-launches-drone-scout-spot-fires-20096065>; cf. Brian Bennett, *Drones Tested as Tools for Police and Firefighters*, L.A. TIMES (Aug. 5, 2012), <http://articles.latimes.com/2012/aug/05/nation/la-na-drones-testing-20120805> (discussing the testing of drones to determine their ability to find the source of a building fire).

²¹ Bennett, *supra* note 19.

²² Isolde Raftery, *Anticipating Domestic Boom, Colleges Rev Up Drone Piloting Programs*, NBC NEWS (Jan. 29, 2013), <http://investigations.nbcnews.com/news/2013/01/29/16726198-anticipating-domestic-boom-colleges-rev-up-drone-piloting-programs>.

²³ *Id.*

²⁴ The US Army recently acquired a 1.8 gigapixel camera for drone use. This camera allows drones to track people and vehicles across almost 65 miles from altitudes above 20,000 feet. *US Army Unveils 1.8 Gigapixel Camera Helicopter Drone*, BBC NEWS (Dec. 29, 2011), <http://www.bbc.co.uk/news/technology-16358851>.

²⁵ See, e.g., *Draganflyer x6 Thermal Infrared Camera*, DRAGANFLY INNOVATIONS INC., <http://www.draganfly.com/uav-helicopter/draganflyer-x6/features/flir-camera.php> (last visited Oct. 20, 2013).

²⁶ *Unmanned Aerial Vehicles Support Border Security*, CUSTOMS AND BORDER PROTECTION TODAY (July–Aug. 2004), http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml.

²⁷ See Clay Dillow, *Army Developing Drones that Can Recognize Your Face from a Distance*, POPSCI (Sept. 28, 2011, 5:01 PM), <http://www.popsci.com/technology/article/2011-09/army-wants-drones-can-recognize-your-face-and-read-your-mind>; see also *Next Generation Identification*, FED. BUREAU OF INVESTIGATION, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi (last visited Oct 20, 2013) (explaining the FBI's current \$1 billion project to enhance its facial recognition capabilities).

1. *Katz Standard*.—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....”²⁸ A qualifying search under the Amendment requires that police first have probable cause or a warrant.²⁹ Under the Exclusionary Rule, any evidentiary fruits from an unreasonable search are barred from being admitted against the wronged individual in court.³⁰ Conversely, if there has been no search, no warrant is necessary.³¹ Therefore, the question of whether police need a warrant to conduct drone surveillance turns on whether drone use counts as a search for Fourth Amendment purposes.

The Supreme Court first considered this question in *Olmstead v. United States*, holding that a Fourth Amendment search only occurs when police physically invade a person or his property.³² The Court employed a purely physical trespass test and, since the government had wiretapped the defendant’s home phone from a location off the property, it concluded that no search implicating constitutional rights had occurred.³³ The Court departed from this property standard almost forty years later to focus on privacy interests.³⁴

In *Katz v. United States*,³⁵ the defendant was convicted of transmitting gambling information through telephone lines after the FBI installed a listening device on the outside of a public telephone booth.³⁶ Rejecting both parties’ arguments centering on whether a phone booth was a “constitutionally protected area,”³⁷ the Court shifted its analysis from a physical property standard to one involving a “reasonable expectation of privacy.”³⁸ Recognizing that the Constitution protects “people not places,”³⁹ the Court looked not to the nature of the area being searched but to the person’s expectations.⁴⁰ Although the phone booth was visible, what the defendant sought to exclude when he

28 U.S. CONST. amend IV.

29 See *Illinois v. Gates*, 462 U.S. 213, 238 (1983).

30 See *Weeks v. United States*, 232 U.S. 383, 391–94 (1914) (applying the Exclusionary Rule to federal cases); see also *Mapp v. Ohio*, 367 U.S. 643, 655–56 (1961) (applying the Exclusionary Rule to state cases).

31 See *California v. Ciraolo*, 476 U.S. 207, 215 (1986) (“The Fourth Amendment simply does not require the police traveling in the public airways at this altitude to obtain a warrant in order to observe what is visible to the naked eye.”).

32 *Olmstead v. United States*, 277 U.S. 438, 466 (1928).

33 *Id.*

34 *Katz v. United States*, 389 U.S. 347 (1967).

35 *Id.*

36 *Id.* at 348.

37 *Id.* at 351. The parties were justified in focusing on the private or public nature of the “area” in which the recording device was installed, given the Court’s earlier holdings that a search was a physical intrusion into a private area such as the home.

38 *Id.* at 359.

39 *Id.* at 351.

40 *Id.*

entered the phone booth was not the “intruding eye—but the uninvited ear.”⁴¹ The Court drew the distinction that “[w]hat a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.”⁴²

The most important development from *Katz*, however, came from Justice Harlan’s concurrence, in which he established a two-fold test that remains the standard today. In order to invoke Fourth Amendment protection, Justice Harlan determined that a person must have an actual, subjective expectation of privacy and the expectation must be one that society is prepared to recognize as “reasonable.”⁴³ Departing from the physical intrusion focus of *Olmstead*, *Katz* redefined Fourth Amendment protection to include intrusive searches that are not physical, showing less concern for the method of invasion and more concern for societal privacy norms.⁴⁴

Despite the shift in *Katz* to “people and not places,” the Court in *United States v. Jones*⁴⁵ observed that a Fourth Amendment search occurs “at a minimum” where “the Government obtains information by physically intruding on a constitutionally protected area”⁴⁶ The majority in *Jones* indicated that *Katz*’s reasonable expectation of privacy test was never meant to overrule the property-based approach of *Olmstead* but instead to supplement it.⁴⁷ This raises the question: Where do individuals enjoy the most and the least Fourth Amendment protection? Subsequent cases have contributed partial answers, delineating zones of protection that may give insight into the likely treatment of domestic drone surveillance under the current jurisprudence.

