# *Notes*

# Policing the Police: Balancing the Right to Privacy Against the Beneficial Use of Drone Technology

JENNIFER M. BENTLEY[†]

*The cost of buying, operating, and maintaining manned aircraft traditionally limited the government's ability to conduct widespread aerial surveillance. But drone technology is eroding this natural limit because they are cheaper, stealthier, and can be used as a platform for other powerful surveillance tools. Drones are ideally suited for numerous law enforcement tasks such as search and rescue, crime scene investigations, and gaining a bird's-eye view in dangerous active shooter or hostage situations. Privacy rights advocates fear that drone capabilities are bringing us closer to a "surveillance society" in which our every move is monitored, recorded, and scrutinized by the government, and have led the fight to either require police to obtain a warrant before using a drone or to ban the use of drones altogether. At the federal government level, only the FAA regulates drones but the Agency considers privacy outside the scope of its authority. Approximately one-third of states require law enforcement to obtain a warrant prior to using a drone to conduct a search or surveillance. A handful of local governments have banned the use of drones by law enforcement entirely in response to privacy concerns. However, overly broad restrictions on drone use have an unintended consequence in that they also curtail non-invasive, beneficial uses of drones. The Fourth Amendment likely does not protect individuals from warrantless drone surveillance provided the drone does not physically trespass and only captures what is visible from public airspace. This Note considers the twin harms of a surveillance society and depriving law enforcement of the beneficial uses of drones and concludes that states, as the laboratories of democracy, must act to reign in the use of unmanned aircraft by law enforcement so that public backlash against the threat to privacy does not result in the total deprivation of this useful technology.*

[†] J.D. Candidate 2019, University of California, Hastings College of the Law; Senior Articles Editor, *Hastings Law Journal*. The Author gratefully acknowledges Professor Eumi K. Lee for her invaluable feedback and suggestions and the Notes team for their diligent efforts. This Note is dedicated to Robert Whitburn for his unflagging support and to my family who listened to me drone on about privacy for months.

TABLE OF CONTENTS

## INTRODUCTION

Drones are swiftly gaining popularity in the United States. In 2016, the Federal Aviation Administration (FAA) estimated there were already 2.5 million drones being flown regularly in the United States, with that number expected to rise to 7 million by 2020.[1] Drones are cheaper, smaller, and stealthier than traditional piloted aircraft, making them a popular tool in the hands of law enforcement[2] and raising concerns for privacy advocates.[3] In light of this new technology, it is vital to balance the public's privacy interests against the numerous beneficial applications of drone technology.[4]

In the hands of law enforcement, drones can be used in a variety of ways which range from innocuous to highly invasive. For example, drones are uniquely capable of assisting with search and rescue operations, accident reconstruction, crime scene investigation, and providing a bird's eye view in dangerous active shooter or hostage situations.[5] However, drones are also potent tools that can be used to invade privacy and conduct highly intrusive surveillance.[6] Because the use of drone surveillance implicates the Fourth Amendment's protection against unreasonable searches, clear guidelines are essential to ensuring the continued and effective use of the powerful technology.[7] In fact, public suspicion and fear surrounding the use of drones by law enforcement has led some municipalities to close the door on all drone use, thus denying local agencies a beneficial tool that could assist in rapidly evolving or dangerous situations.[8]

Clear, strict mandates for permissible use of drones by law enforcement are necessary to ensure continued access for beneficial purposes and to safeguard privacy rights. All levels of government have attempted to regulate law

---

1. Kelsey D. Atherton, *The FAA Says There Will Be 7 Million Drones Flying over America by 2020* POPULAR SCI. (Mar. 24, 2016), https://www.popsci.com/new-faa-report-stares-in-face-drone-filled-future. The Author was unable to locate predictions for the number of law enforcement drones by 2020, but the FAA forecasts that two percent of the estimated 2.7 million commercial (non-hobbyist) drones by that time will belong to the government. FED. AVIATION ADMIN., FAA AEROSPACE FORECAST FISCAL YEARS 2016–2036, at 31, 33, https://www.faa.gov/data_research/aviation/aerospace_forecasts/media/FY2016-36_FAA_Aerospace_Forecast.pdf (last visited Nov. 21, 2018).

2. Office of Cmty. Oriented Policing Servs., U.S. Dep't of Justice, *Unmanned Aircraft Systems (UAS) Guidebook in Development*, COMMUNITY POLICING DISPATCH (Aug. 2014) https://cops.usdoj.gov/html/dispatch/08-2014/uas_guidebook_in_development.asp [hereinafter *Unmanned Aircraft Systems*].

3. *See* Michael J. Schoen & Michael A. Tooshi, *Confronting the New Frontier in Privacy Rights: Warrantless Unmanned Aerial Surveillance*, 25 AIR & SPACE L., no. 3, 2012, at 2.

4. *Id*. at 19.

5. *Unmanned Aircraft Systems*, *supra* note 2.

6. Schoen & Tooshi, *supra* note 3, at 18 (noting that drones have greater potential to invade privacy than manned aircraft and can be outfitted with sophisticated surveillance technology).

7. *Cf.* United States v. Knotts, 460 U.S. 276, 283–84 (1983) (recognizing that if Respondent's argument that twenty-four-hour surveillance of citizens "without judicial knowledge or supervision" comes to fruition, there may be a need to reexamine whether "different constitutional principles may be applicable").

8. *See, e.g.*, Christine Clarridge, *Seattle Grounds Police Drone Program*, SEATTLE TIMES, https://www.seattletimes.com/seattle-news/seattle-grounds-police-drone-program (last updated Feb. 8, 2013, 8:52 AM).

enforcement's use of drones. Federal actions thus far have failed,[9] but eighteen states have passed laws regulating drone use and attempting to protect individuals from warrantless surveillance or searches.[10] At least a half-dozen local governments have also enacted ordinances regulating law enforcement use of drones.[11]

Where the legislature is silent, courts are left to interpret whether current Fourth Amendment doctrine protects individuals from warrantless drone surveillance. There is a noticeable absence of case law examining the constitutionality of drone surveillance, but lower courts applying Fourth Amendment doctrine to similar surveillance issues are reaching inconsistent results.[12] These opinions demonstrate a lack of clear consensus. While the Supreme Court typically does adapt to emerging technologies and often decides in favor of individual rights,[13] it is usually a slow process and a case involving drone surveillance is unlikely to reach the high court for many years.[14] For these reasons, states should enact laws providing law enforcement with clear, strict guidelines for drone usage that protect individual privacy and preserve this technology as a valuable tool in local law enforcement's arsenal.

Part I of this Note presents an overview of drone capabilities, detailing how law enforcement is currently using the technology, with a focus on how the relatively low cost of drones is eroding a natural limit on law enforcement's prior use of aerial surveillance. Part I also surveys various attempts to regulate drone usage by federal, state, and local actors.

Part II provides a brief overview of the Court's current aerial surveillance and high-tech surveillance jurisprudence and then explores how lower courts are interpreting and applying these doctrines. Because the Court has not considered an aerial surveillance case for almost thirty years (prior to the advent of drones), the doctrine is ill-suited to the twenty-first century.[15] And even though the Court has more recently decided high-tech surveillance cases,[16] current Fourth

9. *See infra* Subpart I.D.1.

10. *2017 Unmanned Aircraft Systems (UAS) State Legislation Update*, NAT'L CONF. ST. LEGISLATURES (Jan. 17, 2018), http://www.ncsl.org/research/transportation/2017-unmanned-aircraft-systems-uas-state-legislation-update.aspx [hereinafter *2017 UAS State Legislation Update*].

11. ARTHUR HOLLAND MICHEL, CTR. FOR THE STUDY OF THE DRONE, LOCAL AND STATE DRONE LAWS 2 (2017), http://dronecenter.bard.edu/state-and-local-drone-laws.

12. *See infra* Subpart II.C.

13. *See, e.g.*, Carpenter v. United States, 138 S. Ct. 2206, 2217–20 (2018) (holding that the government's acquisition of cell-site location information constitutes a search under the Fourth Amendment).

14. For an example of the Supreme Court's slow response to emerging technology, see United States v. Jones, 565 U.S. 400, 405–06 (2012) (noting that the Court's position on wiretaps evolved from holding in *Olmstead v. United States*, 277 U.S. 438 (1928), that wiretaps did not constitute a Fourth Amendment search, to *Katz v. United States*, 389 U.S. 347, 351 (1967), where the Court held an eavesdropping device in a public telephone booth violated the Fourth Amendment). Indeed, while *Jones* effectuated a major shift in recognizing that the Fourth Amendment protects people, and not places, this shift took nearly four decades.

15. The last aerial surveillance case the Court decided was *Florida v. Riley*, 488 U.S. 445 (1989).

16. *See, e.g.*, *Carpenter*, 138 S. Ct. 2206 (involving cell-site location information); *Jones*, 565 U.S. 400 (involving GPS monitoring); Kyllo v. United States, 533 U.S. 27 (2001) (involving thermal imaging technology).

Amendment doctrine alone is insufficient to address the technological developments that could lead to widespread surveillance. Part II also considers the flawed logic in police department policies and statutes that expressly require law enforcement to obtain a warrant before using drones when required by the Fourth Amendment, given the fact that the applicability of the warrant requirement in this context remains unsettled.

In Part III, this Note proposes that state legislatures are in the best position to expediently enact laws that balance the public safety benefits of drone use against privacy. Specifically, states can and should experiment with how best to safeguard privacy interests, but all such legislation should include: (1) specific parameters for the circumstances under which law enforcement may use drones; (2) limits on data retention; (3) a policy that renders data collected in violation of the statute inadmissible; and (4) limits on sense-enhancing technology that may be placed on a drone.

## I. BACKGROUND

### A. INTRODUCTION TO DRONES

Unmanned aerial vehicles (UAV),[17] or, unmanned aerial systems (UAS) are unpiloted aircraft or spacecraft, more commonly known as drones.[18] UAV is the term for the vehicle itself, while UAS refers to the entire system, which is comprised of the vehicle, ground control station with pilot, communications, and support.[19] UAS are used by the military, government, and law enforcement because they present benefits over piloted aircraft since they neither risk the lives of pilots, nor do the drones need rest.[20]

Drones are also used by non-governmental actors, from hobbyists to commercial enterprises. Flying drones as a hobby is gaining in popularity, with an estimated 1.5 million hobby drones in the United States in 2016.[21] Moreover, commercial companies are developing and testing drones to deliver everything

17. Elizabeth Howell, *What Is a Drone?* SPACE.COM (Oct. 3, 2018, 2:32 PM), https://www.space.com/29544-what-is-a-drone.html.

18. The FAA refers to drones as unmanned aircraft systems (UAS). *Unmanned Aircraft Systems (UAS) Frequently Asked Questions*, FED. AVIATION ADMIN., https://www.faa.gov/uas/faqs (last visited Nov. 21, 2018).

19. *What Is the Difference Between a UAV and UAS?*, DART DRONES (Jan. 27, 2016), https://www.dartdrones.com/blog/difference-between-uav-and-uas.

20. *Id.*; *see also* Josh Reyes, *Drones Becoming More Common in Peninsula Law Enforcement, Fire and Rescue Agencies*, DAILY PRESS (Jan. 11, 2018, 5:15 PM), http://www.dailypress.com/news/york-county/dp-nws-evg-york-county-sheriff-fire-drone-20171206-story.html (describing how a drone can assist local police officers by providing information and visuals in situations where a subject is barricaded in a building without endangering officers).

21. Atherton, *supra* note 1.

from packages[22] and pizza[23] to blood and pathology samples.[24] Farmers are using drones to gain an aerial view of crops and to better analyze the effectiveness of their growing processes.[25] Scientists use drones to conduct research, such as measuring climate change, studying atmospheric conditions during solar eclipses, and monitoring the health of the rainforest in the Amazon.[26]

Drones can be as large as traditional, manned aircraft[27] or as small as hummingbirds.[28] Smaller versions are both lightweight and highly agile,[29] able to maneuver quietly into tight spaces.[30] A hobbyist illustrated the unprecedented agility and capability of these aircraft to penetrate even the most sacred of spaces when he landed a $400 remote-controlled helicopter on the White House grounds in 2015.[31] Researchers at universities and technology companies continue to advance drone technology, improving modes of flight, flight range, endurance, and carrying capacity.[32] For example, university researchers developed a small drone that "flies like a bat," which could potentially lead to "aircraft that are lighter, quieter and have a longer endurance."[33] By virtue of

22. *See, e.g.*, *Amazon Prime Air*, AMAZON, https://www.amazon.com/Amazon-Prime-Air/b?node=8037720011 (last visited Nov. 21, 2018).

23. David Reid, *Domino's Delivers World's First Ever Pizza by Drone*, CNBC, https://www.cnbc.com/2016/11/16/dominos-has-delivered-the-worlds-first-ever-pizza-by-drone-to-a-new-zealand-couple.html (last updated Nov. 16, 2016, 9:02 AM).

24. *Matternet Unveils the Matternet Station*, CISION: PR NEWSWIRE (Sept. 20, 2017), https://www.prnewswire.com/news-releases/matternet-unveils-the-matternet-station-300522496.html.

25. Press Release, AeroVironment, AeroVironment Automated Quantix Hybrid Drone and AV Decision Support System Now Available; A Powerfully Simple-to-Use and Fully Integrated Drone and Data Processing Solution Delivering Actionable Intelligence for the Farm (Jan. 31, 2018), http://www.avinc.com/resources/press-releases/view/aerovironment-automated-quantix-hybrid-drone-and-av-decision-support-system.

26. DAN GETTINGER & ARTHUR HOLLAND MICHEL, CTR. FOR THE STUDY OF THE DRONE, DRONE YEAR IN REVIEW: 2017, at 13 (2018), http://dronecenter.bard.edu/drone-year-in-review-2017.

27. For example, the U.S. Navy's Triton UAS has a 130-foot wingspan and would "provide high-altitude, real-time intelligence, surveillance and reconnaissance" for up to twenty-four hours at a time. Allen McDuffee, *Navy's 757-Sized Drone Will Provide Big-Time Surveillance*, WIRED (Jan. 7, 2014, 1:37 PM), https://www.wired.com/2014/01/triton.

28. W.J. Hennigan, *It's a Bird! It's a Spy! It's Both*, L.A. TIMES (Feb. 17, 2011), http://articles.latimes.com/2011/feb/17/business/la-fi-hummingbird-drone-20110217 (reporting on the development of a drone with the appearance of a hummingbird).

29. *Id.* (noting that the "hummingbird-like" drone is equipped with a video camera, weighs less than a AA battery, and is able to "hover and fly sideways, backward and forward, as well as go clockwise and counterclockwise").

30. *Drones in Surveillance and Security*, JETLABS, http://jetlabs.info/applications/surveillance-and-security (last visited Nov. 21, 2018).

31. Kevin Poulsen, *Why the US Government Is Terrified of Hobbyist Drones*, WIRED (Feb. 5, 2015, 5:15 AM), https://www.wired.com/2015/02/white-house-drone. Following the incident, where the hobbyist reportedly lost control of the helicopter, the manufacturer of the popular aircraft voluntarily pushed out a mandatory firmware update for the model which would prevent it from flying within a 15.5-mile radius of the White House. This term is called geofencing, and is not foolproof, as it is likely still prone to hacking. *Id.*

32. GETTINGER & MICHEL, *supra* note 26, at 12–13.

33. *Id.* at 12.

their design, size, and unique flight capabilities, UAS "can operate undetected in urban and rural environments."[34]

## B. LAW ENFORCEMENT DRONE CAPABILITIES AND TYPICAL USES

Because drones have unique capabilities, are affordable, and can be operated without risk of harm to the pilot, law enforcement agencies are increasingly turning to UAS to provide them with aerial views.[35] Whereas the cost of buying, operating, and maintaining manned aircraft traditionally limited the government's ability to conduct aerial surveillance on a widespread or regular basis, drones are rapidly changing the equation.[36] According to the American Civil Liberties Union (ACLU), "[n]ow that surveillance can be carried out by unmanned aircraft, this natural limit is eroding."[37] Prior to implementing UAS, police could only gain an aerial view by using helicopters[38] or airplanes.[39] Manned aircraft were not a feasible option for many law enforcement agencies, except in rare situations. Helicopters are not widely available,[40] are costly to operate and maintain, and are too noisy to use in sensitive situations.[41] In contrast to a helicopter or plane that comes with a price tag of $500,000 to $3,000,0000,[42] drones can cost as little as $2,000,[43] travel in excess of 100 miles

34. *Domestic Unmanned Aerial Vehicles (UAVs) and Drones*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/drones (last visited Nov. 21, 2018).

35. *See* Schoen & Tooshi, *supra* note 3, at 1, 2.

36. JAY STANLEY & CATHERINE CRUMP, PROTECTING PRIVACY FROM AERIAL SURVEILLANCE: RECOMMENDATIONS FOR GOVERNMENT USE OF DRONE AIRCRAFT 1 (2011), https://www.aclu.org/report/protecting-privacy-aerial-surveillance-recommendations-government-use-drone-aircraft.

37. *Id.*

38. *Drones in Surveillance and Security*, *supra* note 30.

39. *See, e.g.*, California v. Ciraolo, 476 U.S. 207 (1986) (law enforcement used private plane to conduct aerial surveillance of suspect's backyard); People v. Mayoff, 729 P.2d 166, 173 n.5 (Cal. 1986) (plane that discovered marijuana cultivation flew over the property on two occasions at an altitude of 1,000 feet).

40. *Drones in Surveillance and Security*, *supra* note 30.

41. *Id.*

42. Jay Stanley, *We Already Have Police Helicopters, So What's the Big Deal over Drones?*, ACLU: FREE FUTURE (Mar. 8, 2013, 11:26 AM), https://www.aclu.org/blog/mass-incarceration/we-already-have-police-helicopters-so-whats-big-deal-over-drones. Not only do manned aircraft cost more to acquire, they cost 200 to 800 dollars-per-hour to operate and require highly trained pilots, co-pilots, ground crew, and runways or helipads. *Id.*; *see also* Skyler Swisher, *Palm Beach County Sheriff's Office to Receive $1M in State Funding for Drone Program*, SUN SENTINEL (Mar. 18, 2016, 5:30 PM), http://www.sun-sentinel.com/local/palm-beach/fl-palm-sheriff-drones-20160318-story.html (stating it costs about 800 dollars per hour to operate one of its manned ships).

43. The most popular drones for public safety use are the DJI Phantom and DJI Inspire, which start at 2,000 dollars or less. *See* DAN GETTINGER, CTR. FOR THE STUDY OF THE DRONE, DRONES AT HOME: PUBLIC SAFETY DRONES 3, 4 (2017), http://dronecenter.bard.edu/public-safety-drones; *see also Inspire 1 V2.0*, DJI STORE, https://store.dji.com/product/inspire-1-v2?site=brandsite (last visited Nov. 11, 2018) (offering the Inspire 1 V.20 model for 1,999 dollars); *Phantom 4 Pro V2.0*, DJI STORE, https://store.dji.com/product/phantom-4-pro-v2?pbc=Ph17Whbx&utm_source=performancehorizon&utm_medium=text&utm_campaign=phantom-4-pro&Phclickrefb=1100l5EsJrfq&vid=43151 (last visited Nov. 21, 2018) (DJI Phantom 4 Pro V2.0 model costs 1,499 dollars); Michael De Yoanna, *How Mesa County Used Drones in Search and Rescue Efforts After Landslide*, COLO. PUB. RADIO (June 5, 2014), http://www.cpr.org/news/story/how-mesa-county-used-drones-

per hour,[44] and allow first responders to arrive on scene faster[45] and go unnoticed.[46] For law enforcement, the relatively low cost of UAS adds to their appeal. For example, the DJI Matrice 600 has a base price of $4,999,[47] but when outfitted "with all its bells and whistles [extra batteries which allow it to fly up to twelve hours and camera], costs about $25,000."[48]

A 2017 study showed exponential growth, finding that 347 state and local police, sheriff, fire, and emergency units have acquired drones since 2009, with more units acquired in 2016 than in all previous years combined.[49] Drones enable police to have an "eye in the sky," able to fly continuously for up to twenty-four hours with real-time monitoring from the ground.[50] Not only are drones within most law enforcement budgets, departments can even fund their acquisition through grants from the Department of Homeland Security ("DHS"),[51] donations,[52] or civil forfeiture funds.[53] Drones also put aerial surveillance within the reach of smaller departments that would not have resources to conduct manned aerial missions. Of the 347 known departments that have acquired drones, almost half served populations of 50,000 people or less.[54] Indeed, a department serving a small community is unlikely to have the

search-and-rescue-efforts-after-landslide (describing how drones can be deployed at a "much lower cost" than helicopters).

44. Swisher, *supra* note 42.

45. Joe Fisher, *All the Buzz: How Drones Are Keeping Communities Safe*, WAVY-TV (June 12, 2017, 8:29 AM), http://wavy.com/2017/06/12/all-the-buzz-how-drones-are-keeping-the-communities-safe.

46. Jeff Brown, *Taking to the Air: Drones and Law Enforcement*, DOVER POST (Dec. 13, 2017, 7:40 AM), http://www.doverpost.com/news/20171213/taking-to-air-drones-and-law-enforcement.

47. *Matrice 600 Pro*, DJI STORE, https://store.dji.com/product/matrice-600-pro (last visited Nov. 21, 2018).

48. Reyes, *supra* note 20. DJI supplies sixty-eight percent of all drones to public safety agencies in the United States. Sidney Fussell, *Who Will Police Police Drones?*, GIZMODO (July 11, 2018, 12:40 PM), https://gizmodo.com/who-will-police-police-drones-1826891119.

49. GETTINGER, *supra* note 43, at 3. Although the Federal Bureau of Investigation admits to using drones for surveillance on U.S. soil, such use appears to be minimal, therefore, this Note focuses on use by state and local law enforcement. SARA LOVE, ACLU OF MD., SURVEILLANCE IN THE FREE STATE: ELECTRONIC COMMUNICATIONS, LOCATION TRACKING, AUTOMATIC LICENSE PLATE READERS, DRONES AND FACIAL RECOGNITION 11 (2014) (on file with author).

50. Reyes, *supra* note 20; s*ee also* Swisher, *supra* note 42 (reporting flight times of up to twenty-four hours per mission).

51. U.S. DEP'T OF HOMELAND SEC., FISCAL YEAR 2008–2015 LAW ENFORCEMENT TERRORISM PREVENTION ACTIVITY FUNDING (2016), https://www.fema.gov/media-library/assets/documents/124176; *see also* Kimberly Dvorak, *Homeland Security Increasingly Lending Drones to Local Police*, WASH. TIMES (Dec. 10, 2012), http://www.washingtontimes.com/news/2012/dec/10/homeland-security-increasingly-loaning-drones-to-l (discussing the Department of Homeland Security's distribution of four million dollars in grants to local law enforcement agencies for drone purchases). For an overview of how local law enforcement agencies are able to obtain surveillance technology, often without elected leaders' and the public's awareness, through federal procurement, see Catherine Crump, *Surveillance Policy Making by Procurement*, 91 WASH. L. REV. 1595, 1608 (2016).

52. The New York State Trooper Foundation donated sixteen drones to support New York State Police. Press Release, Governor Andrew M. Cuomo, N.Y. State, Governor Cuomo Announces Deployment of First State Police Aerial Drone Systems (Jan. 10, 2018), https://on.ny.gov/2qQynQB.

53. GETTINGER, *supra* note 43, at 5.

54. *Id.* at 3.

resources for manned aircraft. For example, one small county in Virginia[55] has three drones in its arsenal of tools to dispatch in emergency situations.[56] The county's sheriff's office and fire department teamed up to man a twelve-person team, which operates out of a mobile command center housed in a trailer.[57] Each drone carries both an optical zoom camera that allows first responders to see details when the drone is up to a quarter mile away from its target, and another with thermal imaging that the team says allows it to see through smoke during fires and through trees during search and rescue operations.[58] "York County's never getting a helicopter," said one fire official. "But we can do this."[59]

The main utility of UAS for law enforcement is derived from serving as a platform for surveillance technology.[60] Drones can be outfitted with cameras with zoom lenses, infrared thermal imagers, wireless network sniffers to intercept cell phone calls,[61] license plate readers, and laser radar.[62] These tools allow police to record and stream high-quality video, penetrate password-protected Wi-Fi networks, and record phone conversations and text messages.[63] Thermal imagers allow police to "see" heat signals through walls, trees, or smoke in real-time.[64] License plate readers scan and store the plate number, date, time and GPS location of vehicles.[65]

With the increased access, law enforcement agencies are using UAS for a variety of purposes: to survey damage and search for survivors following natural

55. York County, Virginia covers 106 square miles and has 67,837 residents. YORK CTY. VA. ECON. DEV., https://www.yesyorkcounty.com (last visited Nov. 21, 2018). While York County's population exceeds 50,000, it is characterized as a "small county" by the U.S. Census Bureau because its population is less than 500,000. Haya El Nasser, *More than Half of U.S. Population in 4.6 Percent of Counties*, U.S. CENSUS BUREAU (Oct. 24, 2017), https://www.census.gov/library/stories/2017/10/big-and-small-counties.html.

56. Fisher, *supra* note 45.

57. *Id.*

58. *Id.* ("You can be a quarter of a mile out with that camera on it, with that lens and get as detailed as you want to without having to be over top of them." (comment of Deputy Ron Montgomery)). Thermal imaging is not only useful for seeing through smoke in fires, but also for seeing through walls based on the level of heat projected by objects. *See* RICHARD M. THOMPSON II, CONG. RESEARCH SERV., R42701, DRONES IN DOMESTIC SURVEILLANCE OPERATIONS: FOURTH AMENDMENT IMPLICATIONS AND LEGISLATIVE RESPONSES 3 (2013).

59. Reyes, *supra* note 20.

60. *Id.*

61. *Id.*

62. *See* THOMPSON II, *supra* note 58; *see also* Angela Woodall, *Alameda County Sheriff Plans to Buy a Surveillance Drone*, MERCURY NEWS (Oct. 19, 2012, 12:18 AM), https://www.mercurynews.com/2012/10/19/alameda-county-sheriff-plans-to-buy-a-surveillance-drone.

63. Andy Greenberg, *Flying Drone Can Crack Wi-Fi Networks, Snoop on Cell Phones*, FORBES (July 28, 2011, 2:11 PM), https://www.forbes.com/sites/andygreenberg/2011/07/28/flying-drone-can-crack-wifi-networks-snoop-on-cell-phones/#40d4e4707856; *Surveillance Drones*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/issues/surveillance-drones (last visited Nov. 21, 2018).

64. *Zenmuse-XT*, DJI, https://www.dji.com/zenmuse-xt (last visited Nov. 21, 2018).

65. Lyndsay Winkley, *8 Ways Police Can Spy on Crime, and You*, SAN DIEGO UNION-TRIB. (May 21, 2015, 4:14 PM), http://www.sandiegouniontribune.com/sdut-police-technology-devices-surveillance-privacy-2015may21-story.html.

disasters,[66] take photos and reconstruct crime scenes,[67] reconstruct accidents,[68] locate missing persons,[69] gain a bird's eye view in active shooter situations,[70] apprehend suspects,[71] scout homes prior to serving high-risk search warrants,[72] and monitor railroad tracks for trespassers.[73] In natural disasters or search and rescue operations, drones can be used in situations where it would be too risky to send in officers or volunteers.[74] For example, when a body was spotted in the Ohio River and it was running too swiftly to send rescuers, police used a UAV instead.[75] The drone recorded such high-quality video of the body that the victim's family was able to identify it by the tattoo markings, even though the body was never recovered.[76] Thus, where a manned recovery was impossible, the use of drone technology was able to provide the victim's family with closure.[77]

UAS are also uniquely well-suited to assist with photographing crime scenes and reconstructing accidents. As of April 2018, New York State Police had eighteen drones for use in reconstructing accidents and documenting crime scenes.[78] According to Governor Andrew M. Cuomo's office, UAS can document and reconstruct serious motor vehicle accidents in less time than other methods, reducing the time that roads are closed for investigation.[79] The Governor predicted that UAS "will improve emergency response, improve

66. De Yoanna, *supra* note 43.

67. Nancy Lofholm, *Look to the Skies in Mesa County for the Police Drone Frontier*, DENVER POST (Oct. 19, 2013, 1:50 PM), https://www.denverpost.com/2013/10/19/look-to-the-skies-in-mesa-county-for-the-police-drone-frontier.

68. Press Release, Governor Andrew M. Cuomo, *supra* note 52.

69. *See, e.g.*, Chris Aadland, *Catching Up: Madison Police Say Using Drones Has Helped the Department*, WIS. ST. J. (Jan. 22, 2018), http://host.madison.com/wsj/news/local/ask/catching-up/catching-up-madison-police-say-using-drones-has-helped-the/article_8ff0c737-227f-564f-9287-20ad3bb5271e.html.

70. L.A. POLICE DEP'T, SMALL UNMANNED AERIAL SYSTEM PILOT PROGRAM DEPLOYMENT GUIDELINES AND PROCEDURES 3 (2017), http://assets.lapdonline.org/assets/pdf/2017.10.17%20-%20APPROVED%20FINAL%20-%20sUAS%20Guidelines.pdf.

71. *See* Lofholm, *supra* note 67; *see also* Joe Douglass, *ACLU Raises Privacy Concerns After Sheriff's Office Exhibits Drone on Facebook*, KATU NEWS (July 17, 2017), http://katu.com/news/local/aclu-raises-privacy-concerns-after-sheriffs-office-exhibits-drone-on-facebook.

72. Grant Schulte, *Nebraska Bill Would Criminalize Drone Use to Spy on People, Harass Cows*, INS. J. (Jan. 8, 2018), https://www.insurancejournal.com/news/midwest/2018/01/08/476599.htm.

73. Chris Chase, *Brunswick Council Gets First Look at Police Policy on Drone Use*, PORTLAND PRESS HERALD (Jan. 16, 2018), https://www.pressherald.com/2018/01/16/brunswick-council-gets-first-look-at-police-policy-on-drone-use.

74. *See, e.g.*, De Yoanna, *supra* note 43 (reporting that drones "played a key role in an exhaustive search" to recover the bodies of three men after a massive landslide). York County has used its drones to monitor storm damage and says the thermal imaging will help it see through smoke and trees to aid in search in rescue operations. Fisher, *supra* note 45.

75. Margaret Smykla, *Game of Drones: Eyes in the Sky Can Be Functional, Fun to Fly*, PITTSBURGH POST-GAZETTE (Mar. 22, 2018, 9:41 AM), http://www.post-gazette.com/business/tech-news/2018/03/22/Drones-recreational-commercial-David-Uhrinek/stories/201803150003.

76. *Id.*

77. *See id.*

78. Press Release, Governor Andrew M. Cuomo, *supra* note 52.

79. *Id.*

operational and cost efficiencies and increase Trooper safety."[80] In other localities, drones are being used to shoot crime scene video, which is used not only for investigations,[81] but also to allow jurors to view scenes in their entirety, rather than in still photos.[82]

### C. PUBLIC RESPONSE/BACKLASH TO SURVEILLANCE CAPABILITIES

Given the capabilities of drones, routine aerial surveillance would profoundly alter the character of life in the United States.[83] Privacy advocates like the ACLU,[84] the Electronic Frontier Foundation (EFF), and the Electronic Privacy Information Center (EPIC) have warned that drones are capable of virtually eliminating privacy and creating a surveillance society.[85] When people know the government is watching, they alter their behavior and self-censor.[86] And with good reason—a 2010 ACLU study detailed how "Americans have been put under surveillance or harassed . . . just for deciding to organize, march, protest, espouse unusual viewpoints and engage in normal, innocuous behaviors such as writing notes or taking photographs in public."[87] The technical capabilities of drones and their threat to privacy should not be evaluated as a single tool, but as they fit into the larger picture of surveillance and information gathering.[88] Law enforcement's use of drones also poses the threat of "mission creep" which is using the technology for purposes other than what was originally proposed.[89] "Once a surveillance and data storage infrastructure is in place, however, the temptation to use it for other purposes can prove irresistible."[90]

In 2011, the ACLU published a report on drone use calling for "a system of rules to ensure that we can enjoy the benefits of this technology without bringing us a large step closer to a 'surveillance society' in which our every move is monitored, tracked, recorded, and scrutinized by the authorities," and outlining specific recommendations for use by law enforcement.[91] At the time

80. *Id.* (quoting Governor Cuomo).

81. Douglass, *supra* note 71.

82. Lofholm, *supra* note 67.

83. STANLEY & CRUMP, *supra* note 36, at 1.

84. *Id.*

85. Dvorak, *supra* note 51.

86. In a 2016 study, participants who were aware of government surveillance of their social media posts were significantly less likely to express a minority opinion. Elizabeth Stoycheff, *Under Surveillance: Examining Facebook's Spiral of Silence Effects in the Wake of NSA Internet Monitoring*, 93 JOURNALISM & MASS COMM. Q. 296, 307 (2016).

87. David Kravets, *ACLU Study Highlights U.S. Surveillance Society*, WIRED (June 29, 2010, 4:38 PM), https://www.wired.com/2010/06/aclu-surveillance/ (quoting ACLU attorney Michael German); *see also* ACLU, POLICING FREE SPEECH: POLICE SURVEILLANCE AND OBSTRUCTION OF FIRST AMENDMENT-PROTECTED ACTIVITY (2010), https://www.aclu.org/report/policing-free-speech-police-surveillance-and-obstruction-first-amendment-protected-activity.

88. Fussell, *supra* note 48.

89. *Id.*

90. *Mission Creep*, THEY ARE WATCHING, https://theyarewatching.org/issues/mission-creep (last visited Nov. 21, 2018).

91. STANLEY & CRUMP, *supra* note 36, at 1, 15–16.

of the report, only a handful of police departments were even testing drones.[92] However, the ACLU feared that the "prospect of cheap, small, portable flying video surveillance machines" had the potential "to eradicate existing practical limits on aerial monitoring and allow for pervasive surveillance [and] police fishing expeditions."[93] Since then, the ACLU has continued to advocate for "local laws to require a public, transparent, and democratic process before police departments can acquire new surveillance technologies or military equipment."[94] The ACLU favors regulation of all surveillance technology at the local level and believes the public should have input into when and how law enforcement uses such technology.[95]

The EFF is drawing attention to the threat drones pose to privacy interests through Freedom of Information Act (FOIA) requests. In 2012, the EFF sued the U.S. Department of Transportation demanding the FAA release data about who specifically had obtained authorizations to fly drones above 400 feet in altitude and for what purposes.[96] This suit led to the public's first realization of the FAA's licensing process for UAV and the privacy and surveillance concerns surrounding drone use.[97] The media widely covered the release of information, which resulted in some people learning for the first time that their local police department had drones.[98] EPIC has similarly filed FOIA lawsuits against the DHS seeking the release of information about the Agency's use of drones for domestic surveillance.[99]

Despite strong community opposition, the Los Angeles Police Department (LAPD) is now the largest department in the country with a drone program after its Police Commission approved a year-long test program in 2017.[100] The LAPD first began considering drone use in 2014 when it was gifted two high-powered drones.[101] At that time, public opposition was strong enough to keep the drones

92. *Id.* at 7–8.