2. *Defining the Zones of Privacy.*—*Kyllo v. United States* solidified the home as the zone afforded the greatest privacy protection by the Constitution.⁴⁸ In addition to the Constitution’s express protection against the government’s physical entry and search of the home, *Kyllo* extended this protection to certain technologies used to pierce this zone of privacy.⁴⁹ In *Kyllo*, government agents employed thermal imagers to detect heat signals coming from the external walls of the defendant’s home, and used that information to conclude that there were marijuana grow lamps inside.⁵⁰ The Court refused to allow technology to erode

41 *Id.* at 352.

42 *Id.* at 351.

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

44 *Id.* at 352–53 (majority opinion).

45 *United States v. Jones*, 132 S. Ct. 945 (2012).

46 *Id.* at 951 n.3.

47 *Id.* at 947 (“The *Katz* reasonable-expectation-of-privacy test has been added to, but no substituted for, the common-law trespassory test.”).

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

49 *Id.* at 34.

50 *Id.* at 29–30.

the privacy guaranteed by the Fourth Amendment, holding that “obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area’ constitutes a search—at least where (as here) the technology in question is not in general public use.”⁵¹ The home, however, is not absolutely shielded from government surveillance; the “plain view” doctrine, as noted by Justice Harlan in *Katz*, establishes that “objects, activities, or statements [a person] exposes to the ‘plain view’ of outsiders are not ‘protected’ because no intention to keep them to himself has been exhibited.”⁵² Thus, in some instances, police may conduct warrantless searches of the inside of a home using their natural senses.⁵³ To qualify for this exception, the police must be in a lawful vantage point when they conduct the surveillance outside the home, and the incriminating nature of the evidence must be readily apparent.⁵⁴

Outside of the confines of the home, the degree of an individual’s Fourth Amendment protection depends on whether the search occurs within the “curtilage” or “open fields.”⁵⁵ Curtilage refers to the area immediately surrounding the home, which the Court has defined as “the area to which extends the intimate activity associated with the ‘sanctity of a man’s home and the privacies of life’”⁵⁶ The Court has identified four factors in determining whether an area is curtilage: how close the area is to the home, whether the area is fenced in, how the area is used, and whether the area is shielded from observation by passersby.⁵⁷ Curtilage is generally given the same protection afforded the home while open fields are given less protection.⁵⁸ In *Oliver v. United States*,⁵⁹ the Court affirmed that Fourth Amendment protection did not extend to open fields, which “do not provide the setting for those intimate activities that the Amendment is intended to shelter from governmental interference or surveillance.”⁶⁰ Differentiating between open fields and curtilage is an often difficult task which has important implications for drone surveillance, as the Court has permitted searches in both areas in the manned aerial surveillance cases discussed *infra*.

51 *Id.* at 34.

52 *Katz*, 389 U.S. at 361 (Harlan, J., concurring).

53 *See* *United States v. Hammett*, 236 F.3d 1054, 1061 (9th Cir. 2001) (holding police observation of marijuana plants through a crack in the house’s siding a lawful search).

54 *See* *Coolidge v. New Hampshire*, 403 U.S. 443, 466 (1971).

55 *See* *Hester v. United States*, 265 U.S. 57 (1924) (distinguishing between the doctrines of curtilage and open fields).

56 *Oliver v. United States*, 466 U.S. 170, 180 (1984) (citation omitted).

57 *United States v. Dunn*, 480 U.S. 294, 301 (1987).

58 *Oliver*, 466 U.S. at 180.

59 466 U.S. 170.

60 *Id.* at 179.

3. *Manned Aerial Surveillance*.—In a series of cases providing the closest analogy to drones thus far, the Court considered the constitutionality of manned aerial surveillance, and in each, held that the fly-over at issue was not a prohibited Fourth Amendment search since the areas were open to public view. In *California v. Ciraolo*,⁶¹ a police officer, based on an anonymous tip, flew a winged aircraft at an altitude of 1000 feet and observed marijuana in a suspect's backyard without first procuring a search warrant.⁶² The Court held that because the policeman was in legally navigable airspace, he had a right to be there and “[w]hat a person knowingly exposes to the public . . . is not a subject of Fourth Amendment protection.”⁶³ Despite the area being fenced in, the Court viewed the defendant's expectation of privacy as unreasonable since any member of the public flying overhead could have glanced down and seen the plants.⁶⁴ The Court underscored the fact that the plane was in navigable airspace as defined by federal statute.⁶⁵

Similarly, in *Florida v. Riley*, police observed marijuana growing in a greenhouse in the defendant's backyard through the structure's partially open roof while flying in a helicopter at 400 feet.⁶⁶ The Court ruled the search was reasonable, relying again on the fact that the helicopter had a right to be in the airspace and any member of the public flying in a helicopter over the defendant's property could have observed the marijuana.⁶⁷ The Court held the defendant's expectation of privacy unreasonable since there was “nothing in the record . . . to suggest that helicopters flying at 400 feet are sufficiently rare in this country”⁶⁸ The Court seemed to reason that because the helicopter did not interfere with the defendant's use of the curtilage and since there was no undue noise, wind, dust, or threat of injury, the search was reasonable.⁶⁹ In her concurrence, Justice O'Connor criticized the plurality's decision as resting “the scope of Fourth Amendment protection too heavily on compliance with FAA regulations whose purpose is to promote air safety, not to protect [Fourth Amendment rights].”⁷⁰

Finally, in *Dow Chemical Co. v. United States*,⁷¹ the Court rejected a theory of “industrial curtilage” when a government agency took aerial photographs of a 2000-acre commercial plant.⁷² The Court concluded the open areas of the

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

62 *Id.* at 209.

63 *Id.* at 213 (quoting *Katz v. United States*, 389 U.S. 347, 351 (1967)).

64 *Id.* at 213–14.

65 *Id.* at 213.

66 *Florida v. Riley*, 488 U.S. 445, 451 (1989).

67 *Id.*

68 *Id.*

69 *Id.* at 452.