93. *Id.* at 1.

94. Kade Crockford, *Boston Police Bought Three Drones but Didn't Tell Anyone. We Need Accountability for Surveillance Now*., ACLU (Sept. 27, 2017, 3:30 PM), https://www.aclu.org/blog/privacy-technology/surveillance-technologies/boston-police-bought-three-drones-didnt-tell.

95. *Community Control over Police Surveillance*, ACLU, https://www.aclu.org/issues/privacy-technology/surveillance-technologies/community-control-over-police-surveillance?redirect=feature/community-control-over-police-surveillance (last visited Nov. 21, 2018). Similarly, the ACLU of Washington favors regulation of drones at the local level and believes that "the acquisition of such technology should be driven by policies and decisions made with public input." Clarridge, *supra* note 8 (citing comments of Doug Honig, a spokesman for the ACLU of Washington).

96. *Drone Flights in the U.S.*, ELECTRONIC FRONTIER FOUND., https://www.eff.org/foia/faa-drone-authorizations (last visited Nov. 21, 2018).

97. *Id.*

98. Crump, *supra* note 51, at 1608.

99. *EPIC v. FAA: Challenging the FAA's Failure to Establish Drone Privacy Rules*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/privacy/litigation/apa/faa/drones (last visited Nov. 21, 2018).

100. Kate Mather, *LAPD Becomes Nation's Largest Police Department to Test Drones After Oversight Panel Signs Off on Controversial Program*, L.A. TIMES (Oct. 17, 2017, 9:05 PM), http://www.latimes.com/local/lanow/la-me-ln-lapd-drones-20171017-story.html.

101. *Id.* Interestingly, the Seattle Police Department purchased two drones with federal funds, but after a public hearing outlining how the Department would use drones drew vocal opposition from citizens with privacy

grounded and they were ultimately destroyed.[102] Three years later, the LAPD invited public comment and held community meetings on the issue, using the meetings to describe ways drones would benefit the department, such as in active shooter or barricaded subject scenarios.[103] Despite skepticism from citizens during the public forums, overwhelmingly negative emails, and efforts by the local ACLU to stop the program, police commissioners approved the plan.[104] The Commission believed the LAPD's new test plan placed sufficiently strict limits on the department's use of drones.[105] Drones are to be used only in specific, high-risk situations such as those involving barricaded suspects, active shooter incidents, explosive devices or explosions, hostages, natural disasters, hazardous materials incidents, search and rescue operations, and armed suspects with superior firepower, an extraordinary tactical advantage, or who are wanted in connection with firing at a police officer.[106] All requests to deploy drones are to be documented and reviewed, and the Police Commission is to receive quarterly reports that will be made public.[107] Video transmissions must be recorded and retained, but the department may not weaponize drones or equip them with facial recognition technology.[108]

One of the main concerns about law enforcement's use of UAS is mission creep,[109] which is the idea that police will expand the use of the technology beyond what was first allowed.[110] Even where drones are initially proposed for innocuous purposes like search and rescue and firefighting missions, law enforcement is quick to contemplate more controversial ways to use them, such as for deterring crime, writing traffic tickets,[111] or observing crowds at political rallies.[112] An example of the potential for mission creep is presented by a town where police officers state they intend to use drones "primarily" to patrol lengths

---

concerns, Mayor Mike McGuinn "pulled the plug" on the program. Clarridge, *supra* note 8. The Department then gifted these drones to the LAPD. *Id.*

102. Mather, *supra* note 100.

103. *Id.*

104. *Id.*

105. *Id.*

106. L.A. POLICE DEP'T, *supra* note 70, at 3.

107. Mather, *supra* note 100.

108. L.A. POLICE DEP'T, *supra* note 70, at 3–4.

109. ACLU WASHINGTON LEGISLATIVE OFFICE, WRITTEN STATEMENT OF THE AMERICAN CIVIL LIBERTIES UNION FOR A HEARING ON "THE FUTURE OF DRONES IN AMERICA: LAW ENFORCEMENT AND PRIVACY CONSIDERATIONS" 6 (2013), https://www.aclu.org/sites/default/files/field_document/aclu_statement_domestic_drones_senate_judiciary032013_final.pdf [hereinafter THE FUTURE OF DRONES IN AMERICA].

110. Kate Mather, *Should the LAPD Use Drones? Here's What's Behind the Heated Debate*, L.A. TIMES (Aug. 8, 2017, 8:15 PM), http://www.latimes.com/local/lanow/la-me-ln-lapd-drones-20170808-story.html.

111. *Id.*

112. Brown, *supra* note 46 (documenting the use of drones to fly over a rally supporting Muslim community); Fisher, *supra* note 45 (documenting the use of drones to monitor crowds at a rally for Representative Scott Taylor); Fran Spielman, *ACLU Sounds the Alarm About Bill Allowing Use of Drones to Monitor Protesters*, CHI. SUN-TIMES (May 1, 2018, 5:17 PM), https://chicago.suntimes.com/politics/aclu-sounds-the-alarm-about-bill-allowing-use-of-drones-to-monitor-protesters (discussing proposed legislation to allow drones equipped with facial recognition technology to monitor public protests).

of railroad tracks for trespassers starting in the spring of 2018.[113] The Department states it does not intend to install high-powered audio recording devices or cameras due to cost and "guarantees" police will not fly over privately owned property without a search warrant.[114] A town councilor expressed concerns about whether the Department's policy adequately ensured the privacy of residents whose properties are near the tracks or of people who happen to be in the area.[115] Although the intended purpose for the first two years is to educate people about the dangers of trespassing near the railroad tracks, if officers monitoring a drone's video feed happen to "find another crime in progress," they are authorized to act upon it.[116]

Critics of the LAPD's new drone program point to the ways the Department's use of other tactical equipment has expanded and warn that the use of drone technology will similarly creep.[117] According to the citizen group Stop LAPD Spying, police helicopters were initially proposed for use in "limited circumstances" such as for traffic control, but soon were routinely used for tracking fleeing suspects or conducting aerial surveillance.[118] SWAT teams were first used only during riots, but now are regularly used to serve search warrants and search for drugs.[119] The LAPD acquired a StingRay cellphone tracker through a DHS grant and promised to use it *only* to investigate terrorist activities, but has since used it in drug investigations.[120] When police have a powerful tool in their arsenal to fight crime, the scope of the mission tends to expand.

Some police departments acknowledge the public's privacy concerns and fear that drone surveillance will create a "Big Brother" society, yet still fail to curb that possibility. For example, the Wichita Police Department purchased a drone and proposed a policy for drone use at a Citizen Review Board meeting, seeking feedback from the public.[121] The Department intends to use the drone for accident reconstruction, crime scene documentation, SWAT responses, and surveilling music festivals, but its nine-page proposed policy does not limit it to any such uses.[122] The proposed policy states in the first paragraph that its "operational procedures are designed to minimize risk to people, property, and aircraft during the operation of the sUAS while continuing *to safeguard the right*

113. Chase, *supra* note 73.

114. *Id.* (citing comments of Brunswick Patrol Commander Thomas Garrepy).

115. *Id.*

116. Elizabeth Clemente, *Brunswick Police Promise Drones Won't Leave the Tracks*, FORECASTER (Jan. 17, 2018), http://www.theforecaster.net/brunswick-police-promise-drones-wont-leave-the-tracks (quoting Brunswick Patrol Commander Thomas Garrepy).

117. *See* Fussell, *supra* note 48.

118. *Id.*

119. *Id.*

120. *Mission Creep*, *supra* note 90.

121. Jason Tidd, *Wichita Police Are Buying a Drone, and They Want Public Input on Its Use*, WICHITA EAGLE (July 2, 2018, 10:05 AM), https://www.kansas.com/news/local/article214032819.html.

122. *Id.*

*to privacy of all persons*."[123] There is no mention of privacy again in the policy and it is silent on warrant requirements.[124] At the meeting, board members raised privacy concerns and asked for more information on drone capabilities, data retention, prohibited uses, and whether drones would be used to target individuals or properties.[125] A department spokesman stated the policy will likely "be rewritten with a greater emphasis on privacy."[126]

The above examples illustrate a recurring theme in this issue: absent federal, state, or local regulations outlining the permissible use of UAS by law enforcement, the police are left to police themselves. When the public expresses concern about how law enforcement will use UAS and questions whether privacy interests are implicated, law enforcement officials ostensibly offer transparency[127] and guarantees that UAS will not be used for improper purposes.[128] For instance, New York State Police averred they will not use their eighteen drones to bypass warrant requirements and that "privacy is a top priority."[129] Across the nation, law enforcement agencies offer assurances they will use drones legally and that current search and seizure laws already protect the public's civil liberties.[130]

### D. CURRENT ATTEMPTS TO REGULATE DRONE USE

At the federal level, UAS are regulated only by the FAA, although Congress has attempted several times to pass laws that either address privacy concerns at the federal level or delegate authority to regulate to the states, thereby limiting the FAA's authority.[131] Numerous states have already enacted drone legislation, despite the FAA's assertion that it has exclusive authority to regulate the national airspace system (NAS).[132] Similarly, a small number of local governments have passed ordinances attempting to address the issue.[133]

#### *1. Federal Regulation and Legislation*

On the federal level, there has been limited regulation of drones. In 2012, Congress charged both the FAA and the Secretary of Transportation to integrate unmanned aircraft systems into the NAS through the National Defense

123. Wichita Police Dep't, *Policy No. 802: Unmanned Aircraft System (UAS) Team Guidelines*, CITY WICHITA KAN., http://www.wichita.gov/WPD/PoliceDocuments/Pol802.pdf#search=uas%20team%20guidelines (last visited Nov. 21, 2018) (emphasis added).

124. *See id.*

125. Tidd, *supra* note 121.

126. *Id.* (citing comments of Wichita Police Department Captain Doug Nolte).

127. Woodall, *supra* note 62.

128. Chase, *supra* note 73 (citing comments of Brunswick Patrol Commander Thomas Garrepy).

129. *State Police Unveil New Drone Program*, NEWS12 WESTCHESTER, http://westchester.news12.com/story/37330404/state-police-unveil-new-drone-program (last updated Feb. 12, 2018, 9:31 AM).

130. *See, e.g.*, Douglass, *supra* note 71.

131. *See infra* Subpart I.D.1.

132. MICHEL, *supra* note 11, at 4.

133. *Id.*

Authorization Act for Fiscal Year 2012[134] and the FAA Modernization and Reform Act of 2012 (FMRA).[135] Section 332 of the FMRA governs the integration of drones into the NAS but omits any reference to privacy.[136] Instead, Congress's intent in enacting both laws was to address issues of aviation safety and to develop certification standards for both civil and public UAS.[137] According to the FAA, it "does not regulate how UAS gather data on people or property."[138] The FAA states that its mission is to provide a safe and efficient aerospace system, and that "does not include regulating privacy."[139]

The FAA oversees drone regulations and safety standards for all drones, whether flown by hobbyists, commercial entities, or federal, state, or local government offices.[140] Generally, anyone can fly a drone under the Small UAS Rule provided by 14 C.F.R. § 107, so long as they obtain a Remote Pilot Certificate,[141] register the UAS,[142] and follow operational rules.[143] These rules include maintaining a line of sight with the UAS during flight, flying only during daylight hours (or civil twilight) below 400 feet in altitude, and not over people or vehicles.[144] Law enforcement agencies have the choice of either flying under

134. National Defense Authorization Act for Fiscal Year 2012, Pub. L. No. 112–81, § 1097, 125 Stat. 1298, 1608 (2011).

135. FAA Modernization and Reform Act of 2012, Pub. L. No. 112–95, § 332, 126 Stat. 11, 73 (2012).

136. *Id.*

137. Section 1097 of the National Defense Authorization Act for Fiscal Year 2012 (NDAA) requires the FAA to establish a program which shall "safely designate nonexclusionary airspace" at "six test ranges" and "develop certification standards and air traffic requirements for unmanned flight operations at test ranges" which "address both civil and public unmanned aircraft systems." National Defense Authorization Act for Fiscal Year 2012 § 1097. Similar to the FAA Modernization and Reform Act of 2012 (FMRA), section 1097 of the NDAA speaks only of safety concerns and is silent on the issue of privacy. Section 332 of the FMRA requires the FAA to use its authority to recommend standards for operation, certification, and registration of UAS and standards and licensing for UAS operators and pilots "to ensure the safe operation of civil unmanned aircraft systems and public unmanned aircraft systems simultaneously in the national airspace system." FAA Modernization and Reform Act of 2012 § 332(a)(2)(b)(H).

138. Press Release, Fed. Aviation Admin., DOT and FAA Finalize Rules for Small Unmanned Aircraft Systems (June 21, 2016), https://www.faa.gov/news/press_releases/news_story.cfm?newsId=20515.

139. Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42064, 42190 (June 28, 2016) (to be codified at 14 C.F.R. pts. 21, 43, 61, 91, 101, 107, 119, 133, 183).

140. *See Unmanned Aircraft Systems (UAS) Frequently Asked Questions*, *supra* note 18.

141. Certificates are available to pilots age sixteen and older who pass an exam at an FAA-approved testing center and are valid for two years. *See Unmanned Aircraft Systems: Becoming a Pilot*, FED. AVIATION ADMIN., https://www.faa.gov/uas/getting_started/part_107/remote_pilot_cert (last visited Nov. 21, 2018).

142. UAS weighing between 0.55 and 55 pounds must be registered with the FAA at a cost of five dollars. *See FAA DroneZone*, FED. AVIATION ADMIN., https://faadronezone.faa.gov/# (last visited Nov. 21, 2018). The FAA instituted the registration requirement in 2015 and a hobbyist brought a challenge in federal court arguing that the FAA lacked statutory authority to promulgate rules or regulations regarding model aircraft under the FMRA. Taylor v. Huerta, 856 F.3d 1089, 1090 (D.C. Cir. 2017). The D.C. Circuit Court agreed, holding that "the Registration Rule is unlawful to the extent that it applies to model aircraft." *Id.* at 1093. This decision exempted hobbyists from the registration rule for just a short time, as Congress passed the National Defense Authorization Act for Fiscal Year 2018, Pub. L. No. 115–91, § 1092(d), 131 Stat. 1610, 1611 (2017), explicitly reinstating the rule shortly after the court's decision in *Taylor*.

143. *See* Small Unmanned Aircraft Systems, 14 C.F.R. § 107 (2018).

144. *Id.* For the full list of operational limitations, see *Summary of Small Unmanned Aircraft Rule (Part 107)*, FED. AVIATION ADMIN. (June 21, 2016), https://www.faa.gov/uas/media/Part_107_Summary.pdf.

the more restrictive Small UAS Rule or obtaining a Certificate of Waiver or Authorization (COA) to Part 107.[145] According to the FAA, 122 police or sheriff's departments had received Part 107 waivers as of July 2018.[146] The FAA also offers a "blanket" exemption (Blanket COA) under section 333 of the FMRA, which permits UAS operators to fly most anywhere in the country—even outside their jurisdiction—except in restricted airspace, at an altitude of 400 feet or less during daylight hours, so long as pilots maintain a visual line of sight.[147] Many law enforcement agencies also opt for a jurisdictional COA, which allows them to operate within their jurisdiction at higher altitudes and at night, in addition to the Blanket COA.[148]

Because the FAA's congressional mandate focuses on promoting safe flight of civil aircraft and setting standards for safe operation,[149] the Agency has declined to address concerns raised by privacy groups such as EPIC.[150] In 2012, EPIC petitioned the FAA to "conduct a rulemaking to address the threat to privacy and civil liberties that will result from the deployment of aerial drones within the United States."[151] EPIC, joined by more than 100 organizations, experts, and advocates, filed its petition due to concern about the threat drones pose to both privacy and civil liberties.[152] The FAA denied the petition in 2016 and issued a final rule on drones stating that privacy issues "are beyond the scope of this rulemaking."[153] In response, EPIC filed a lawsuit in 2016 against the FAA for its failure to establish drone privacy safeguards[154] and another lawsuit in 2018 seeking injunctive relief to compel the FAA's Drone Advisory Committee to comply with its transparency obligations.[155] EPIC's 2016 suit was dismissed by the U.S. Court of Appeals for the District of Columbia Circuit in June of 2018 for lack of standing.[156]

---

145. *See Unmanned Aircraft Systems: Beyond the Basics*, FED. AVIATION ADMIN., https://www.faa.gov/uas/beyond_the_basics (last visited Nov. 21, 2018).

146. *Unmanned Aircraft Systems: Part 107 Waivers Granted*, FED. AVIATION ADMIN., https://www.faa.gov/uas/request_waiver/waivers_granted (last visited Nov. 21, 2018).

147. *See Unmanned Aircraft Systems: Petitioning for Exemption Under Section 333*, FED. AVIATION ADMIN., https://www.faa.gov/uas/beyond_the_basics/section_333/how_to_file_a_petition (last visited Nov. 21, 2018); *see also So, What's a COA?*, SKYFIRE CONSULTING (Apr. 7, 2017), https://www.skyfireconsulting.com/skyfire-drone-blog/certificate-of-authorization-guid-coa.