70 *Id.* (O'Connor, J., concurring).

71 *Dow Chem. Co. v. United States*, 476 U.S. 227, 239 (1986).

72 *Id.* at 239.

industrial plant were more like open fields than intimate curtilage of the home and that photographing the plant from navigable airspace was not a search.⁷³

4. *Government Tracking*.—Like the aerial surveillance cases, individuals have reduced expectations of privacy from government tracking during their travel in public places. This has allowed warrantless tracking of a vehicle's movements on public streets.⁷⁴ In *United States v. Knotts*,⁷⁵ the police tracked a vehicle's movements solely on public streets using both visual surveillance and a radio transmitter.⁷⁶ The Court held that no Fourth Amendment search had occurred because people do not have a reasonable expectation of privacy in their movements on public streets.⁷⁷ In contrast, in *United States v. Karo*,⁷⁸ the police tracked a beeper they had placed in a container in the defendant's possession while he was on public streets and in his home.⁷⁹ Holding that the monitoring of a beeper in a private residence violates the Fourth Amendment rights of those with a justifiable interest in the privacy of the residence, the Court observed that the “[i]ndiscriminate monitoring of property that has been withdrawn from public view would present far too serious a threat to privacy interests in the home to escape entirely some sort of Fourth Amendment oversight.”⁸⁰

Although government tracking of public movements is generally not considered a search, if it is prolonged and pervasive, it might be. In 2012, in *United States v. Jones*,⁸¹ the government attached a GPS tracking device to the defendant's Jeep and tracked the vehicle's movement for twenty-eight days.⁸² The defendant was subsequently charged with drug trafficking conspiracy and sought to suppress the evidence as fruits of an unreasonable search.⁸³ The Court declined to apply *Katz*'s “reasonable expectation of privacy” test and instead applied *Olmstead*'s property-based approach, holding the Government's physical intrusion on an “effect” (the vehicle) for the purpose of obtaining information constituted a “search.”⁸⁴ The Court found “such a physical intrusion would have been considered a ‘search’ within the meaning of the Fourth Amendment when it was adopted.”⁸⁵

73 *Id.*

74 *See United States v. Knotts*, 460 U.S. 276, 285 (1983).

75 *Id.*

76 *Id.* at 281.

77 *Id.* at 281–82.

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

79 *Id.* at 708.

80 *Id.* at 716.

81 *United States v. Jones*, 132 S. Ct. 945 (2012).

82 *Id.* at 948.

83 *Id.*

84 *Id.* at 949–50.

85 *Id.* at 949.

In his concurrence, Justice Alito expressed concern that the majority's opinion would be difficult to apply due to vast changes in trespass law since the country's founding.⁸⁶ In his view the majority's opinion was flawed, ignoring what was really important—the use of a GPS for long-term tracking—and left unanswered many questions incompatible with a property-based test.⁸⁷ For instance, what if the government gained remote access to a vehicle's on-board GPS? Although no physical trespass has occurred, would the search be lawful?⁸⁸ Further, what if the police used aerial surveillance instead?⁸⁹ Justice Alito suggested that the suspect's "reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove,"⁹⁰ and applying the *Katz* test would allow a more workable rule for searches involving technology, making the element of physical intrusion unnecessary for finding that a search occurred. Justice Alito also observed that "[i]n the pre-computer age, the greatest protections of privacy were neither constitutional nor statutory, but practical" noting traditional surveillance for extended periods was "difficult and costly and therefore rarely undertaken."⁹¹

In her concurrence, Justice Sotomayor elaborated on practical concerns as they relate to privacy, noting that extensive GPS monitoring generates a precise record of peoples' travel patterns revealing intimate details about their daily lives such as "familial, political, professional, religious, and sexual associations."⁹² Taking this into account, she suggested a *Katz* approach under which she would ask, "whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."⁹³ Technological surveillance has become more intrusive in effect than traditional surveillance, primarily because of the practical limitations that once restrained extended monitoring. Thus, Justice Sotomayor warned that extended GPS monitoring in investigations of most offenses violates expectations of privacy.⁹⁴ The rationales expressed in the concurring opinions offer insight into "the

86 *See id.* at 957 n.2 (Alito, J., concurring) (joined by Ginsburg, Breyer, & Kagan, JJ.) (noting that a common law trespass for chattels, unlike today, did not require actual damage to the chattel and that the car in this case did not sustain any damage).

87 *See id.* at 961.

88 *See id.* at 962 ("Would the sending of a radio signal to active [a stolen vehicle detection system] constitute a trespass to chattels? Trespass to chattels has traditionally required a physical touching of the property.")

89 *See id.* at 961 ("If the police attach a GPS device to a car and use the device to follow the car for even a brief time, under the Court's theory, the Fourth Amendment applies. But if the police follow the same car for a much longer period using unmarked cars and aerial assistance, this tracking is not subject to any Fourth Amendment constraints.")

90 *Id.* at 958.

91 *Id.* at 963.

92 *Id.* at 955 (Sotomayor, J., concurring).

93 *Id.* at 956.

94 *Id.* at 955.

direction the Court might lead us in the light of technological advancements and privacy concerns”⁹⁵ Despite the direction of Fourth Amendment jurisprudence, in light of current technology, individuals may be unprotected from government drone surveillance.

II. WHY ARE DRONES A PRIVACY ISSUE?

A. Lack of Practical Safeguards

Drone technology presents a unique threat to privacy by eliminating practical safeguards against Fourth Amendment searches. First, drones can be substantially smaller than traditional aircrafts, making them practically invisible at altitudes where traditional aircraft could be spotted from the ground.⁹⁶ Second, unlike traditional aircraft such as helicopters, many drones can operate almost silently, allowing them to conduct surveillance virtually unnoticed.⁹⁷ Third, as one legal scholar notes: “[w]ith the ability to hover or circle in the sky for hours, [drones] present a potential intrusion far more pervasive than the mere flyover of a plane or helicopter.”⁹⁸ As Justice Alito observed in *Jones*, constant long-term surveillance without technology (such as GPS tracking) requires many agents, multiple vehicles, and perhaps aerial assistance, practically rendering such surveillance impossible.⁹⁹ Drone capabilities have even further opened the doors to previously unknown levels of invasive government monitoring by rendering it relatively easy and cheap.

Similarly, drone surveillance allows a depth of information collection previously impossible. Like the *Jones* concurrences’ concern with GPS monitoring, drones allow the collection of a vast amount of intimate personal information—travel patterns or shopping habits to name a few¹⁰⁰—but on a much larger scale, and surveillance is not limited merely to an individual but all people beneath the drone’s all-seeing eye.

B. Is Fourth Amendment Jurisprudence Applicable to Drones?

The constitutionality of domestic drone surveillance may depend on the context in which the surveillance takes place. Both the technology used and

⁹⁵ *United States v. Wilkerson*, No. 11–027 Section “B”(3), 2012 U.S. Dist. LEXIS 8527, at *2 n.1 (E.D. La. Jan. 23, 2012) (“The competing rationales between the majority opinion and the concurring ones could be insightful to the direction the Court might lead us in the light of technological advancements and privacy concerns”).

⁹⁶ Travis Dunlap, *We’ve Got Our Eyes on You: When Surveillance by Unmanned Aircraft Systems Constitutes a Fourth Amendment Search*, 51 S. TEX. L. REV. 173, 201 (2009).

⁹⁷ *Id.*

⁹⁸ *Id.*

⁹⁹ *Jones*, 132 S. Ct. at 963 (Alito, J., concurring) (joined by Ginsburg, Breyer, & Kagan, JJ.).

¹⁰⁰ *Id.* at 955–56 (Sotomayor, J., concurring); *see id.*

the location of the surveillance may factor into the Fourth Amendment's application to drone surveillance.

1. Location of Search.—Previous Fourth Amendment jurisprudence established zones of privacy around the home, each with distinguishing levels of protection against unreasonable searches and seizures. Based on existing case law, it is reasonable to assume that drone surveillance of an individual in his home—the area afforded greatest privacy protection under the Constitution—would be unlawful. Specifically, in *Kyllo*, the Court considered the police's use of thermal technology to gain information about the inside of an individual's home.¹⁰¹ Drones can now be equipped with similar technology and will soon be able to see through walls and ceilings.¹⁰² Under the *Kyllo* standard, warrantless searches aided by technologies not in general public use should not pass muster under the Fourth Amendment. While the more powerful equipment—such as facial recognition technology and certain high-powered cameras—might fail this test, thermal imaging technology like that used in *Kyllo* is more available to the general public today than it was when *Kyllo* was decided.¹⁰³ Therefore, an important unanswered question concerning the *Kyllo* standard is what is meant by technology “not in general public use.” To be in “general public use,” does the technology have to be used by a majority of the public, or is it enough that the technology is readily available and affordable to the public? It is only a matter of time before technology like facial recognition and high-powered cameras are widely used by the public.¹⁰⁴ What seems clear, however, is that the use of low-powered cameras and other unsophisticated technology, which are in general use, to view people and objects in their home while in plain view would probably be constitutional under the *Kyllo* standard, because an officer does not have to “shield his eyes” from illegal activity in plain view.¹⁰⁵

It is unclear whether the same protection against surveillance afforded to the home would be extended to areas immediately surrounding the home—say, a deck, pool, or garden.¹⁰⁶ Although the Court has generally given the

¹⁰¹ *Kyllo v. United States*, 533 U.S. 27, 29–30 (2001).

¹⁰² RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R42701, DRONES IN DOMESTIC SURVEILLANCE OPERATIONS: FOURTH AMENDMENT IMPLICATIONS AND LEGISLATIVE RESPONSES 13 (2013), available at <http://www.fas.org/sgp/crs/natsec/R42701.pdf>.

¹⁰³ See, e.g., Draganflyer x6, *supra* note 25.

¹⁰⁴ See Andy Bloxham, *Facial Recognition Software to Go Public*, THE TELEGRAPH (Aug. 22, 2010, 3:55 PM), <http://www.telegraph.co.uk/technology/news/7958511/Facial-recognition-software-to-go-public.html>.

¹⁰⁵ See *California v. Ciraolo*, 476 U.S. 207, 213 (1986).

¹⁰⁶ See Paul McBride, *Beyond Orwell: The Application of Unmanned Aircraft Systems in Domestic Surveillance Operations*, 74 J. AIR. L. & COM. 627, 655–56 (2009) (“While framing the question presented in *Kyllo*, Justice Scalia reiterated that *Dow Chemical*, which upheld the constitutionality of high-resolution aerial photography of an industrial complex, was ‘not an area immediately adjacent to a private home, where privacy expectations are most heightened.’ This implies that although the curtilage does not benefit from the absolute protection afforded to the interior of the home, there

same protection to curtilage as the home itself, it has found manned aerial surveillance of curtilage outside the scope of Fourth Amendment protection. The manned aerial surveillance cases, most comparable to drone surveillance, can therefore give insight into the legality of drone surveillance under the Fourth Amendment. There are three main questions to consider when analyzing aerial surveillance of curtilage: First, was the surveillance conducted in airspace where the aircraft had a legal right to be under FAA regulations? Second, was the aircraft's flight at that particular altitude sufficiently rare, so as to violate reasonable expectations of privacy? Third, did the surveillance interfere with the defendant's use of the property—for example, by creating noise, wind, or dust?¹⁰⁷ Under the first and third factors, it seems likely that drone surveillance of curtilage would not warrant Fourth Amendment protection since drones will likely be in FAA approved airspace and there “already are UAVs that do not make detectable noise or wind even at nearly five feet.”¹⁰⁸ As to the second factor, with only 327 licenses issued for use in U.S. airspace as of February 2013,¹⁰⁹ drone surveillance might be sufficiently rare, so that such surveillance would violate an individual's reasonable expectations of privacy. But in several years, drones might be prevalent enough to pass *Katz* reasonableness standards.