148. *See Unmanned Aircraft Systems: Petitioning for Exemption Under Section* 333, *supra* note 147; *So, What's a COA?*, *supra* note 147. In 2011, the Mesa County Sheriff's Department received permission from the FAA to operate its drones anywhere in the county, which spans 3,309 square miles. STANLEY & CRUMP, *supra* note 36, at 7; *About Us: Geography*, MESA CTY., https://www.mesacounty.us/contact-us/about-us/geography/ (last visited Nov. 21, 2018). This is noteworthy because it is the first police department permitted to operate in such a broad area. STANLEY & CRUMP, *supra* note 36, at 7.

149. 49 U.S.C. § 44701(a) (2012).

150. *EPIC v. FAA: Challenging the FAA's Failure to Establish Drone Privacy Rules*, *supra* note 99.

151. *Id.*

152. *Id.*

153. *Id.*

154. Elec. Privacy Info. Ctr. v. FAA, 892 F.3d 1249, 1252 (D.C. Cir. 2018).

155. *See* Elec. Privacy Info. Ctr. v. Drone Advisory Comm., No. 18–833 (D.D.C. filed Apr. 11, 2018).

156. *Elec. Privacy Info. Ctr.,* 892 F.3d at 1256. EPIC argued that increased testing of delivery and reconnaissance drones would cause a loss of privacy and impair freedom of travel due to fears of constant

Despite these efforts, there are currently no federal standards for individual privacy protection from drones and their potential to effect "invasive and pervasive surveillance."[157] Because the FAA's scope is limited to safety concerns and not privacy, some members of Congress have proposed legislation focused on protecting the privacy interests of citizens from governmental intrusion.[158] Massachusetts Senator Edward Markey introduced the Drone Aircraft Privacy and Transparency Act of 2017, which would provide strict guidelines to minimize data collection and retention by drones and require law enforcement to obtain warrants for surveillance absent "extreme exigent circumstances."[159] The bill defines extreme "exigent circumstances" to mean that law enforcement "reasonably believes there is an imminent danger of death or serious physical injury" or a "high risk of an imminent terrorist attack by a specific individual or organization," which the Secretary of Homeland Security identified as a credible threat.[160] Senator Markey has previously introduced earlier versions of this bill twice in the Senate and twice in the House of Representatives.[161] Some have criticized the proposed legislation as underinclusive, because it does not address hobbyists, and fear that it will preempt "areas of law typically left to the states, such as privacy, trespass, and state and local police power."[162]

Other U.S. senators believe that states are in the best position to protect the public's privacy from drone misuse.[163] The Drone Federalism Act was introduced in 2017 "as a way for local governments . . . to create drone rules

monitoring, *id.* at 1253, but the court found this chain of causation to potential injuries to be too attenuated, *id.* at 1255.

157. Drone Aircraft Privacy and Transparency Act of 2017, S. 631, 115th Cong. § 2(5) (2017).

158. *See, e.g.*, Drone Aircraft Privacy and Transparency Act of 2017, S. 631, 115th Cong. (2017); Drone Innovation Act of 2017, H.R. 2930, 115th Cong. (2017); Drone Aircraft Privacy and Transparency Act of 2015, S. 635, 114th Cong. (2015); Preserving Freedom from Unwarranted Surveillance Act of 2013, S. 1016, 113th Cong. (2013); Preserving Freedom from Unwarranted Surveillance Act of 2013, H.R. 972, 113th Cong. (2013); Drone Aircraft Privacy and Transparency Act of 2013, S. 1639, 113th Cong. (2013); Preserving Freedom from Unwarranted Surveillance Act of 2012, H.R. 5925, 112th Cong. (2012); Preserving Freedom from Unwarranted Surveillance Act of 2012, S. 3287, 112th Cong. (2012); Drone Aircraft Privacy and Transparency Act of 2012, H.R. 6676, 112th Cong. (2012).

159. Press Release, Senator for Mass. Ed Markey, Senator Markey & Rep. Welch Introduce Legislation to Ensure Transparency, Privacy for Drone Use (Mar. 15, 2017), https://www.markey.senate.gov/news/press-releases/-senator-markey-and-rep-welch-introduce-legislation-to-ensure-transparency-privacy-for-drone-use.

160. Drone Aircraft Privacy and Transparency Act of 2017, S. 631 § 340(b)(2).

161. *See S. 631: Drone Aircraft Privacy and Transparency Act of 2017*, GOVTRACK, https://www.govtrack.us/congress/bills/115/s631 (last visited Nov. 21, 2018) (providing an overview of the bill's history); sources cited s*upra* note 158; *see also* Keith Lang, *Sen. Markey Files Bill to Protect Privacy in Commercial Drone Use*, HILL (Nov. 4, 2013, 5:32 PM), http://thehill.com/policy/transportation/189208-sen-markey-files-bill-to-protect-privacy-in-commercial (describing how Senator Markey's proposed legislation would require the FAA to consider privacy interests in its regulation of drones).

162. Scott Hall, *The Drone Privacy and Transparency Act of 2017: Overdue or Over-Reaching?*, JDSUPRA (Mar. 29, 2017), https://www.jdsupra.com/legalnews/the-drone-privacy-and-transparency-act-42426.

163. *See* Jonathan Vanian, *New Senate Drone Bill Would Give Power to States and Local Governments*, FORTUNE (May 25, 2017), http://fortune.com/2017/05/25/senate-drone-bill-faa-regulations.

specific to their regions without butting heads with the federal government."[164] The text of the bill limits the FAA's authority "to the extent necessary to ensure the safety and efficiency of the national airspace system for interstate commerce" and reserves state and local governments the right to regulate and protect public safety, personal privacy, property rights, and other interests.[165] According to the bill's sponsor, California Senator Diane Feinstein, "State, local, and tribal governments have a legitimate interest in protecting public safety and privacy from the misuse of drones."[166] The Drone Federalism Act would cede authority to regulate from the earth to 200 feet above its surface to state and local government.[167] If the bill does pass, it would leave the space between 200 and 400 feet above ground unregulated locally and subject only to FAA regulations.[168] However, the bill would place no specific limits on the use of UAS by law enforcement; it would merely allow local government to regulate the swath of airspace closest to the earth.[169]

### *2. State Legislation*

In response to pressure from privacy advocates and the public, many states have passed legislation regulating the use of drones by law enforcement.[170] In the past five years, all fifty states have proposed drone legislation of some kind.[171] More than half of states have actually passed laws regulating drones and addressing privacy concerns posed by both law enforcement and non-governmental actors, such as commercial entities or private citizens.[172] Fifteen

164. *Id.*

165. Drone Federalism Act of 2017, S. 1272, 115th Cong. § 2(a) (2017).

166. Vanian, *supra* note 163.

167. *Id.*

168. Georeen Tanner, *Drones Becoming a Threat to First-Responder Operations*, FOX NEWS, https://www.foxnews.com/tech/drones-becoming-a-threat-to-first-responder-operations (last visited Nov. 21, 2018).

169. *See id*. ("[The] bill . . . would give local governments the power to regulate drones flying below 200 feet.").

170. Gregory McNeal, *Drones and Aerial Surveillance: Considerations for Legislatures*, BROOKINGS INST. 2 (Nov. 2014), https://www.brookings.edu/research/drones-and-aerial-surveillance-considerations-for-legislatures. Eight states passed laws regulating drones in 2013 and five states passed such laws in 2014, "with eleven of those thirteen states requiring a warrant before the government may use a drone." *Id.*

171. MICHEL, *supra* note 11, at 4–5. As of March 2017, only South Dakota had not considered any type of drone legislation. *Id.* However, effective July 1, 2017, South Dakota amended its definition of "trespassing to eavesdrop," making it a crime for private actors to use a drone to conduct unlawful surveillance. S.D. CODIFIED LAWS § 22-21-1 (2018). The law does not apply to law enforcement while engaged in their lawful duties. *Id.*

172. Twenty-six states have adopted some type of legislation as of January 17, 2018: Alaska, Arkansas, California, Florida, Idaho, Illinois, Indiana, Iowa, Kansas, Louisiana, Maine, Michigan, Mississippi, Montana, Nevada, New Jersey, North Carolina, North Dakota, Oregon, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia and Wisconsin. *See 2017 UAS State Legislation Update*, *supra* note 10. Nineteen states have passed laws protecting against privacy invasions from non-government operators, with several criminalizing the use of drones to commit the offense of voyeurism. *Id.*

states have enacted laws preempting localities from regulating drones in some way.[173]

The FAA has pushed against these efforts, viewing all attempts to regulate airspace use as infringing on its exclusive domain to regulate aircraft because federal law has preempted the field.[174] The FAA cites safety concerns and fractionalized control of the airspace when state or local governments attempt to regulate UAS, or any aircraft.[175] "A navigable airspace free from inconsistent state and local restrictions is essential to the maintenance of a safe and sound air transportation system."[176]

State measures regulating drone use by law enforcement have been criticized by some as misguided because they focus on the technology of drones, rather than the "threat of pervasive surveillance."[177] According to Gregory McNeal of the Brookings Institution, "the legislation is rarely tailored in such a way to prevent the harm that advocates fear."[178] Focusing on drone technology, rather than the threat of a surveillance society, creates an unintended result because it forecloses the use of drones for beneficial tasks such as accident and crime scene documentation, while still allowing pervasive surveillance from manned aircraft or by other means.[179]

### *a. State Laws Regulating Drone Use by Law Enforcement*

Eighteen states have enacted laws requiring law enforcement to obtain search warrants prior to using drones to conduct a search or surveillance.[180] Some of these laws merely reaffirm the Fourth Amendment's baseline guarantee of a person's right to be free from warrantless searches, while other states

173. *Id.* The following states preempt local government from regulating drones in some way: Arizona, Connecticut, Delaware, Florida, Georgia, Louisiana, Maryland, Michigan, Montana, New Jersey, Oregon, Rhode Island, Texas, Utah and Virginia. *Id.* It is noteworthy that nine of the states preempting local regulation of drones have themselves either failed or chosen not to institute warrant requirements. *Id.* One such state, Colorado, did pass H.B. 1070 in 2017, authorized a study to "identify ways to integrate UAS within local and state government functions relating to firefighting, search and rescue, accident reconstruction, crime scene documentation, emergency management, and emergencies involving significant property loss, injury or death." *Id.*

174. *See* OFFICE OF THE CHIEF COUNSEL, FED. AVIATION ADMIN., STATE AND LOCAL REGULATION OF UNMANNED AIRCRAFT SYSTEMS (UAS) FACT SHEET 2 (2015), https://www.faa.gov/uas/resources/uas_regulations_policy/media/uas_fact_sheet_final.pdf ("To ensure the maintenance of a safe and sound air transportation system and of navigable airspace free from inconsistent restrictions, FAA has regulatory authority over matters pertaining to aviation safety.").

175. *Id.*

176. *Id.* (citing Montalvo v. Spirit Airlines, 508 F.3d 464 (9th Cir. 2007)).

177. McNeal, *supra* note 170, at 2.

178. *Id.*

179. *Id.* at 3.

180. Alaska, Florida, Idaho, Illinois, Indiana, Iowa, Maine, Montana, Nevada, North Carolina, North Dakota, Oregon, Tennessee, Texas, Utah, Vermont, Virginia, and Wisconsin currently require law enforcement to obtain search warrants prior to using UAS for search or surveillance. *See 2017 UAS State Legislation Update*, *supra* note 10.

provide more robust protection that far exceeds the Fourth Amendment's warrant requirement.[181]

For example, Oregon's law preventing warrantless drone surveillance is the most protective state measure in the United States, making clear that information gathered in violation of the law cannot be used by law enforcement.[182] The law, which was enacted in 2013, prohibits law enforcement's use of drones except when: (1) a warrant is issued authorizing the use of UAS that specifies the period of operation and not to exceed thirty days which is renewable by the court upon motion and showing of good cause; (2) the agency has probable cause to believe there has been or will be a crime *and* exigent circumstances exist making it unreasonable to obtain a warrant authorizing drone use; (3) an individual gives written consent; (4) conducting search and rescue activities; (5) assisting an individual during an emergency if the agency believes there is an imminent threat to life or safety of the individual; (6) preserving public safety, private property, or assessing environmental or weather-related damage during a state emergency that is declared by the governor; (7) performing crime scene reconstruction; or (8) conducting training exercises.[183] Any data that is obtained in violation of the statute (including during training exercises), is not admissible in any court proceeding and cannot be used to establish probable cause.[184] The ACLU advocated for the bill's passage[185] and after it was passed, EPIC praised it as an exemplar designed to "prevent mass and/or suspicionless surveillance."[186]

At the opposite end of the spectrum are state measures that afford no further protection than the Fourth Amendment does. For example, Wisconsin prohibits the use of a drone to gather evidence from a place where an individual has a reasonable expectation of privacy, without first obtaining a search warrant.[187] Excepted from the warrant requirement are: (1) drones used in public places; (2) search and rescue operations; (3) searching for an escaped prisoner; (4) surveillance conducted prior to serving an arrest warrant; or (5) if a law enforcement officer believes use of a drone is necessary to prevent imminent danger or to prevent the imminent destruction of evidence.[188] This law is similar to the Fourth Amendment, which already requires a warrant where there is a reasonable expectation of privacy, as discussed in Part II. Therefore, Wisconsin's law, as well as those of a handful of other states, "place[s] no

181. *See, e.g.*, OR. REV. STAT. §§ 837.310–837.345 (2017).

182. *State Drone Law and UAV Policy*, ELECTRONIC PRIVACY INFO. CTR., https://epic.org/state-policy/drones (last visited Nov. 21, 2018).

183. OR. REV. STAT. §§ 837.310–837.345.

184. *Id.*

185. *Privacy: Regulate Use of Drones in Oregon (HB 2710, SB 71)* (2013), ACLU, https://aclu-or.org/en/legislation/privacy-regulate-use-drones-oregon-hb-2710-sb-71-2013 (last visited Nov. 21, 2018).

186. *State Drone Law and UAV Policy*, *supra* note 182.

187. WIS. STAT. ANN. § 175.55(2) (West 2018).

188. *Id.*

meaningful restrictions on government use of drones."[189] And unlike Oregon's law, Wisconsin's does not explicitly preclude evidence obtained in violation of the statute from being admitted in court or to establish probable cause, nor does it require that any warrant obtained specify that a drone may be used.[190]

Most states with laws restricting law enforcement use of drones fall somewhere in the middle of the spectrum, in that the exceptions to the warrant requirement are more explicit, rather than a "broadly-worded exception."[191] For instance, Florida prohibits drone searches and seizures by law enforcement except in limited circumstances, including (1) when there is a high risk of terrorist attack; (2) the agency obtains a search warrant from a judge authorizing the use of a drone; (3) when law enforcement officers believe there is an imminent danger to life or serious property damage; or (4) to forestall the escape of a suspect or destruction of evidence.[192] Evidence obtained in violation of the statute is inadmissible in any criminal prosecution.[193]

### *b. Failed State Attempts to Regulate Law Enforcement Use of Drones*

Thirty-two states have tried and failed to enact laws requiring law enforcement to obtain a warrant absent exigent circumstances.[194] California Governor Edmund Gerald "Jerry" Brown vetoed such a bill in 2014,[195] which also would have required that most data, photos, or videos collected by drones be destroyed within one year.[196] In a letter to the California State Assembly explaining why he vetoed the bill, Governor Brown stated the exceptions to the warrant requirement were too narrow and went beyond those required by both the Fourth Amendment and the California Constitution.[197] Although the bill had bipartisan support, it was opposed by law enforcement groups, including the California Police Chiefs Association, the California State Sheriffs'

189. Michael L. Smith, *Regulating Law Enforcement's Use of Drones: The Need for State Legislation*, 52 HARV. J. ON LEGIS. 423, 436 (2015). Iowa, Montana, and Utah similarly use language that is very broad and affords no greater protection than the Fourth Amendment does. *Id.*

190. *Compare* OR. REV. STAT. §§ 837.310–837.345 (2017), *with* WIS. STAT. ANN. § 175.55.

191. Smith, *supra* note 189, at 429.

192. FLA. STAT. § 934.50 (2018).

193. *Id.* § 934.50(6).

194. *See 2017 UAS State Legislation Update*, *supra* note 10.

195. Lily Hay Newman, *California Governor Vetoes Bill Requiring Warrant for Police Surveillance Drones*, SLATE (Sept. 30, 2014, 5:47 PM), http://www.slate.com/blogs/future_tense/2014/09/30/california_governor_jerry_brown_vetoes_drone_surveillance_law_enforcement.html.

196. Aaron Mendelson, *California Senate Approves Measure Banning Warrantless Drone Surveillance*, REUTERS (Aug. 26, 2014, 10:44 PM), https://www.reuters.com/article/us-usa-california-drones/california-senate-approves-measure-banning-warrantless-drone-surveillance-idUSKBN0GR0E020140827.

197. Letter from Governor Edmund G. Brown Jr. to the Members of the Cal. State Assembly (Sept. 28, 2014) (on file with author).

Association,[198] and the Los Angeles District Attorney's Office.[199] More recently, lobbyists employed by drone manufacturers successfully blocked a similar bill in 2016.[200] Thus, special interest groups have defeated the California legislature's efforts to regulate the use of drone technology.

An Ohio bill requiring law enforcement to obtain warrants prior to using drones for evidence gathering met a similar fate,[201] even though it had bi-partisan support. The bill was sponsored by a Democrat and a Republican senator and both expressed concerns about protecting the constitutional rights of Ohioans and preserving civil liberties.[202] One of the bill's sponsors, Senator Kris Jordan, warned that "[t]here aren't enough guardrails . . . to limits [sic] . . . the potential for spying. . . . we need to put guardrails out there to protect the individual rights of citizens."[203] After the first bill stalled in the state senate,[204] the two lawmakers introduced a similar bill in 2017.[205] Police have been using drones in Ohio since at least 2014, yet there are still no laws regulating drone use by law enforcement.[206]

### *3. Local Ordinances Regulating Law Enforcement Use of Drones*

Where states have failed to act to regulate law enforcement use of drones, some local governments are passing measures to guard the public's privacy and

198. Mendelson, *supra* note 196.

199. Conor Freidersdorf, *Why Police Don't Need Warrants to Snoop with Drones*, ATLANTIC (Aug. 28, 2014), https://www.theatlantic.com/politics/archive/2014/08/california-lawmakers-back-a-restraining-order-on-police-drones/379267.

200. Jazmine Ulloa, *Why California May Not See Statewide Rules on the Use of Drones Anytime Soon*, L.A. TIMES (July 31, 2016, 12:05 AM), http://www.latimes.com/politics/la-pol-sac-drone-bills-california-20160731-snap-story.html. Assemblyman Bill Quirk's bill would have prohibited drone surveillance of private property without a warrant in most situations and required police to adopt policies prior to employing drones. Mike Maharrey, *California Bill Taking on Warrantless Drone Surveillance Passes Assembly 61-12*, TENTH AMEND. CTR. (May 28, 2015), http://blog.tenthamendmentcenter.com/2015/05/california-bill-taking-on-warrantless-drone-surveillance-passes-assembly-61-12. The bill passed the Assembly with a vote of 61 to 12, but languished in the state senate until it was withdrawn. *See* Assemb. B. 56, 2015–16 Leg., Reg. Sess. (Cal. 2015).

201. *See* S.B. 251, 131st Gen. Assemb., Reg. Session (Ohio 2015). The bill was introduced on December 8, 2015, reached 25% progression, and died in committee. *Ohio Senate Bill 251*, LEGISCAN, https://legiscan.com/OH/bill/SB251/2015 (last visited Nov. 21, 2018).

202. *Bill Would Restrict Police Use of Drones*, OHIO PUB. RADIO (Mar. 24, 2017), http://wcbe.org/post/bill-would-restrict-police-use-drones.

203. *Id.*

204. Ohio S.B. 251.

205. *See* S.B. 60, 132d Gen. Assemb., Reg. Sess. (Ohio 2017); Richard Wilson, *Eyes in the Sky: Law Enforcement Drone-Use Sparks Privacy Concerns*, DAYTON DAILY NEWS (Oct. 21, 2017), http://www.daytondailynews.com/news/eyes-the-sky-law-enforcement-drone-use-sparks-privacy-concerns/KnO52eZi9NijumCI6hXvAJ ("State Sen. Michael Skindell (D-Cleveland) and State Sen. Kris Jordan (R-Delaware) are co-sponsors of Senate Bill 60 . . . .").

206. *Id.* Chief Deputy Mike Eberle, stated that the Auglaize County Sheriff's Office uses drones "primarily in cases of missing persons and serious traffic crash investigations." *Id.* However, if during such a flight the drone captured photographic evidence of another crime, police could likely use that evidence as probable cause to obtain a warrant. *Id.* ("It's no different than if you're in somebody's house and you notice a marijuana plant. If you think there's more, you've got to go get a warrant . . . but you stumbled upon it legally.").

civil liberties.[207] However, the majority of local measures target private drone use—127 of the 133 ordinances passed as of 2017 restrict private actors only.[208] At least six local municipalities have passed ordinances restricting law enforcement or government use of drones.[209] These have taken a variety of approaches, from prohibiting all drone use by law enforcement[210] to adopting "future-proof" policies, which require approval by local government prior to law enforcement's use of any new surveillance technology,[211] to protection no broader than the Fourth Amendment affords.[212]

The Syracuse City Council passed a resolution in 2013 prohibiting law enforcement or other city agencies from using drones until the federal and state governments adopt legislation "that adequately protects the privacy of the population."[213] The resolution specifically points to the need for research regarding privacy considerations, the fact that the FAA is not tasked with addressing privacy or civil liberties, and the lack of safeguards preventing drones from being used to infringe upon fundamental privacy rights and obtain large amounts of data without a warrant.[214]

Seattle is now one of a handful of localities that prohibits law enforcement use of drones.[215] The Seattle Police Department originally acquired two drones using federal funds, which it intended to use to locate missing persons and investigate crimes.[216] However, when local residents became aware of the plan, they vocally opposed it at a public hearing outlining proposed restrictions for the Department's use.[217] In response, the city's mayor ended the program before it even started, saying police need to stay focused on "community building."[218] Seattle then passed an ordinance addressing not drones specifically, but the

207. *See* MICHEL, *supra* note 11, at 1, 2.

208. MICHEL, *supra* note 11, at 2.

209. *Id.* (listing Syracuse, New York; Pierce County, Washington; Seattle, Washington; and Spokane, Washington as having ordinances specifically restricting law enforcement).

210. Tim Knauss, *Syracuse Bans Police Drones Until Privacy Regulations in Place*, SYRACUSE.COM (Dec. 16, 2013), http://s.syracuse.com/I4663FB.

211. *See, e.g.*, Eric Kurhi, *Pioneering Spy-Tech Law Adopted by Santa Clara County*, MERCURY NEWS, https://www.mercurynews.com/2016/06/07/pioneering-spy-tech-law-adopted-by-santa-clara-county (last updated Sept. 22, 2016, 12:23 AM); *Seattle Adopts Nation's Strongest Regulations for Surveillance Technology*, ACLU OF WASH. (Aug. 8, 2017), https://www.aclu-wa.org/news/seattle-adopts-nation's-strongest-regulations-surveillance-technology.

212. *See* PIERCE COUNTY, WASH., CODE §§ 1.30.010–.040 (2018) ("No County department or agency shall use a drone or other unmanned aircraft . . . except as authorized by state and federal law.").

213. Knauss, *supra* note 210.

214. *Resolution to Syracuse Common Council to Prevent the Unregulated Use of Drones in Syracuse*, SYRACUSE PEACE COUNCIL, http://peacecouncil.net/resolution-to-syracuse-common-council-to-prevent-the-unregulated-use-of-drones-in-syracuse (last visited Nov. 21, 2018).

215. Laura L. Myers, *Seattle Mayor Grounds Police Drone Program*, REUTERS (Feb. 7, 2013, 10:00 PM), https://www.reuters.com/article/us-usa-drones-seattle/seattle-mayor-grounds-police-drone-program-idUSBRE91704H20130208.

216. *Id.*

217. Clarridge, *supra* note 8.

218. *Id.*

acquisition of all surveillance technology by the city.[219] The measure allows the public an opportunity to express its concerns before the acquisition of any surveillance technology, including equipment, hardware, or software.[220] At the time it was passed, the ACLU praised the ordinance as "the strongest measure adopted by an American city to regulate the acquisition of surveillance technology."[221] Given the vocal opposition to the proposal to allow police use of drones in 2013, the city is unlikely to change its position in the near future, since any new technology would require community meetings prior to city council approval.[222] In fact, Seattle prohibits drone use anywhere within the city unless the drone activity is for commercial filming with a permit.[223]

The City of Spokane passed a similar ordinance in 2013, requiring city council approval for the acquisition of any new surveillance equipment, such as drones or camera networks.[224] However, Spokane's ordinance went a step further and also requires approval before using third-party surveillance equipment.[225] Thus, city departments cannot circumvent the law's intent by "outsourcing" surveillance to third parties.[226] According to the ACLU, this is a critical provision making Spokane's ordinance even more protective than Seattle's.[227]

In California, Santa Clara County has similarly adopted a "future-proof" model for electronic surveillance, requiring police agencies to establish policies prior to acquiring emerging surveillance technologies.[228] The ordinance was in response to various local agencies' acquisitions of a drone and Stingray cellphone tracker[229] and plans to build a "Domain Awareness Center" information hub.[230] Santa Clara County's ordinance does not target particular

219. *Seattle Adopts Nation's Strongest Regulations for Surveillance Technology*, *supra* note 211.

220. *Id.*

221. *Id.*

222. *Id.*

223. SEATTLE SPECIAL EVENTS OFFICE, SPECIAL EVENTS PERMITTING HANDBOOK: DRONES, https://www.seattle.gov/special-events-office/handbook/drones (last visited Nov. 21, 2018).

224. Jamela Debelak, *Surveillance: Spokane Acts to Protect Privacy and Provide Transparency*, ACLU OF WASH. (Aug. 21, 2013), https://www.aclu-wa.org/blog/surveillance-spokane-acts-protect-privacy-and-provide-transparency.

225. *Id.*

226. *Id.*

227. *Id.*

228. Kurhi, *supra* note 211.

229. A StingRay is a surveillance device that impersonates a cellular network bas station and tricks all nearby phones and other mobile devices into identifying themselves by revealing their unique serial numbers. State v. Andrews, 134 A.3d 324, 340–41 (Md. Ct. Spec. App. 2016). As each device identifies itself, the StingRay can determine the location from which the signal came. *Id.* at 341. The device can be handheld, installed on a vehicle, or mounted on a drone. *Id.*

230. Kurhi, *supra* note 211. The City of Oakland planned to build a Domain Awareness Center that would have linked the 700 plus cameras throughout Oakland's public schools and public housing. The plan was successfully opposed by area residents and the ACLU. Brian Hofer, *How the Fight to Stop Oakland's Domain Awareness Center Laid the Groundwork for the Oakland Privacy Commission*, ACLU OF N. CAL. (Sept. 21, 2018), https://www.aclunc.org/blog/how-fight-stop-oaklands-domain-awareness-center-laid-groundwork-oakland-privacy-commission. Privacy advocates warn that centers which "collect so much information about

technologies, but places the burden on public agencies to notify the Board of Supervisors and the public "in advance about all potentially invasive innovations."[231]

Pierce County in Washington adopted an ordinance entitled "Freedom from Unwarranted Surveillance" in 2013.[232] It prohibits any county agency from using a drone to gather evidence, "*except as authorized by state and federal law*."[233] The ordinance also includes an exception for exigent circumstances but does not define the term.[234] Washington is not among the eighteen states that require a warrant.[235] Thus, the county's measure affords no greater protection than the Fourth Amendment.

## II. THE FOURTH AMENDMENT: AERIAL SURVEILLANCE AND HIGH-TECH SURVEILLANCE DOCTRINES AND HOW COURTS ARE APPLYING THEM

Current Fourth Amendment doctrine is ill-equipped to address the technological developments that lead to widespread surveillance, which is the precise challenge that drones present. The Supreme Court has articulated two primary tests to determine whether a search has occurred for Fourth Amendment purposes: the trespassory test and the reasonable expectation of privacy test.[236] Because drones can surveil without ever trespassing on an individual's property and capture large amounts of information that is exposed to public view, even long-term surveillance might not constitute a search for Fourth Amendment purposes.[237]

Under the Court's aerial surveillance doctrine, brief overhead searches from manned aircraft do not violate the Fourth Amendment,[238] but it is unclear whether the same reasoning would apply to drones conducting surveillance and continuously monitoring individuals or their property. Similarly, the Court has held that when the government uses sense-enhancing technology not in general use to conduct surveillance that would have previously only been possible by

---

people from various sources" can be used to create a picture of a person's daily activities, whether or not they are suspected of any wrongdoing, and "have the potential to become the nerve center of the "total surveillance society." LOVE, *supra* note 49, at 16.

231. Kurhi, *supra* note 211.

232. PIERCE COUNTY, WASH., CODE §§ 1.30.010–.040 (2018).

233. *Id.* § 1.30.020 (emphasis added).

234. *Id.* § 1.30.030.

235. *See 2017 UAS State Legislation Update*, *supra* note 10.

236. United States v. Jones, 565 U.S. 400, 409 (2012) ("[T]he *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test.").

237. *See, e.g.*, United States v. Bucci, 582 F.3d 108, 116–17 (1st Cir. 2009) (holding that surveillance of the front of a home conducted by a pole-top camera for eight months did not constitute a search because there was no reasonable expectation of privacy).

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

physical intrusion, the Fourth Amendment is implicated.[239] However, drones present a technology that is both widely used by the general public[240] and equipped with cameras and other tools that enhance the senses beyond what any human could perceive.[241] Despite a recent Supreme Court decision recognizing a right to privacy in the whole of an individual's movements,[242] it is unlikely the current aerial and high-tech surveillance doctrines protect individuals from the invasive and pervasive nature of drone surveillance and the unprecedented level of intrusion it presents.

### A. DIFFERING APPROACHES TO INTERPRETING THE FOURTH AMENDMENT

As discussed in Part I, many states and local governments rely on the Fourth Amendment's protection against unreasonable searches and seizures as the sole limitation on law enforcement's use of UAS. Alternately, enacted measures—such as Wisconsin's statute or Pierce County's ordinance—parallel the protections of the Fourth Amendment, without adding to it.[243] However, it is uncertain whether the Fourth Amendment provides any protection with respect to UAS surveillance, as the Supreme Court has not decided an aerial surveillance case in almost three decades, pre-dating the advent of UAS.[244] Under either the trespassory test or the reasonable expectation of privacy test, law enforcement may likely use a drone to conduct ongoing surveillance of a person or property that is invisible from the air,[245] provided it does not actually trespass[246] or create a physical disturbance.[247]

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."[248] For almost two-hundred years,[249] the Court interpreted the Fourth Amendment literally to mean that a search occurred only when the government searched tangible things: the person, house, papers, or effects, and refused to

239. *See* Kyllo v. United States, 533 U.S. 27, 40 (2001).

240. Atherton, *supra* note 1 (reporting 1,500,000 drone hobbyists in the United States as of March 2016).

241. *See supra* Subpart I.B.

242. *See* Carpenter v. United States, 138 S. Ct. 2206, 2210 (2018).

243. *See* WIS. STAT. ANN. § 175.55(2) (2018); PIERCE COUNTY, WASH., CODE §§ 1.30.010–.040 (2018).

244. *See* Florida v. Riley, 488 U.S. 445 (1989).

245. AMY ALBANO & LISA S. KURIHARA, INVASION OF THE DRONES 20 (2016), https://www.cacities.org/Resources-Documents/Member-Engagement/Professional-Departments/City-Attorneys/Library/2016/Spring-2016/5-2016-Spring-Drones-Flying-By-Your-City-Amy-Alban. The length of time the Supreme Court would find permissible is undefined, but it is "for some period of time that is less than four weeks," as the Court stated in *Jones*. *Id.*

246. United States v. Jones, 565 U.S. 400, 404–05 (2012) (holding that a search occurs when the government physically occupies private property for the purpose of obtaining information).

247. *See, e.g.*, State v. Davis, 360 P.3d 1161, 1172 (N.M. 2015) (holding that an aerial search from a helicopter constituted a search because the prolonged hovering created a physical disturbance and transformed the "surveillance from a lawful observation of an area left open to public view to an unconstitutional intrusion into [the defendant's] expectation of privacy").

248. U.S. CONST. amend. IV.

249. This accounts for the span between *Ex parte Jackson*, 96 U.S. 727 (1877) and *Katz v. United States*, 389 U.S. 347 (1967).

extend Fourth Amendment protections "to forbid hearing or sight," such as conversations recorded by wiretap.[250] However, the Court now characterizes that interpretation as only a baseline protection, stating "[w]hen 'the Government obtains information by physically intruding' on persons, houses, papers, or effects, 'a "search" within the original meaning of the Fourth Amendment' has 'undoubtedly occurred.'"[251] This physical intrusion on the property rights of an individual is known as the trespassory test.[252]

In 1967, the Court expanded its view of the Fourth Amendment radically in *Katz v. United States*, holding that a search could occur in the absence of a physical intrusion by the government and that the trespass doctrine was no longer controlling.[253] "For the Fourth Amendment protects people, not places."[254] *Katz* also articulated the plain-view doctrine, which states 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."[255] Conversely, even in an area exposed to the public, what a person seeks to preserve as private may be constitutionally protected if that person's expectation of privacy is reasonable under the circumstances.[256] Applying *Katz*, the Fourth Amendment affords protection from invasion by the government when a person claims a justifiable, reasonable, or legitimate expectation of privacy.[257]

In the wake of *Katz*,[258] it was unclear whether the reasonable expectation of privacy test had fully supplanted the trespassory test.[259] Later cases applied the two-prong reasonable expectation of privacy test articulated by Justice Harlan in his concurrence to *Katz*.[260] First, a person must have exhibited an actual (subjective) expectation of privacy.[261] Second, society must be prepared to recognize that expectation as reasonable.[262]

---

250. Olmstead v. United States, 277 U.S. 438, 464–65 (1928). The Court held that the Fourth Amendment is not violated "unless there has been an official search and seizure of [a defendant's] person, or such a seizure of his papers or his tangible material effects, or an actual physical invasion of his house 'or curtilage' for the purpose of making a seizure." *Id.* at 466.

251. Florida v. Jardines, 569 U.S. 1, 5 (2013) (quoting United States v. Jones, 565 U.S. 400, 406–07 n.3 (2012)).

252. *See* United States v. Jones, 565 U.S. 400, 405 (2012) ("[O]ur Fourth Amendment jurisprudence was tied to common-law trespass.").

253. 389 U.S. at 353.

254. *Id.* at 351.

255. *Id.*

256. *See id.* at 351; *id.* at 361 (Harlan, J., concurring).

257. Smith v. Maryland, 442 U.S. 735, 740 (1979).

258. *See* Kyllo v. United States, 533 U.S. 27, 32 (2001) ("We have since decoupled violation of a person's Fourth Amendment rights from trespassory violation of his property . . . .").