So called “open fields” have traditionally been excluded from Fourth Amendment protection from searches because they “do not provide the setting for those intimate activities that the Amendment is intended to shelter from government interference or surveillance.”¹¹⁰ Therefore, it is unlikely drone surveillance conducted in open fields would violate the Fourth Amendment. However, depending on the pervasiveness of the surveillance, citizens worried about prolonged government tracking of their activities in public places might find solace if in the future the Court follows the logic of the *Jones* majority discussed *infra*.

2. Technology Used.—In addition to the location of a search, the technology used in a search might factor into a court's determination of the constitutionality of drone surveillance. In *Dow*, the Court seemingly found aerial surveillance with unsophisticated cameras lawful under the Fourth Amendment.¹¹¹ Noting that the device used was a standard mapmaking camera, and although it gave the government more information than could have been seen with the naked eye, the Court held that the camera did not reveal intimate activities to a level

is a close relationship between the two, and that technology directed at the home and its curtilage will be subjected to a more skeptical analysis than would be applied in a case involving open fields or industrial areas.”) (footnote omitted).

107 See *Florida v. Riley*, 488 U.S. 445, 451–52 (1989).

108 See *Roberts*, *supra* note 19, at 508 (footnote omitted).

109 *Fact Sheet — Unmanned Aircraft Systems (UAS)*, FED. AVIATION ADMIN. (Feb. 19, 2013), http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153.

110 *Oliver v. United States*, 466 U.S. 170, 179 (1984).

111 *Dow Chem. Co. v. United States*, 476 U.S. 227, 238–39 (1986).

necessary to warrant constitutional protection.¹¹² It opined that if the target was on private property, the equipment highly sophisticated and not in public use, the result might be different.¹¹³

Departing from the “results-based” methodology of *Katz*, which focused on individual privacy expectations despite the technological method used, *Dow* seemed to return to the technology-based approach of earlier cases. This suggests that the Court will look to the type of technology employed in drone surveillance to determine whether a Fourth Amendment violation has occurred.¹¹⁴ *Dow* requires that constitutional searches be enhanced only by technology in general public use, similar to the approach in *Kyllo*.¹¹⁵ This would suggest that for now, facial recognition technology, license plate scanners, and high-powered cameras used in conjunction with drone surveillance might be found unconstitutional.

However, considering the limiting language of *Dow* and *Kyllo*, drone surveillance may soon fall outside the realm of protection offered by current Fourth Amendment jurisprudence as these technologies and drones themselves become available to and used by the general public. Current Fourth Amendment jurisprudence, with its focus on the reasonable privacy expectations of society, might not be effective to protect society from drone surveillance as technological advances chip away at privacy norms. The Court seems aware of this emerging trend, as Justice Alito observed, joined by three other justices, in his *United States v. Jones* concurrence:

[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. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes. New technology may provide increased convenience or security at the expense of privacy, and many people may find the tradeoff worthwhile. And even if the public does not welcome the diminution of privacy that new technology entails, they may eventually reconcile themselves to this development as inevitable.¹¹⁶

Justice Alito hints at the best fix for this problem: “In circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative.”¹¹⁷

¹¹² *Id.* at 238.

¹¹³ *Id.*

¹¹⁴ See Roberts, *supra* note 19, at 514–15.

¹¹⁵ Compare *Kyllo v. United States*, 533 U.S. 27, 34 (2001) (“We think that obtaining by sense-enhancing technology any information regarding the interior of the home that could not otherwise have been obtained without physical ‘intrusion into a constitutionally protected area’ constitutes a search—at least where (as here) the technology in question is not in general public use.”) (citation omitted), with *Dow*, 476 U.S. at 238 (“It may well be, as the Government concedes, that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant.”)

¹¹⁶ *United States v. Jones*, 132 S. Ct. 945, 962 (2012) (Alito, J., concurring) (footnote omitted).

¹¹⁷ *Id.* at 964.

C. Proposed Legislative Solutions Are Inadequate

Several proposed bills are currently making their way through Congress, but perhaps the most comprehensive and promising is the Drone Aircraft Privacy and Transparency Act of 2013 (DAPTA), introduced by Congressman Edward J. Markey on March 19, 2013.¹¹⁸ DAPTA prescribes, among other things, the following:

- 1) The Secretary of Transportation shall establish procedures to integrate drones in the U.S. airspace in compliance with privacy principles.¹¹⁹
- 2) Applicants for drone operation licenses shall submit a “data collection statement” which includes the following information:
 - a) who will be operating the drone
 - b) specific locations the drone will be used
 - c) maximum time period of each flight
 - d) if data will be collected about individuals and if so, how data will be used, how long it will be retained, how it will be disposed of, and if and on what conditions it will be sold.
 - e) establish a system where citizens may inquire about violations, file complaints, and have data disposed of.¹²⁰
- 3) Applicants who are, or affiliated with, a law enforcement agency must also file a “data minimization statement” which includes:
 - a) minimize collection of data unrelated to warranted searches
 - b) require destruction of above info
 - c) establish procedures of destruction
 - d) audit procedures by applying agency to enforce compliance with statement.¹²¹
- 4) FAA shall publish a website containing all drone licenses, and information relevant to when, where, and how long

¹¹⁸ Drone Aircraft Privacy and Transparency Act of 2013, H.R. 2868, 113th Cong. (2013). DAPTA was reintroduced without substantive change by Congressman Peter Welch in the 1st Session of the 113th Congress, July 30, 2013.

¹¹⁹ *Id.* § 338.

¹²⁰ *Id.* § 339(b).

¹²¹ *Id.* § 339(c).

drones will be operated.¹²²

5) A warrant for government drone service shall be required, except when threats of imminent death, serious injury, or terrorist attack are present.¹²³

6) Use of unlawful evidence in courts shall be prohibited.¹²⁴

7) The Federal Trade Commission (FTC) will enforce regulations and can enact regulations to aid in enforcement.¹²⁵

8) There shall be available civil and private rights of action for violations of the act, including injunction and damages.¹²⁶

9) The Federal Aviation Administration shall have the power to revoke a drone operator's license for violations of the act.¹²⁷

Disconcertingly, DAPTA is overly broad in certain areas and vague in others. For DAPTA to be an effective safeguard against the diminishment of privacy due to domestic drone operation, it must be as complete and forward-looking as possible to minimize privacy violations. Several parts of DAPTA are not sufficiently thorough and prospective. For instance, the Act does not establish a uniform process for oversight and organization because it delegates the responsibility to would-be operators, thus dulling the Act's sharpest weapon in defense of privacy.¹²⁸ In another provision, DAPTA requires the FAA to post approved drone operation licenses on its website within ninety days if granted before the Acts enactment and "as soon as practicable" if granted after.¹²⁹ The vague wording of this section creates confusion in the law and opens the door to privacy violations. The purpose of posting approved drone operators and schedules to the public is transparency but this goal is pointless if rights have been irrevocably violated through confusion or disorganization.

DAPTA is a big step in the right direction towards ensuring privacy protections in the days of drone surveillance. However, it is incomplete because it overlooks several important areas of regulation that would ensure privacy protections, as discussed in the next section. It establishes privacy safeguards but fails to ensure proper application and enforcement. Amendments to DAPTA are necessary to ensure a solid foundation that will withstand domestic drone

¹²² *Id.* § 340.

¹²³ *Id.* § 341(a)–(b).

¹²⁴ *Id.* § 341(b)(6).

¹²⁵ *Id.* § 4(b)(2).

¹²⁶ *Id.* § 4(c)(1), (d)(1).

¹²⁷ *Id.* § 4(f).

¹²⁸ *Id.* § 339(c)(2).

¹²⁹ *Id.* § 340(b)(1)–(2).

use and other technological advancements that chip away at privacy.

III. PROPOSED APPROACH: BALANCING PRIVACY CONCERNS WITH INDUSTRY GROWTH THROUGH ONGOING AUDIT AND REPORTING PROCEDURES

The rapid expansion of drone technology and use renders Fourth Amendment privacy safeguards inadequate, necessitating federal legislative action. Congress has previously passed preemptive legislation to address potential privacy issues in the face of technological advances.¹³⁰ If proper privacy protections are not in place when the drone boom occurs, the legislature may not be able to respond fast enough to address infractions and civil rights concerns. If Congress does not act, privacy violations could occur without redress, privacy norms could be diminished, and society could become complacent. As one scholar noted, now is the time to establish a proper regulatory framework to address privacy concerns associated with domestic drone use.¹³¹

Additionally, such legislation might be a sufficient safeguard to appease the privacy advocates and the general public alike, so that the expansion of drone technology and the economic benefits associated with it can move forward unhindered. Currently, drone industry experts worry that legislative intervention will delay or possibly stifle economic and technological growth in the U.S. drone industry,¹³² citing such privacy concerns as “a distraction.”¹³³ Unless the industry gets serious about privacy, however, federal legislation might be the only way for industry experts and privacy enthusiasts to find common ground.

Some have argued for state and local, rather than federal, regulation of

130 See Electronic Communications Privacy Act of 1986, Pub. L. No. 99-508, 100 Stat. 1848 (codified as amended in scattered sections of 18 U.S.C. §§ 2701–2712 (2002)); Jason Koebler, *Drone Moans: Privacy Advocates Urge Drone Limits 'Before it's Too Late'*, U.S. NEWS & WORLD REP. (Jan. 15, 2013), <http://www.usnews.com/news/articles/2013/01/15/drone-moans> [hereinafter Koebler, *Drone Moans*] (statement of Orin Kerr) (“With the Electronic Communications Privacy Act of 1986, Congress was protecting people’s emails before most people knew what email was.”).

131 Ben Wolfgang, *Laws Urged to Curb Snooping by Drones*, WASH. TIMES (Jan. 15, 2013), <http://p.washingtontimes.com/news/2013/jan/15/experts-coming-drone-world-current-law-inadequate/> (statement of Orin Kerr) (“This is a natural space for Congress to step in and say that we have a new technology, and we’re worried about its privacy implications. Ultimately, we don’t have to accept new technologies and let them go and see how they work. We can try and regulate the privacy implications at the outset.”). In fact, one scholar believes that in order to realize the ultimate potential benefits of domestic drones, Congress needs to address the privacy issues initially to appease public concern and create an atmosphere receptive to drone innovation and application. See Ryan Calo, *As Drone Technology Advances, Who is Responsible?*, GLOBALPOST RIGHTS BLOG (Oct. 16, 2012, 5:38 PM), <http://www.globalpost.com/dispatches/globalpost-blogs/rights/drone-technology-privacy-liability-responsibility>.

132 Jason Koebler, *Drone Industry: Privacy 'Distractions' Could Have Major Economic Impacts*, U.S. NEWS & WORLD REP. (Mar. 13, 2013), <http://www.usnews.com/news/articles/2013/03/13/drone-industry-privacy-distractions-could-have-major-economic-impacts> [hereinafter Koebler, *Drone Industry*]; see also Anderson, *supra* note 6 (discussing the commercial potential of drones).