259. Some argued the *Katz* decision was a "watershed in fourth amendment jurisprudence," while others viewed it not as a move away from the *Olmstead* framework, but merely as reemphasizing a "loose property-based view." Orin S. Kerr, *The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution*, 102 MICH. L. REV. 801, 820 (2004) (footnote omitted).

260. United States v. Jones, 565 U.S. 400, 406 (2012).

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

262. *Id.*

Forty-five years later, the Court clarified in *United States v. Jones* that "the *Katz* reasonable-expectation-of-privacy test has been *added to*, not *substituted for*, the common-law trespassory test."[263] Writing for the Court, Justice Scalia held that by placing an electronic tracking device on a vehicle for a period of twenty-eight days, the government had trespassed and it constituted a search.[264] In *Jones*, the government argued that the vehicle's driver had no reasonable expectation of privacy because the vehicle traveled on public roads and was visible to all.[265] The majority reached its decision by returning to the trespassory test,[266] stating that *Katz* did not narrow the Fourth Amendment's scope or change the principle that when the government physically intrudes into a constitutionally protected area, the Fourth Amendment is implicated.[267] According to Justice Scalia, relying on the trespassory test, rather than the reasonable expectation of privacy test, avoids the "thorny problem" presented by *Katz*'s open-ended inquiry and leaves for a future case the question of how much surveillance is reasonable.[268]

The Court's decision in *Jones* left unanswered the question of when ongoing surveillance becomes a search.[269] It also did not address surveillance that occurs without a physical intrusion.[270] Justice Sotomayor's concurrence in *Jones* notes that because physical intrusion is now unnecessary to many forms of surveillance, the majority's physical trespass test provides little guidance in cases presenting novel methods of surveillance.[271] According to the majority, "[s]ituations involving merely the transmission of electronic signals without trespass would *remain* subject to *Katz* analysis."[272] Justice Sotomayor's concurrence also raised the question of informational privacy, warning that the "government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse."[273] After the Court's decision in *Jones*, there are two tests for determining if a search has occurred for Fourth Amendment purposes: the trespassory test and the reasonable expectation of privacy test.[274]

---

263. 565 U.S. at 409.

264. *Id.* at 403–04.

265. *Id.* at 406.

266. *Id.* at 404.

267. *Id.* at 407–08.

268. *Id.* at 412–13.

269. KURIHARA & ALBANO, *supra* note 245, at 21.

270. *Jones*, 565 U.S. at 425 (Alito, J., concurring in the judgment) (noting the majority's decision still provided no protection from long-term government monitoring that could be accomplished "without committing a technical trespass").

271. *Id.* at 414–15 (Sotomayor, J., concurring).

272. *Id.* at 411 (alteration in original).

273. *Id.* at 416 (Sotomayor, J., concurring). Justice Sotomayor went on to state,

> [W]hen considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements[,] I 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.

*Id.*

274. *See id.* at 409.

## B. AERIAL SURVEILLANCE AND HIGH-TECH SURVEILLANCE DOCTRINES

The Supreme Court applied the *Katz* reasonable expectation of privacy test to three key cases in the 1980s, which form the basis for its current aerial surveillance doctrine: *California v. Ciraolo*,[275] *Dow Chemical Co. v. United States*,[276] and *Florida v. Riley*.[277] Additionally, the Court examined the government's use of sense-enhancing technology in *Kyllo v. United States*[278] and its ability to surveil retroactively in *Carpenter v. United States*.[279] Because law enforcement can use UAS both to conduct aerial surveillance and as a platform for sense-enhancing technology, this Note will examine each case in turn. In general, the Court has remained consistent to its understanding that "mere visual observation does not constitute a search."[280]

In *California v. Ciraolo*, the Court held that police flying in a fixed-wing aircraft 1,000 feet above an individual's home and yard deliberately looking for marijuana plants did not constitute a search.[281] At common law, the small area immediately adjacent to a home is its curtilage and enjoys a heightened expectation of privacy.[282] However, the Court opined that the fact that an area is within curtilage was not a bar to all police observation.[283] The Court applied the *Katz* framework and held that the expectation of privacy was not reasonable, even though the yard had high double fences, because any member of the public flying overhead could have observed exactly what the officers did.[284] "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."[285]

In a companion case to *Ciraolo*, the Court held that aerial photography of Dow Chemical's plant complex conducted by the U.S. Environmental Protection Agency was not a search for Fourth Amendment purposes.[286] Dow argued that its 2,000-acre plant complex was industrial curtilage[287] entitled to heightened constitutional protection, similar to the curtilage of a private home.[288] Applying the *Katz* test, the Court concluded Dow had a "reasonable, legitimate, and

275. 476 U.S. 207 (1986).
276. 476 U.S. 227 (1986).
277. 488 U.S. 445 (1989).
278. 533 U.S. 27 (2001).
279. 138 S. Ct. 2206 (2018).
280. United States v. Jones, 565 U.S. 400, 412 (2012).
281. 476 U.S. 207, 209–10 (1986).
282. *Id.* at 212–13.
283. *Id.*
284. *Id.*
285. *Id.* at 213.
286. Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).
287. Curtilage is contrasted with open fields: "[O]pen fields do not provide the setting for those intimate activities that the [Fourth] Amendment is intended to shelter from governmental interference or surveillance." *Id.* at 235 (alteration in original) (quoting Oliver v. United States, 466 U.S. 170, 179 (1984)). The *Dow Chemical* Court noted that Dow's industrial complex fell somewhere between curtilage and open fields. *Id.* at 236.
288. *Id.* at 235.

objective expectation of privacy within the interior of its covered buildings," but not to the open areas of the plant complex.[289] The Court opined that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public" might require a warrant, but that the photographs at issue were "not so revealing of intimate details as to raise constitutional concerns."[290] The dissent warned that determining "the existence of an asserted privacy interest . . . solely by reference to the manner of surveillance used to intrude on that interest" would erode Fourth Amendment rights as technology advanced.[291]

Three years later in *Florida v. Riley*, the Court held that flying a helicopter just 400 feet above a partially-covered greenhouse was not a search, reaffirming its decision in *Ciraolo*.[292] Although the property searched was within the curtilage of the home, because the roof and sides of the greenhouse were left partially open, the Court held that the defendant had no reasonable expectation of privacy since private and commercial flight by helicopter were not "unheard of" in the area.[293] Because it was navigable airspace and any member of the public could legally have flown over the property in a helicopter at an altitude of 400 feet and observed the defendant's greenhouse, the police officer also legally could.[294] In her concurrence, Justice O'Connor reasoned that the inquiry should not be whether the helicopter could conceivably observe the curtilage without violating FAA regulations, but whether the aircraft was "in the public airways at an altitude at which members of the public travel with sufficient regularity" that defendant's expectation of privacy was not objectively reasonable.[295]

While *Ciraolo*, *Dow Chemical*, and *Riley* all involved either naked-eye observation or camera, the Court examined the government's use of sense-enhancing technology in *Kyllo*, twelve years later.[296] The case considered the legality of the government's use of a thermal imager, which detects infrared radiation and operates like a video camera, to show heat images inside a home.[297] The scan was performed from the officer's parked vehicle across the street and showed that parts of the defendant's home were hot compared to the rest of the three-unit dwelling, leading to an inference that halide lights were being used to

289. *Id.* at 236, 239.

290. *Id.* at 238.

291. *Id.* at 240 (Powell, J., concurring in part and dissenting in part).

292. Florida v. Riley, 488 U.S. 445, 449 (1989).

293. *Id.* at 450.

294. *Id.* at 450–51.

295. *Id.* at 454 (O'Connor, J., concurring in the judgment). Justice O'Connor went on to say that the defendant has the burden of proving his expectation is reasonable and because *Riley* had introduced no evidence to the contrary, his expectation was not reasonable. *Id.* This seems to leave open the question of whether an individual can offer evidence to show that aircraft are not flown over his home with sufficient regularity to render his expectation of privacy reasonable.

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

297. *Id.*

grow marijuana inside.[298] The thermal scans, along with other evidence, formed the basis to obtain a search warrant of the home, where police found more than one hundred marijuana plants.[299] Here, the Court held that the government's use of a "device that is not in general public use, to explore details of the home that would previously have been unknowable without physical intrusion" constituted a search for Fourth Amendment purposes "and is presumptively unreasonable without a warrant."[300]

In 2018, the Court held in *Carpenter* that a person has a "reasonable expectation of privacy in the whole of his physical movements."[301] There, the government obtained by court order the defendant's historical cell-site records from wireless carriers for 127 days, providing the government with 12,898 location points cataloging his daily movements.[302] The Court noted the unique privacy concerns posed by the government's ability to access information and "travel back in time to retrace a person's whereabouts."[303] Applying *Katz's* reasonable expectation of privacy test, the Court reasoned that the government's access to cell-site records infringes on that expectation, giving the government an "intimate window into . . . [a person's] 'familial, political, professional, religious, and sexual associations,'" thus revealing "'the privacies of life.'"[304] Because the government invaded the defendant's reasonable expectation of privacy in his physical movements, the Court held that a Fourth Amendment search occurred[305] and the government must obtain a warrant supported by probable cause before acquiring cell-site location information.[306]

In *Carpenter*, the Court provided two guideposts for determining which expectations of privacy are protected, based on historical understanding of the Fourth Amendment at the time of its adoption.[307] First, the Fourth Amendment secures the "'privacies of life' against 'arbitrary power.'"[308] Second, the Framers intended to place obstacles in the way of "too permeating police surveillance."[309] The Court kept these guideposts in mind when applying the Fourth Amendment in *Carpenter* and will likely continue to do so when considering future innovations in surveillance.[310]

### C. LOWER COURT DECISIONS SINCE *CIRAOLO*, *DOW CHEMICAL*, *RILEY*, AND

298. *Id.*
299. *Id.*
300. *Id.* at 40.
301. Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).
302. *Id.* at 2212.
303. *Id.* at 2218.
304. *Id.* at 2217 (first quoting United States v. Jones, 565 U.S. 400, 415 (2012); then quoting Riley v. California, 134 S. Ct. 2473, 2495 (2014)).
305. *Id.* at 2219–20.
306. *Id.* at 2221.
307. *Id.* at 2214.
308. *Id.* (quoting Boyd v. United States, 116 U.S. 616, 630 (1886)).
309. *Id.* (internal quotation marks omitted) (quoting United States v. Di Re, 332 U.S. 581, 595 (1948)).
310. *See id.*

*KYLLO*

The Court has not decided a case involving the government's use of aerial surveillance in almost thirty years.[311] Thus, the current aerial surveillance doctrine is largely based on outdated assumptions regarding manned aircraft, only some of which apply to unmanned aircraft.[312] Similarly, there have been no decisions regarding sense-enhancing technology since 2001.[313] As technology continues to advance and methods of surveillance become more sophisticated, lower courts must decide warrantless surveillance cases in light of either the trespassory test used in *Jones*, or the reasonable expectation of privacy test the Court applied in *Ciraolo*, *Dow Chemical*, and *Riley*.[314] An interpretation of these cases by one city attorney's office to the League of California Cities summarizes the current constitutional framework:

> Based on these cases one can glean that police may engage in the following activities without a warrant: fly a drone within legally permissible airspace to conduct visual surveillance of outdoor property (*Ciraolo*, *Dow Chemical*, *Riley*); use sense-enhancing technology to observe certain exterior details of property, as long as technology is in general public use (*Dow Chemical*, *Kyllo*); and conduct short-term ongoing surveillance (some period less than 4 weeks) (*Jones* concurrence). However, from a private citizen's perspective, such usage may be unsettling.[315]

Thus, under current Fourth Amendment doctrine, there is likely little protection from warrantless drone surveillance.[316] Under the trespassory test, the small, lightweight drones popular with law enforcement are unlikely to cause a physical intrusion.[317] Under the *Katz* test, there is no reasonable expectation of privacy in what a person exposes to public view,[318] even if an officer must be

311. The last aerial surveillance case the Court decided was *Florida v. Riley*, 488 U.S. 445 (1989).

312. Schoen & Tooshi, *supra* note 3, at 4.

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

314. *See, e.g.*, United States v. Garcia-Gonzalez, No. 14-10296-LTS, 2015 WL 5145537, at *23 (D. Mass. Sept. 1, 2015) ("[I]n the face of advancing technology, 'what a person knowingly exposes to the public,' engenders profoundly different ramifications than it did in 1967, when *Katz* was decided." (citing Katz v. United States, 389 U.S. 347, 351 (1967))).

315. ALBANO & KURIHARA, *supra* note 245, at 21.

316. According to a report prepared by the Congressional Research Service, which cited *Kyllo*, drones outfitted with especially powerful cameras and thermal imagers that can see through walls would probably constitute a search because they are not generally available to the public. THOMPSON II, *supra* note 58, at 13. However, the use of lower-powered cameras and less sophisticated technology to view people and objects visible from public airways are likely not protected by the Fourth Amendment. *Id.*

317. *See* State v. Davis, 360 P.3d 1161, 1171 (N.M. 2015) ("[W]hen low-flying aerial activity leads to more than just observation and actually causes an unreasonable intrusion on the ground—most commonly from an unreasonable amount of wind, dust, broken objects, noise, and sheer panic—then at some point courts are compelled to step in and require a warrant.").

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

perched in a high place to gain that view[319] unless "the whole of [a person's] physical movements" are invaded.[320]

Only a fraction of states and a handful of local governments have enacted laws regulating law enforcement's use of UAS; of these, some still provide no further protection than the Fourth Amendment.[321] To date, there have been no published court opinions addressing whether the use of UAS by local law enforcement to conduct surveillance implicates the Fourth Amendment.[322] However, the lower court decisions applying the Supreme Court's Fourth Amendment doctrine to both manned aircraft and pole-top cameras demonstrate there is no clear framework in place that can be consistently applied to the more complicated issue of UAS.[323] Because the *Carpenter* decision is so recent,[324] it is unclear how lower courts would apply the guideposts the Court offered for determining whether an innovation in surveillance invades a constitutionally protected area.

### *1. Aerial Surveillance Using Helicopters*

Since the decisions in *Ciraolo*, *Dow Chemical*, and *Riley*, state courts have taken differing approaches in determining whether a search has occurred when law enforcement uses helicopters to conduct aerial surveillance.[325] Some courts rely solely on whether the helicopter was in public airspace,[326] holding the search is reasonable if police are in a place "they have a right to be."[327] Other state courts have relied on considering the intrusiveness of the search as articulated by the *Riley* Court, including the duration of flight and whether it created noise or wind, or otherwise interfered with the defendant's use of the property.[328] A remaining group of states have articulated their own factors for determining whether a search has occurred, such as giving weight to whether

319. Even fences do not provide a reasonable expectation of privacy for Fourth Amendment purposes from overhead surveillance. *See* California v. Ciraolo, 476 U.S. 207, 211 (1986) (observing that respondent's 10-foot fence might not have shielded his marijuana plants from view of a policeman perched at a higher vantage point).

320. *See* Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018).

321. *See supra* Subparts I.D.2, I.D.3.

322. The Author conducted numerous searches using legal databases, the most recent on LexisAdvance on November 16, 2018, searching all federal and state reported cases using search terms "drone or UAS and surveillance and 'Fourth Amendment.'" *Cf.* Scott Bomboy, *A Legal Victory for Drones Warrants a Fourth Amendment Discussion*, NAT'L CONST. CTR.: CONST. DAILY (Feb. 7, 2014), https://constitutioncenter.org/blog/a-court-victory-for-drones-warrants-a-fourth-amendment-discussion (reporting a state court case in North Dakota where the judge upheld the admission of evidence gathered by a drone without a warrant).

323. *See supra* Subparts II.C.1, II.C.2.

324. *Carpenter*, 138 S. Ct. 2206, was decided on June 22, 2108.

325. *See* State v. Bryant, 950 A.2d 467, 476 (Vt. 2008) (providing an overview of the different approaches taken by state courts to aerial surveillance).

326. *Id.* (citing State v. Ainsworth, 801 P.2d 749, 750–52 (Or. 1990)); *see also* Commonwealth v. Oglialoro, 579 A.2d 1288, 1292 (Pa. 1990) ("As long as the police have the right to be where they are, and the activity is clear and visible, the fact they are peering into curtilage is of no significance.").

327. *E.g.*, *Ainsworth*, 801 P.2d at 751.

328. *Bryant*, 950 A.2d at 478.

"concentrating a surveillance on a particular place, as opposed to random investigation to discover criminal activity" is justified.[329] The state courts' applications of the Supreme Court's current aerial surveillance doctrine shows the issue is far from settled.

Even within the same state, courts may still disagree on which test to use. For example, in *State v. Davis*, the New Mexico state courts considered the legality of a search where police used a helicopter to conduct aerial surveillance looking for marijuana plants.[330] The defendant was home and stated he heard a helicopter flying low over his house and making "a considerable racket."[331] He observed the helicopter about fifty feet "above his head 'kicking up dust and debris that was swirling all around.'"[332] Nearby residents described the helicopter flyovers as "terrifying and highly disruptive" and stated that the downdraft caused physical damage to their properties.[333] Both the Court of Appeals of New Mexico and the New Mexico Supreme Court held the search was unconstitutional, but they reached this conclusion on different bases.[334]

The New Mexico Court of Appeals applied *Katz*'s reasonable expectation of privacy test and held the search did not violate the Fourth Amendment because what was observed was in open view and the defendant's expectation of privacy from the air was unreasonable.[335] However, the court held the search violated New Mexico's Constitution[336] because the government intended to obtain information through aerial surveillance that it could not have obtained without a physical intrusion into the home or curtilage.[337] The New Mexico Supreme Court used an intrusion analysis and held that the search violated the Fourth Amendment.[338] The court held that when aerial surveillance by police

329. *Id.* at 478 (quoting Commonwealth v. One 1985 Ford Thunderbird Auto., 624 N.E.2d 547, 551 (Mass. 1993)).