133 Koebler, *Drone Industry*, *supra* note 132.

drones,¹³⁴ opining these governmental bodies are better equipped to handle and react to the nuances of an emerging technology, but recent state drone legislation failures suggest otherwise.¹³⁵ Recently, many state drone regulation bills have been struck down as legislators vie to secure their states as FAA drone-testing sites. It is estimated that within the next few years domestic drone use will create over 70,000 jobs and generate \$82 billion.¹³⁶ One of the factors considered by the FAA when choosing test sites is the presence of “drone-restrictive” laws and state legislators have been hesitant to jeopardize their states’ chances at being selected.¹³⁷ After a North Dakota bill that would have banned police from warrantless use of drones was struck down, a state senator remarked, “Now that we’ve defeated that bill in the Senate, it sends a clear message to the FAA that North Dakota’s open for business”¹³⁸ Attitudes and remarks like this suggest that state and local governments cannot be counted on to protect privacy interests in the face of competing economic opportunity. Baseline federal privacy safeguards would sufficiently protect privacy interests and still allow for technological and economic growth in the drone industry.

IV. SPECIFIC REGULATORY RECOMMENDATIONS

Future federal regulation should be written to provide baseline privacy protections against government drone usage without being over-inclusive so as to stifle industry growth and its attendant economic benefits. Most important to this legislation are provisions that provide for transparency between the government operator and the public. Proposed solutions include operators supplying updated statements about the nature of the data being collected (e.g., purpose of surveillance, duration of surveillance, incidental data collected), a general statement of when and where such surveillance data will be collected, and this data subsequently being published to a website for public notice and review. Almost just as important is oversight through external audit procedures, which would work as a check on malfeasance. DAPTA includes several of the

134 See Margot E. Kaminski, *Drone Federalism: Civilian Drones and the Things They Carry*, 4 CALIF. L. REV. CIRCUIT 57, 57 (2013), http://www.californialawreview.org/assets/circuit/Kaminski_4_57.pdf (arguing standards for civilian drone use would be best established through a trial and error process by state governments, which could more effectively respond to drone technological advancements and capabilities than an overbroad blanket federal regulation); see also Liz Goodwin, *Privacy a Looming Issue as Drone Regulation Loosens*, YAHOO NEWS (May 30, 2013, 7:14 AM), <http://news.yahoo.com/blogs/ticket/privacy-looming-issue-drone-regulation-loosens-111425343.html>.

135 See Sean McElwee, *States “Race to the Bottom” on Drone Privacy*, MODERATE VOICE (May 7, 2013), <http://themoderatevoice.com/181175/states-race-to-the-bottom-on-drone-privacy/>.

136 DARRYL JENKINS & BIJAN VASIGH, ASS’N FOR UNMANNED VEHICLE SYS. INT’L, *THE ECONOMIC IMPACT OF UNMANNED AIRCRAFT SYSTEMS INTEGRATION IN THE UNITED STATES* 3-4 (2013), available at http://qzprod.files.wordpress.com/2013/03/econ_report_full2.pdf.

137 Luckerson, *supra* note 5.

138 *Id.*

safeguards necessary in any legislation to protect privacy but could be improved to address several shortcomings. With the following improvements, DAPTA could stand as a solid legislative framework to protect privacy standards and still allow for industry growth.

First and foremost, DAPTA is virtually silent on the issue of oversight in its implementation. For instance, DAPTA requires would-be drone operators to submit data collection and minimization statements outlining when, where, and how data will be collected; when and how long data will be retained; and how data will be disposed of, but fails to establish a reliable process for monitoring if operators are complying with these statements.¹³⁹ Though DAPTA does outline how the public can request information regarding the operator's drone usage, this process is not much better than the cumbersome one established by the Freedom of Information Act that currently controls drone transparency.¹⁴⁰

Continuing oversight by an objective agency is necessary to ensure DAPTA is being followed and standards are not being relaxed. Public monitoring may fail as an effective check on misfeasance and/or malfeasance—if the disclosure process is too burdensome or inconvenient, many citizens might forgo even trying to request information from the operators, weakening the disclosure process as an oversight tool.¹⁴¹ In addition, and perhaps more problematic, the clandestine nature of drone technology makes it difficult for citizens to monitor surveillance violations. It is impossible to complain about something that one is not aware is happening.¹⁴²

DAPTA should be amended to require operators to submit updates to report on their drone operations process. These reports should detail when information was collected, where it was collected, and when and how the

139 See Drone Aircraft Privacy and Transparency Act of 2013, H.R. 2868, 113th Cong. § 339(c) (2) (2013) (leaving audit procedures be adopted by the operating agency, but failing to proscribe the necessary regularity of such procedures or to consider potential conflicts of interest present in deferring audit procedures to the operating agency). Delegating the establishment of audit procedures to a sole governing agency would create uniformity, predictability, and reliability in audit procedures.

140 See Press Release, Congressman Ed Markey, Markey, Barton: Privacy Protections, Transparency a “Blind Spot” in FAA Oversight of Non-Military Domestic Drones (Nov. 29, 2012), *available at* <http://votesmart.org/public-statement/756018/markey-barton-privacy-protections-transparency-a-blind-spot-in-faa-oversight-of-non-military-domestic-drones#.Uh6DIGSG18N>.

141 Though DAPTA prescribes that operators provide contact information citizens can use to confirm “personally identifiable data” concerning them that has been collected, it fails to outline what constitutes a proper response time once a request for confirmation has been made. Drone Aircraft Privacy and Transparency Act of 2013, H.R. 2862, 113th Cong. § 339(b)(7) (2013). Similarly, DAPTA allows for an individual to obtain by request such data collected, if any, through a “reasonable process” and that such data be distributed in a “timely” manner but fails to prescribe what is a “reasonable process” and what constitutes a “timely” dispersal. *Id.* at § 339(b)(8). This imprecision could be problematic considering DAPTA has a two-year statute of limitations for private rights of action. *Id.* at § 4(d)(4).

142 David Nather, *Drones: Tough Talk, Little Scrutiny*, POLITICO (Feb. 9, 2013, 7:01 AM), <http://www.politico.com/story/2013/02/drones-tough-talk-little-scrutiny-87405.html>.

information was used and disposed of. This information should then be posted to the FAA (or other appropriate agency) website for public viewing. Also, the designated oversight agency should have to compile a report detailing the information gathering and disposal procedures of operators and submit such report yearly to Congress to ensure ongoing objective oversight.¹⁴³ Such monitoring requirements are necessary if legislative privacy safeguards are to be effective, as a recent report indicates.¹⁴⁴

Second, while the FTC is prescribed to enforce DAPTA,¹⁴⁵ other agencies, or even a wholly distinct agency, might be better equipped to monitor and ensure DAPTA compliance. As an already overburdened agency, the FTC might not be able to devote appropriate time and resources to monitoring DAPTA compliance in the face of an exponentially increasing amount of drone operators. Additionally, the FTC is not in the best position to enforce DAPTA because it lacks control as only a piece of DAPTA's implementation machinery, which compartmentalizes responsibility among various agencies and parties. For instance, under DAPTA, the Secretary of Transportation is in charge of rulemaking and approval of drone operation applications,¹⁴⁶ the FAA is in charge of disclosure of approved licenses,¹⁴⁷ and the FTC is in charge of compliance.¹⁴⁸ Another possibility is appointing the FAA to monitor and enforce DAPTA, since it is already tasked with publishing a list of operators approved by the Secretary of Transportation with their respective data collection and minimization statements on the FAA website.¹⁴⁹

Third, as part of ongoing oversight, DAPTA should require random external program audits of drone operators in accordance with government auditing standards.¹⁵⁰ Random audits would discourage malfeasance and verify the accuracy of operators' data collection and minimizations statements.¹⁵¹ While the above proposals (requiring operator reports and creating a workable administrative and oversight system) would promote transparency between

143 Congress requires a similar reporting standard of the Justice Department in its use of pen register and trap and trace order devices under the Electronic Communications Privacy Act of 1986. See Naomi Gilens, *New Justice Department Documents Show Huge Increase in Warrantless Electronic Surveillance*, ACLU FREE FUTURE BLOG (Sept. 27, 2012, 1:32 PM), <http://www.aclu.org/blog/national-security-technology-and-liberty/new-justice-department-documents-show-huge-increase>.

144 *Cf. id.* (discussing the Justice Department's repeated failures to comply with reporting requirements mandated under the Electronic Communications Privacy Act of 1986 and how these failures render privacy safeguards ineffective).

145 H.R. 2868 § 4(b).

146 *Id.* §§ 338–339.

147 *Id.* § 340(a).

148 *Id.* § 4(b).

149 *Id.* § 340(a).

150 U.S. GOV'T ACCOUNTABILITY OFFICE, GAO-12-331G, GOVERNMENT AUDITING STANDARDS 17-18 (2011), available at <http://www.gao.gov/assets/590/587281.pdf>.

151 *See id.*

the operators and the public, auditing would “provide a direct link between transparency and the credibility of the public sector entity.”¹⁵² Auditing ensures all of the information disclosed to the public about drone operational activities is honest and complete.¹⁵³ For example, if an operator reports that information gathered through a particular surveillance operation was destroyed on a specific date, the operator is aware that if audited, and his information does not correlate, he might face a lawsuit and forfeiture of his license. The persistent possibility of an audit encourages compliance with statutes and regulations even if U.S. residents become complacent due to changes in privacy norms.¹⁵⁴

Fourth, while DAPTA requires disclosure of the “specific locations in which the unmanned aircraft system will operate,”¹⁵⁵ it fails to account for the fact that operators inevitably change surveillance plans. DAPTA assumes the operators’ comprehensive understanding of their surveillance plans when they apply for a license. Therefore, the supposed “transparency” of the licensing process and data collection statement requirements is based on information that could change. DAPTA should be amended to require operators to supplement their data collection statements, which would detail any changes to drone deployment locations and times. The FAA should then post the changes to its website within a reasonable time. In order to protect fundamental principles of privacy, oversight must keep pace with fast growing technologies that challenge privacy.

CONCLUSION

Growth in the market for government and commercial drone use could result in worldwide expenditures of \$89.1 billion over the next decade.¹⁵⁶ For better or for worse, drones will soon be everywhere.¹⁵⁷ Current law is unprepared to protect Americans’ privacy from what will be a drone’s ever-watchful “eye in the sky.” However, a proper balance must be struck between privacy concerns and stifling growth and technological advancement in a fledgling drone industry. Federal legislation could offer a solution, and an amended DAPTA could provide a decent model. In order for us to realize the full potential of drones we must address privacy issues right from the start.¹⁵⁸ If Congress allays concerns

152 INST. OF INTERNAL AUDITORS, SUPPLEMENTAL GUIDANCE: THE ROLE OF AUDITING IN PUBLIC SECTOR GOVERNANCE II (2d ed. 2012), https://na.theiia.org/standards-guidance/Public%20Documents/Public_Sector_GovernanceI_1_.pdf.

153 *See id.*

154 *See id.* at 15.

155 H.R. 2868 § 339(b)(2).

156 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 2 (2012), available at <http://www.gao.gov/assets/650/648348.pdf> (citing TEAL GRP. CORP., WORLD UNMANNED AERIAL VEHICLE SYSTEMS (2012)).

157 *See* FED. AVIATION ADMIN., *supra* note 4.

158 Calo, *supra* note 131.

before there is a problem, the drone boom will be met by a social and political climate more receptive to drones and their potential for positive results. The time to address drone privacy is now. “[T]he technologies are still visible. In 10 years, they’ll be small, they’ll be everywhere, it’ll be too late.”¹⁵⁹ As the law stands now, citizens are left asking themselves “who watch the watchmen?”¹⁶⁰

¹⁵⁹ Koebler, *Drone Moans*, *supra* note 130 (statement of Bruce Schneier).

¹⁶⁰ The Latin phrase *quis custodiet ipsos custodes?*, “who will keep the keepers themselves?” is also sometimes translated as in the text. *Quis Custodiet Ipsos Custodes?*, MERRIAM WEBSTER, <http://www.merriam-webster.com/dictionary/quis%20custodiet%20ipsos%20custodes> (last visited Oct. 22, 2013).