330. 360 P.3d 1161, 1164 (N.M. 2015).

331. *Id.* (internal quotation marks omitted).

332. *Id.*

333. *Id.* at 1164–65.

334. *Id.* at 1172.

335. *See* State v. Davis, 321 P.3d 955, 959 (N.M. Ct. App. 2014), *aff'd in part*, *rev'd in part*, *Davis*, 360 P.3d 1161.

336. N.M. CONST. art. II, § 10 ("The people shall be secure in their persons, papers, homes and effects, from unreasonable searches and seizures, and no warrant to search any place, or seize any person or thing, shall issue without describing the place to be searched, or the persons or things to be seized, nor without a written showing of probable cause, supported by oath or affirmation."); *see also Davis*, 321 P.3d at 961 ("We fail to see how an analysis of intrusiveness factors aids in the determination of whether an aerial surveillance is a search. The privacy interest protected by Article II, Section 10 is not limited to one's interest in a quiet and dust-free environment. It also includes an interest in freedom from visual intrusion from targeted, warrantless police aerial surveillance, no matter how quietly or cleanly the intrusion is performed.").

337. *Davis*, 321 P.3d at 962.

338. The New Mexico Supreme Court rejected the Court of Appeals' suggestion to "move away from an intrusion analysis in anticipation of future surveillance conducted by 'ultra-quiet drones' and other high-tech devices." *Davis*, 360 P.3d at 1172. But, because the case before the court involved surveillance only by helicopters, it was "unnecessary to speculate about problems—and futuristic technology—that may or may not arise in the future." *Id.* Instead, the court decided to "reserve judgement and await a proper case with a developed record." *Id.*

goes beyond a brief flyover and involves prolonged hovering close enough to the ground to cause interference with the property, a search occurs.[339] The court concluded that the dust and disturbance caused by the helicopter demonstrated that an unconstitutional intrusion under the Fourth Amendment had occurred, making it unnecessary to consider whether the search also violated the state's constitution.[340]

### *2. Aerial Surveillance Using Pole-Top Cameras*

Pole-top cameras are similar to drones in that they are capable of observing and recording from overhead and can be used without a physical trespass.[341] The lack of consensus regarding the constitutionality of surveillance using pole-top cameras in lower courts foreshadows the likelihood that courts will be divided when confronting UAS surveillance in the absence of clear guidance from legislatures or the United States Supreme Court. Some courts have applied the *Katz* test and held there is a reasonable expectation of privacy in the curtilage of one's home, which is violated when the government uses a camera to record activity for an extended period of time.[342] Other courts have held that the Fourth Amendment is not violated when law enforcement uses a camera to record what is exposed to public view,[343] despite the length of the surveillance involved, even while noting the government's conduct was "highly intrusive."[344]

In an early case involving the use of a pole-top camera to surveil a suspected drug trafficker, the Fifth Circuit held that the Fourth Amendment's protections extend to activities conducted in the defendant's backyard.[345] Federal agents had placed a camera on a utility pole that overlooked the 10-foot-high fence surrounding the defendant's yard.[346] The government argued that

339. *Id.*

340. *Id.* The New Mexico Supreme Court inferred from *California v. Ciraolo*, 476 U.S. 207 (1986), and *Florida v. Riley*, 488 U.S. 445 (1989) that:

> [T]he Fourth Amendment affords citizens no reasonable expectation of privacy from aerial surveillance conducted in a disciplined manner—mere observation from navigable airspace of an area left open to public view with minimal impact on the ground. It also seems, however, that warrantless surveillance can go beyond benign observation in a number of different ways, one of those being when surveillance creates a "hazard"—a physical disturbance on the ground or unreasonable interference with a resident's use of his property. In that case, surveillance more closely resembles a physical invasion of privacy which has always been a violation of the Fourth Amendment.

*Davis*, 360 P.3d at 1169.

341. *See* United States v. Vargas, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672, at *2, *16 (E.D. Wash. Dec. 15, 2014).

342. *See, e.g.*, United States v. Cuevas-Sanchez, 821 F.2d 248, 250–51 (5th Cir. 1987) (concluding the defendant had a reasonable expectation of privacy when a camera was pointed at his backyard for eight weeks); *Vargas*, 2014 U.S. Dist. LEXIS 184672, at *16–17 (holding the defendant had a reasonable expectation of privacy when a camera was pointed at his front yard for six weeks).

343. United States v. Wymer, 40 F. Supp. 3d 933, 939 (N.D. Ohio 2014).

344. *Id.* at 936.

345. *Cuevas-Sanchez*, 821 F.2d at 251.

346. *Id.* at 250.

under *Ciraolo*, it was not a search because portions of the yard were visible from the street and a power company lineman on top of the pole or a policeman on top of a truck could have peered over the fence.[347] The court considered this argument to be stretching *Ciraolo* "far beyond its natural reach" because the intrusion was not a minimal, one-time overhead flight from 1,000 feet, but the type of "indiscriminate video surveillance [that] raises the spectre of the Orwellian state."[348] According to the court, the defendant's expectation "to be free from *this type* of video surveillance in his backyard is one that society is willing to recognize as reasonable."[349] Indeed, the court characterized this type of monitoring—recording all of the backyard activities for almost sixty days—as provoking an "immediate negative visceral reaction," opining that just because a brief, one-time overhead flight was permissible under *Ciraolo*, it does not follow that far more intrusive aerial surveillance is permissible.[350]

Similarly, a district court in Washington held that installing a pole-top camera 150-feet away from the defendant's home was a search for Fourth Amendment purposes because "[t]he American people have a reasonable expectation of privacy in the activities occurring in and around the front yard of their homes particularly where the home is located in a very rural, isolated setting."[351] Here, police installed a hidden camera on a telephone pole which recorded everything in the defendant's unfenced front yard and transmitted it to the police station twenty miles away.[352] Detectives could rotate and zoom the camera remotely, controlling it via computer, and recorded continuously for six weeks.[353] Finding the trespassory test was not applicable because a physical trespass did not occur, the court applied the reasonable expectation of privacy test.[354] The court ruled that given the invasive nature of the surveillance, whether or not the front yard was included in the home's curtilage was not controlling.[355] The court distinguished the challenged surveillance from the observations permitted in *Ciraolo* because the view the detective had in the instant case was "so different in its intrusiveness that it does not qualify as a plain-view observation."[356] The court determined that the defendant's conduct over the six-

347. *Id.*

348. *Id.* at 250, 251.

349. *Id.* at 251 (emphasis added). The Fifth Circuit upheld the search here because the government had obtained a court order and there was no evidence the government continued the surveillance after the proscribed thirty-day period ended and before it obtained an extension. *Id.* at 252.

350. *Id.* at 251.

351. United States v. Vargas, No. CR-13-6025-EFS, 2014 U.S. Dist. LEXIS 184672, at *3 (E.D. Wash. Dec. 15, 2014).

352. *Id.* at *6.

353. *Id.* at *6–7.

354. *Id.* at *16.

355. *Id.* at *17–18. The court did go on to apply the four factors set forth in *United States v. Dunn*, 480 U.S. 294, 300 (1987), and hold that the defendant's property here was curtilage. *Id.* at *19–22.

356. *Id.* at *27.

week period manifested a subjective expectation of privacy.[357] The court reasoned that society expects law enforcement's continuous and covert surveillance of an individual's front yard for such an extended period to be judicially approved, and thus the objective prong of the *Katz* reasonable expectation of privacy test was also satisfied.[358] Acknowledging that the surveillance would have passed Fourth Amendment muster if the officer himself had actually sat atop the pole, the court observed that the likelihood of such an effort going unnoticed by the defendant was remote.[359]

Other courts have reached the opposite conclusion and have upheld the warrantless use of pole-top cameras because there is no reasonable expectation of privacy in an area that is exposed to public view.[360] The defendant in one such case argued that the camera *actually* trespassed by entering the premises for the purposes of obtaining information, but the district court found this argument lacking in merit because the camera was not installed on his property and there can be no trespassory search without a trespass.[361] The court also analyzed the defendant's claim that the government's use of the camera violated his reasonable expectation of privacy.[362] Because it was a commercial property and exposed to public view, the court held the defendant had no reasonable expectation of privacy.[363] While the court opined about the "intrusive nature" of the round-the-clock surveillance, with the camera recording continuously for nearly five months, it concluded that, under current and prevailing law, the use of long-term video surveillance to monitor the open and exposed commercial property did not constitute a search.[364]

The First Circuit in *United States v. Bucci* also held that video surveillance from a pole-top camera for a period of eight months did not violate the Fourth Amendment, even though the camera afforded law enforcement a view inside the defendant's garage when the door was open.[365] Following this decision, a district court in that circuit also held that warrantless surveillance using a pole-

357. *Id.* at *17. The court noted that the defendant used the yard for target practice and socializing with friends and that the fact that one of the defendant's guests urinated near the fence underscored the expectation that it was a private activity. *Id.* at *20–21.

358. *Id.* at *17.

359. *Id.* at *26. The court commented, "Although having an agent sit on top of a telephone pole may seem far afield, it is consistent with Justice Scalia's 'constable' example in *Jones*." *Id.* (citing United States v. Jones, 565 U.S. 400, 406 n.3 (2012)).

360. *See, e.g.*, United States v. Wymer, 40 F. Supp. 3d 933, 939–40 (N.D. Ohio 2014).

361. *Id.* at 938; *see also id.* at 936 ("Despite my considerable reservations about the failure of the officers to have secured a warrant to conduct such highly intrusive surveillance, I conclude I must, in light of controlling law, deny the motion [to suppress].").

362. *Id.* at 938.

363. *Id.* at 939–40.

364. *Id.* at 942. Although the defendant testified he had been sleeping in a recreational vehicle on the property for four months, the court characterized his testimony as "vague and uncertain" and determined the property was commercial; thus, the defendant had a "diminished expectation of privacy in his activities there." *Id.* at 939.

365. 582 F.3d 108, 116–17 (1st Cir. 2009).

top camera did not violate the Fourth Amendment,[366] even though it considered the approach and analysis of courts which had found a reasonable expectation of privacy in such cases to be persuasive.[367] In the district court case, the defendant urged the court to adopt Justice Sotomayor's reasoning in her concurrence to *Jones*,[368] in which she warned that the government's ability to "assemble data that reveal private aspects of identity is susceptible to abuse."[369] The defendant argued the pole-top camera captured more than what he exposed to public view; it captured "the aggregate of all of his coming and going from the home, . . . all types of intimate details of [his] life."[370] The court agreed the surveillance was intrusive, acknowledging that "the pole camera was akin to stationing a police officer at the front door by whom every person and object must pass"[371] and that the "secret nature of the surveillance prevent[ed] the target from choosing to shield his behavior from public view."[372] Nonetheless, the court held the search was constitutional because it was bound by First Circuit precedent that there is no reasonable objective expectation of privacy when the camera captures what is visible to the public.[373]

In light of the fact that lower courts disagree about whether warrantless aerial surveillance for a prolonged period of time violates the Fourth Amendment,[374] there seems to be an inherent contradiction in policies advising police officers to obtain a warrant when the Fourth Amendment requires it, or in law enforcement agencies promising to self-police when a warrant is necessary.[375] *If experienced judges who wrestle with constitutional questions on a daily basis cannot know what is constitutional, how can law enforcement?* For example, current LAPD policy guidelines require officers to obtain a warrant before using a drone "when required under the Fourth Amendment or other provision of the law."[376] As one observer pointed out, LAPD's policy "looks all well and good, except that the Fourth Amendment and California law provide little protection when it comes to aerial surveillance."[377]

366. United States v. Garcia-Gonzalez, No. 14-10296-LTS, 2015 U.S. Dist. LEXIS 116312, at *27 (D. Mass. Sept. 1, 2015).

367. *Id.* at *25.

368. *Id.* at *14–15.

369. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

370. *Garcia-Gonzalez*, 2015 U.S. Dist. LEXIS 116312, at *15.

371. *Id.* at *16.

372. *Id.* at *18.

373. *Id.* at *28–29 (citing United States v. Bucci, 582 F.3d 108, 116–17 (1st Cir. 2009)).

374. *See supra* Subpart II.C.

375. *See, e.g.*, MIKE DEWINE, OHIO ATTORNEY GEN., ADVISORY GROUP ON UNMANNED AIRCRAFT SYSTEMS 5 (2018), http://www.ohioattorneygeneral.gov/Files/Publications-Files/Publications-for-Law-Enforcement/Advisory-Group-on-Unmanned-Aircraft-Systems-Final; Douglass, *supra* note 71.

376. L.A. POLICE DEP'T, *supra* note 70, at 3.

377. Matthew Feeney, *LAPD Drones Threaten Privacy*, CATO INST. (Oct. 17, 2017, 4:59 PM), https://www.cato.org/blog/lapd-drones-threaten-privacy.

Similarly, because the Ohio legislature failed to provide guidance,[378] the Ohio Attorney General created a model law enforcement policy with specific recommendations for departments to develop and implement their own written policies to address privacy concerns.[379] It stated that "[l]aw enforcement agencies should obtain a search warrant before any use where people would have a reasonable expectation of privacy."[380] The ACLU criticized the model policy and regulations as "inadequate" because they fail to "address the potential for widespread or around-the-clock surveillance."[381] The ACLU noted that under current case law, there is virtually no reasonable expectation of privacy once a person sets foot outside their home.[382]

Thus, policies advising police officers to obtain a warrant before using a drone "where an individual has a reasonable expectation of privacy"[383] offer only circular logic and little practical guidance. Because drone surveillance is unlikely to involve a physical trespass, courts would likely apply the *Katz* test. Even the limited protection the *Katz* test might afford could diminish over time. As Justice Alito noted in his partial concurrence in *Jones*, the reasonable expectation of privacy test "involves a degree of circularity"[384] because technology changes what society expects and will accept as reasonable. The increasing popularity of drones with law enforcement and non-governmental actors may erode the public's privacy expectations as they become more commonly seen in the airspace, altering whether society is prepared to recognize a person's expectation of privacy as objectively reasonable.[385] If law enforcement is permitted to use technology to increase public safety at the expense of privacy, the public may come to view the intrusion as inevitable.[386]

## III. THE SOLUTION: STATE-BASED STANDARDS

### A. STATE LEGISLATURES ARE IN THE BEST POSITION TO SAFEGUARD PRIVACY AND PRESERVE UAS AS A TOOL FOR LAW ENFORCEMENT

Legislation regulating law enforcement's use of UAS should be enacted at the state level, as an exercise of the states' police power. Reliance on administrative policies to safeguard individual privacy[387] or on law enforcement

378. Barrie Barber, *Ohio Gives Police Agencies Guidelines on Drone Use*, DAYTON DAILY NEWS (Jan. 29, 2018), http://www.daytondailynews.com/news/local/ohio-gives-police-agencies-guidelines-drone-use/zpg7zCSnaEbYwCqFQkKxqK ("It was an emerging issue that there was no model policy in Ohio.") (quoting a spokesman for the attorney general)).

379. DEWINE, *supra* note 375.

380. *Id.* at 5.

381. Barber, *supra* note 378.

382. *Id.*

383. DEWINE, *supra* note 375, at 5.

384. United States v. Jones, 565 U.S. 400, 427 (2012) (Alito, J., concurring in the judgment).

385. *See* Katz v. United States, 389 U.S. 347, 361 (1967) (Harlan, J., concurring).

386. *Jones*, 565 U.S. at 427 (Alito, J., concurring in the judgment).

387. *See* STANLEY & CRUMP, *supra* note 36, at 12 (noting the potential for institutional abuse of surveillance technology by government agencies).

to police itself is an insufficient safeguard for Fourth Amendment freedoms.[388] Cases applying Fourth Amendment jurisprudence to technology-based surveillance have produced inconsistent results, as the pole-top camera cases demonstrate.[389] Drone technology is advancing at such a rapid rate[390] that any court decisions analyzing whether surveillance goes too far and becomes a search would likely be outdated by the time an opinion is rendered.[391] As a free society, we are dependent upon our civil liberties,[392] which are threatened by law enforcement's ability to engage in "mass tracking" of Americans, absent any evidence of wrongdoing.[393] Civil liberties are too important to wait decades for the Supreme Court's jurisprudence to catch up to UAS. In light of the unique capabilities of drone technology and the privacy interests at stake, the public should look to the law to provide clear boundaries for permissible governmental use of drone technology.[394]

The federal government has failed to address privacy concerns with respect to drones, despite requests from privacy advocates as early as 2012.[395] Congress is divided as to whether the federal government or states are the appropriate actor to enact legislation regulating law enforcement's use of drones, with some viewing it as a question of federalism.[396] Even if Congress could successfully pass legislation regulating this issue, such regulation would likely be challenged by those who view it as the federal government overstepping its constitutionally

---

388. *See* Kathryn Watson, *What Is the Future of Privacy, Surveillance and Policing Technologies Under Trump?*, CBS NEWS (June 22, 2017, 6:00 AM), https://www.cbsnews.com/news/future-of-privacy-surveillance-and-policing-technologies-trump (citing comments of Matthew Feeney, a policy analyst at the Cato Institute).

389. *See supra* Subpart II.C.2.

390. STANLEY & CRUMP, *supra* note 36, at 4.

391. UAVs can be equipped with:

> [I]ncreasingly powerful lenses that allow significant zooming, increasing the chance that individuals will come under scrutiny from faraway aircraft without knowing it. And the density of photo sensors is growing at an exponential pace (in line with Moore's law), allowing for higher and higher resolution photos to be taken for the same price camera.

ACLU, *supra* note 109, at 5 (citing Nathan Myhrvold, *Moore's Law Corollary: Pixel Power*, N.Y. TIMES (June 7, 2006), https://www.nytimes.com/2006/06/07/technology/circuits/07essay.html). Moore's law stands for the proposition that the power of computers doubles every two years. *Id.* Applying this to digital cameras, the technology will continue to advance at such a rate that court decisions will always be based on outdated assumptions.

392. Laird v. Tatum, 408 U.S. 1, 24 (1972) (Douglas. J., dissenting).

393. Marguerite Rigoglioso, *Civil Liberties and Law in the Era of Surveillance*, STAN. LAW. (Nov. 13, 2014), https://law.stanford.edu/stanford-lawyer/articles/civil-liberties-and-law-in-the-era-of-surveillance (citing comments of Catherine Crump, staff attorney for the ACLU).

394. *See* STANLEY & CRUMP, *supra* note 36, at 15.

395. *See* Petition to Michael P. Huerta, Acting Adm'r, Fed. Aviation Admin. (Feb. 24, 2012), https://epic.org/apa/lawsuit/EPIC-FAA-Drone-Petition-March-8-2012.pdf (petitioning the FAA to "conduct a rulemaking to address the threat to privacy and civil liberties that will result from the deployment of aerial drones within the United States").

396. *See, e.g.*, Drone Aircraft Privacy and Transparency Act of 2017, S. 631, 115th Cong. (2017); Drone Federalism Act of 2017, S. 1272, 115th Cong. (2017); Preserving Freedom from Unwanted Surveillance Act of 2013, S. 1016, 113th Cong. (2013); Preserving Freedom from Unwanted Surveillance Act of 2013, H.R. 972, 113th Cong. (2013); Preserving Freedom from Unwanted Surveillance Act of 2013, S. 1016, 113th Cong. (2013).

prescribed role[397] and regulating an area left to the states under federalist principles.[398] Privacy is an area traditionally related to state and local police power,[399] and has only been subject to federal regulation in limited circumstances.[400] Further, any federal legislation would likely be criticized as a one-size-fits-all solution for states with differing constitutional privacy protections (which reflect their constituents' differing views of privacy)[401] and geography.[402]

Nor would regulation on the local level prove effective. Allowing local municipalities to regulate law enforcement's use of drones would create an inconsistent patchwork of regulations, which could not only impair safety in the NAS but would wreak havoc on reasonable expectations of privacy. For example, it would not be reasonable to expect the average resident of Seattle to know whether a city an hour away, which he or she might visit occasionally, permits warrantless drone surveillance, unlike the robust protection that same person enjoyed at home.[403] Also, consider the issue of an individual on the outskirts of a locality where warrantless drone surveillance is prohibited, yet the neighboring police department could record that person's movements from a

397. Garcia v. San Antonio Metro. Transit Auth., 469 U.S. 528, 550–51 (1985) ("[T]he composition of the Federal Government was designed in large part to protect the States from overreaching by Congress.").

398. Scott Gaylord, Opinion, *States Need More Control over the Federal Government*, N.Y. TIMES, https://www.nytimes.com/roomfordebate/2013/07/16/state-politics-vs-the-federal-government/states-need-more-control-over-the-federal-government?mcubz=0 (last updated July 17, 2013, 8:54 AM) (citing states' challenges to the Affordable Care Act and various actions of the Environmental Protection Agency); *see also* Hall, *supra* note 162, at 2.

399. Operation and Certification of Small Unmanned Aircraft Systems, 81 Fed. Reg. 42064, 42194 (June 28, 2016) (to be codified at 14 C.F.R. pts. 21, 43, 61, 91, 101, 107, 119, 133, 183) ("[L]aws traditionally related to State and local police power—including land use, zoning, privacy, trespass, and law enforcement operations—generally are not subject to Federal regulation."). Interestingly, this exact language was quoted by the federal district court in *Singer v. City of Newton*, 284 F. Supp. 3d 125, 130 (D. Mass. 2017), even though it struck down portions of a city ordinance regulating drones because the ordinance was preempted by a federal regulation, *id.* at 133. Some have criticized the opinion as flawed, because it relied on a provision in the U.S. Code that was miscodified to conclude that "Congress extensively controls much of the field," and relied on an amorphous definition of "national airspace." Stephen Migala, *A Critical Review of the 1st Drone Preemption Case,* LAW360 (Dec. 1, 2017, 12:50 PM), https://www.law360.com/publicpolicy/articles/989147?utm_source=rss&utm_medium=rss&utm_campaign=section (citing *Newton*, 284 F. Supp. 3d at 129).

400. *See, e.g.*, Privacy Act of 1974, 5 U.S.C. § 552a (2012) (regulating the collection, maintenance, use, and dissemination of personal information collected by the federal government).

401. For example, Hawaii's Supreme Court has rejected the third-party doctrine as inconsistent with the privacy protection afforded in article 1, section 7 of the Hawaii Constitution. State v. Walton, 324 P.3d 876, 901 (Haw. 2014). In comparison, the Supreme Court of the United States affirmed in both *United States v. Miller*, 425 U.S. 435 (1976) and *Smith v. Maryland*, 442 U.S. 735 (1979) that an individual has no expectation of privacy in information voluntarily conveyed to a third party. In *Walton*, the Hawaii Supreme Court also observed that drones may soon become too numerous to sustain a claim of expectation of privacy, further highlighting the need for states to protect privacy rights. *Id.* at 907 n.27.

402. *See* United States v. Jackson, 825 F.2d 853, 869 (5th Cir. 1987) ("Because the geography of the United States is not homogenous, the rights of citizens that live in its different parts cannot be viewed as a uniform, seamless web."). Thus, searches that are permissible in some areas would not be permissible in others, because uniformity would not be in the public's interest. *See id.*

403. *See Seattle Adopts Nation's Strongest Regulations for Surveillance Technology*, *supra* note 211.

significant distance away. This would defeat the locality's intention with the warrant requirement and still permit a surveillance society in other areas.

Such uncertainty about whether or not there is a reasonable expectation of privacy in a given locality could result in people changing their behavior.[404] As Justice Sotomayor noted in her concurrence in *Jones*: "Awareness that the government may be watching chills associational and expressive freedoms."[405] Relying on local regulations that create an inconsistent patchwork would create fluctuating expectations of privacy, could have a chilling effect on behavior, and would create gaps where the public might have less privacy protection than they believe.

In addition, the few measures enacted by local governments thus far have been largely reactionary, excluding UAS for all uses, including those that are beneficial or even innocuous.[406] Such measures foreclose the use of drones to perform the numerous law enforcement tasks they are uniquely well-suited for, as outlined in Part I. Some local measures have also foreclosed the use of drones to help keep the public safe at events with large crowds, such as music festivals[407] or sporting events like marathons.[408] As one critic of such overprotective measures observed, allowing police to use drones in those situations would place little or no burden on privacy because such events take place in public, there are numerous spectators photographing the event, and the event may even be televised.[409] Thus, people in cities like Syracuse and Seattle are likely less safe, because law enforcement has been deprived of a tool that could enhance public safety.

Thus, states are in the best position to balance the constitutional rights of the public against public safety because state legislatures are closer to the people they represent than the federal government but large enough to avoid the patchwork problem. States also have "greater resources and greater ability to mobilize public attention" than local governments, because of "their relatively larger size and fewer numbers."[410] The enactment of state UAS statutes will promote administrative efficiencies in courts, which will become familiar with

404. *See* ACLU, *supra* note 109, at 7 (noting that people tend to behave differently when they are being watched).

405. United States v. Jones, 565 U.S. 400, 416 (2012) (Sotomayor, J., concurring).

406. *See supra* Subpart I.D.3.

407. *See* Brown, *supra* note 46 (discussing the use of UAS by police in Dover to monitor the Firefly Music Festival); Bruce Fessier, *Coachella Using Drones, Security Plans Enacted After 9/11 to Prevent Las Vegas-Type Incident*, DESERT SUN, https://www.desertsun.com/story/life/entertainment/music/coachella/2018/04/04/coachella-using-drones-security-plans-enacted-after-9-11-prevent-another-las-vegas-type-incident/487502002/ (last updated Apr. 4, 2018, 4:09 PM) (discussing the Indio Police Department's contract with independent drone operators to provide additional security at an outdoor music festival).

408. McNeal, *supra* note 170, at 3 ("[A] marathon is the type of event where the police would want to use a drone to monitor for unknown attackers, and in the unfortunate event of an attack, use the footage to identify the perpetrators.").

409. *Id.* at 4.

410. Richard Briffault, *"What About the 'Ism'?" Normative and Formal Concerns in Contemporary Federalism*, 47 VAND. L. REV. 1303, 1349 (1994).

the statutes' parameters. Additionally, state laws will provide clear guidelines to law enforcement agencies *ex ante*, so they do not expend resources gathering evidence that could be thrown out when a court analyzes the legality of the surveillance under the Fourth Amendment or the state's equivalent.

In other areas of privacy, states have proven to be effective and important laboratories for experimenting with remedies[411] because they have been the first to identify areas in need of regulation and to act, offering innovative solutions which allow simultaneous experiments with different policies.[412] As Justice Brandeis famously observed, "It is one of the happy incidents of the federal system that a single courageous State may, if its citizens choose, serve as a laboratory; and try novel social and economic experiments without risk to the rest of the country."[413] Thus far, many states have tried and failed to pass drone legislation, while others, such as Oregon, have enacted a law that vigorously protects privacy. Invariably, some states may be slow to respond to this emerging issue, while others may take an even more forward-thinking and innovative approach. In either event, the states' role as laboratories of democracy should not be usurped. As Justice O'Connor noted, "the . . . challenging task of crafting appropriate procedures for safeguarding . . . liberty interests is entrusted to the 'laboratory' of the States . . . in the first instance."[414]

### B. MODEL PROPOSAL

States should enact drone legislation that adequately addresses the privacy concerns of individuals and allows the public to benefit from law enforcement's use of drones. Factors to consider when tailoring legislation to the state's unique needs are geography, public views on privacy and safety, and state constitutional protections. Safeguards must be in place regulating when and where drones can be used, limiting data retention to specific periods of time based on how and why the data is collected, and restricting the tools that may be added to drone platforms to avoid the Orwellian surveillance state that privacy advocates fear. Legislation should not merely create a blanket warrant requirement that unduly burdens drone use and may actually reduce public safety. Rather, the focus should be on the danger that drones present—the possibility of pervasive surveillance and warehousing of data against individuals.[415] Accordingly, this Note recommends[416] the following be incorporated into any state drone legislation:

---

411. *See, e.g.*, Crump, *supra* note 51, at 1660 (noting that after California passed a data breach notification law, forty-six other states followed suit). "Action in one prominent state or a handful of states on surveillance policy . . . could lead to a similar snowball effect." *Id.*

412. Paul M. Schwartz, *Preemption and Privacy*, 118 YALE L.J. 902, 916–18 (2009).

413. New State Ice Co. v. Liebmann, 285 U.S. 262, 311 (1932) (Brandeis, J., dissenting).

414. Washington v. Glucksberg, 521 U.S. 702, 737 (1997) (O'Connor, J., concurring) (quoting Cruzan v. Dir., Mo. Dep't of Health, 497 U.S. 261, 292 (1990) (O'Connor, J., concurring)).

415. McNeal, *supra* note 170, at 2.

416. The Author relied on Oregon's robust statute as a starting point for her recommendations. *See* OR. REV. STAT. §§ 837.310–.345 (2017).

*1. Section 1: Limits on Law Enforcement Use of Drones*

Law enforcement agencies are prohibited from using drones except: (1) when a warrant is issued authorizing drone use, specifying the period of operation which is not to exceed fourteen days but is renewable by the court upon motion and showing of good cause; (2) when the agency has probable cause to believe there has been or will be a crime *and* exigent circumstances exist which make it unreasonable to obtain a warrant authorizing drone use; (3) during sporting events, concerts, rallies, or other events where attendance is expected to exceed 10,000 persons, drones may be used during the period twelve hours prior to the event through four hours past its conclusion; (4) when an individual gives written consent; (5) for search and rescue activities; (6) for assisting an individual during an emergency if the agency believes there is imminent threat to life or safety of the individual; (7) for preserving public safety, private property, or assessing environmental or weather related damage during a state emergency that is declared by the governor; (8) for purposes of crime scene reconstruction or accident investigation; or (9) for training exercises.

For (2) above, the government bears the burden of demonstrating that exigent circumstances did exist and in no case shall exigent circumstances authorize drone use for a period which exceeds eight hours. Any data that is obtained in violation of the statute, including during training exercises, crime scene reconstruction, or accident investigation, cannot be used to establish probable cause and is not admissible in any court proceeding, except as provided by Section 2.

*2. Section 2: Limits on Data Retention*

The following limitations apply to data retention: (1) Data collected pursuant to a warrant may be retained for a period of up to five years, after which time, the data must be deleted permanently; (2) Data that is not collected pursuant to a warrant, but is incidental to activities two through seven in Section One is accessible to law enforcement agencies for a period of up to sixty days and treated as a contemporaneous or near-contemporaneous observation; (3) After sixty days, data collected pursuant to activities two through seven in Section One must be moved to a server and stored for a period of no more than five years from the date of collection (retention period to coincide with the period for data obtained with a warrant). Such information may only be retrieved by law enforcement pursuant to a court order upon a showing of probable cause. At the end of the allotted retention period, the data must be permanently deleted; (4) Data collected for purposes of crime scene investigation and accident reconstruction may only be used in the scope of those particular accidents or crimes. Any data inadvertently captured during the course of such activities which pertains to other, unrelated criminal activity may be preserved by court order issued within sixty days of the date the data was collected and is admissible in a court proceeding.

*3. Section 3: Limits on Technology Placed on the Drone Platform*

Except when used in accordance with Section One to conduct surveillance at an event where attendance is expected to exceed 10,000 persons, or, to conduct search and rescue activities, drones may not be used as a platform for sense-enhancing technology that is not in general public use without a warrant. Under no circumstances may law enforcement agencies weaponize drones, even with non-lethal force.

## C. DISCUSSION OF THE MODEL PROPOSAL

Drones allow police to conduct surveillance and stockpile data at a fraction of the cost of traditional surveillance methods, so laws must safeguard the public and act as a barrier against the threat of a surveillance society. These recommendations will allow law enforcement to use drones to increase public safety, such as by providing an eye in the sky during events which pose a heightened security risk or threat of terrorist attack, or, to conduct search and rescue missions without endangering officers' lives. However, the data retention limits, warrant requirement, and time limitation on exigent circumstances should prevent law enforcement from abusing this powerful platform and using it for dragnet surveillance.

The purpose of the warrant requirement in Section 1 is to address the intrusive nature of drone surveillance by securing the privacies of life and placing obstacles in the way of pervasive surveillance.[417] Strict limits on what constitutes exigent circumstances and the maximum period warrantless surveillance may be conducted in exigent circumstances also serve these ends. Similarly, prohibiting the use of data obtained during training exercises, accident investigation, or crime scene reconstruction (with limited exceptions) in criminal proceedings will deter police from engaging in these legitimate activities as a pretext for evidence gathering.

The data retention limits in Section 2 will specifically address public concern about the potential for aggregating large amounts of data as they will preclude law enforcement from mining the data without a warrant or court order. The maximum period that data gathered pursuant to a warrant may be retained should be determined by the individual legislature and should bear some relevance to the statute of limitations on most crimes. Foreclosing evidence gathered in violation of the rules from being used in any court proceeding will encourage law enforcement to either obtain a warrant or rely on traditional means of investigation which are less intrusive.

Allowing law enforcement to use drones before, during, and immediately after large-scale events will increase public safety without intruding into a constitutionally protected area because there is no expectation of privacy at such an event. Section 3 permits UAS to carry sense-enhancing technology such as facial recognition software and license plate readers only in limited

417. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018).

circumstances. This will increase public safety by helping law enforcement identify threats at large-scale events more quickly, serving as a deterrent to criminal activity, and aiding in prosecutions. However, limiting the use of sense-enhancing technology further prevents law enforcement from gathering and aggregating large amounts of data to be stockpiled and used against individuals at a later date.

## CONCLUSION

With the advent of drones, the natural limits on law enforcement's ability to conduct widespread aerial surveillance are disappearing. Law enforcement cannot be expected to police itself and determine the appropriate uses and limits of this powerful tool. While the Fourth Amendment provides the baseline protection against warrantless searches, current jurisprudence likely provides no protection from warrantless drone surveillance. Instead, individuals must look to the government to provide firm laws which balance the beneficial uses of drone technology against the weighty privacy interests at stake.

States, as laboratories of democracy, are the most suitable actors to enact laws to serve as guardrails for law enforcement and regulate their use of drones. Without clear guidance from the states, local law enforcement agencies and communities will create an ad hoc patchwork of rules and policies that will compromise overall expectations of privacy and lead to inconsistent results from one city or county to the next. This inconsistent patchwork may not only make the NAS less safe, as the FAA fears, it will jeopardize public safety because beneficial drone use by law enforcement will be prohibited in some areas. Thus, states should enact clear regulations that preserve the beneficial uses of drones as a tool in the hands of law enforcement.

***