Eyes in the Sky: Constitutional and Regulatory Approaches to Domestic Drone Deployment

Hillary B. Farber

Introduction

The defense and aerospace industries are propelling drones into our lives faster than the courts and lawmakers can prepare for their ubiquitous and powerful presence. By 2020, it is estimated that 30,000 drones will be occupying national airspace.[1] In 2012, Congress passed the Federal Aviation Administration Modernization and Reform Act, which ordered the FAA to promulgate regulations for the integration of drones into the national airspace.[2] On June 19, 2013, FBI Director Robert Mueller told Congress that the FBI has deployed drones for surveillance on domestic soil and is developing guidelines for their future use in law enforcement.[3]

State and local police departments are eager to equip themselves with drones because they are cheaper and more efficient than helicopters and other types of manned aircraft.[4] Police departments in cities such as Miami, Houston, Seattle, Arlington, Texas, and other areas such as

[1] *Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing before S. Judiciary Comm.*, 113 Cong. (2013) (statement of Patrick Leahy, Chairman, S. Judiciary Comm.).

[2] Federal Aviation Administration Modernization and Reform Act of 2012 (FMRA), Pub L 112-95 sec 331-336. President Obama has ordered the FAA to promulgate these regulations no later than September 2015. H.R. REP. NO. 112-381, at 64 (2012)(Conf. Rep.).

[3] Phil Mattingly, FBI chief admits agency uses drones in domestic surveillance, WASHINGTON POST, http://articles.washingtonpost.com/2013-06-19/world/40070544_1_drones-mueller-privacy-guidelines (June 19, 2013). See also http://www.usatoday.com/story/news/politics/2013/06/19/fbi-mueller-irs-investigation-drones/2437993/. See also, http://www.cbsnews.com/8301-250_162-57590065/fbi-director-acknowledges-domestic-drone-use/. Director Mueller testified that the FBI's use has been seldom. According to Director Mueller the last time the FBI used a drone for surveillance purposes was in February 2013 during the Alabama hostage situation.

[4] Jay Stanley, a senior policy analyst with the Speech, Privacy, and Technology Project at the American Civil Liberties Union "worries that drones, because of their low prices, will prove irresistible to police departments seeking cheap ways to conduct aerial surveillance. . . . Despite that precedent, Stanley said that police departments have long faced practical limits on their ability to conduct aerial surveillance because of the enormous costs of buying helicopters or planes and then hiring crews. Drones are cheap by comparison and require no special personnel. 'In a policy vacuum, police departments won't have much trouble affording to use these drones pretty widely,' he said." *See* Yochi J. Dreazen, *From Pakistan, With Love: the technology used to monitor the skies over Waziristan is coming to your hometown.* NATIONAL JOURNAL, http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313 (March 13, 2011).

Mesa, Colorado and Queen's Anne County, Maryland have purchased drones and are testing the new technology with the hope of incorporating them soon into their fleet.[5] Records released by the Federal Aviation Administration reveal that police departments in Kansas, Washington, Texas, Arkansas, Idaho, Alabama, Colorado, North Dakota, Ohio, and Utah have applied for permission to fly drones in U.S. airspace.[6] Federal agencies are also increasingly using drones for policing. As of May 2013, four Department of Justice (DOJ) divisions had acquired drones: the FBI; Bureau of Alcohol, Tobacco, and Firearms (ATF); Drug Enforcement Agency (DEA); and, the U.S. Marshals Service.[7]

According to the Electronic Frontier Foundation, a digital privacy watchdog group, the Customs and Border Protection (CBP) increased its drone flights eight-fold between 2010 and 2012.[8] Moreover, records reveal that the CBP has conducted drone surveillance for federal, state

[5] "I'm tickled to death" about using the drone, said Chief Deputy Randy McDaniel of the Montgomery County Sheriff's Office in Conroe, Texas, which paid $300,000 in federal homeland security grant money for the ShadowHawk, an unmanned aerial vehicle made by Vanguard Defense Industries. "It's so simple in its design and the objectives, you just wonder why anyone would choose not to have it," said McDaniel. See Stephen Dean, *First Unmanned Police Drone in Texas set to Launch North of Houston*, Houston Examiner, Oct. 29, 2011, http://www.examiner.com/article/first-unmanned-police-drone-texas-set-to-launch-north-of-houston. See also: http://miami.cbslocal.com/2013/05/09/unmanned-drones-now-patrolling-south-florida-skies/ (detailing Miami's use) http://www.examiner.com/article/first-unmanned-police-drone-texas-set-to-launch-north-of-houston (detailing Houston's use); http://www.bloomberg.com/news/2012-05-31/drones-take-to-american-skies-on-police-search-missions.html (detailing Mesa County's use and the relatively inexpensive operating costs of drones as compared to manned aircraft); Sara Sorcher, The Backlash Against Drones, National Journal (Feb. 21, 2013).

[6] See Jennifer Lynch, *Just how Many Drones Licenses Has the FAA Really Issued,* ELECTRONIC FRONTIER FOUNDATION, (Feb. 21, 2013), https://www.eff.org/deeplinks/2013/02/; http://www.huffingtonpost.com/2013/02/08/drone-list-domestic-police-law-enforcement-surveillance_n_2647530.html. For a complete list see https://www.eff.org/sites/default/files/filenode/faa_coa_list-2012.pdf.

[7] Local police departments awarded grants include those in Gadsen, Alabama, Miami-Dade County, North Little Rock, Arkansas, and San Mateo County, California. See U.S. DOJ Office of the Inspector General Audit Division, Interim Report on the Department of Justice Use and Support of Unmanned Aircraft Systems (September 2013), *available at* http://www.justice.gov/oig/reports/2013/a1337.pdf.

[8] Jennifer Lynch, *Customs & Border Protection Logged Eight-Fold Increase in Drone Surveillance for Other Agencies*, ELECTRONIC FRONTIER FOUNDATION, (July 3, 2013), https://www.eff.org/deeplinks/2013/07/customs-border-protection-significantly-increases-drone-surveillance-other. The government provided the flight data following a FOIA request made by the Electronic Frontier Foundation (EFF). Much of the increase in numbers of surveillance flights can be attributed to an increase in border patrol and drug trafficking monitoring. A 2013 DHS Budget-in-Brief report list includes in its 2011 "Accomplishments" section that the use of UASs on the United

and local law enforcement agencies.[9] These surveillance missions have ranged from specific drug related investigations and missing person searches to aerial reconnaissance and surveillance.[10]

Meanwhile, Fourth Amendment privacy jurisprudence has yet to grapple with drones and their unprecedented surveillance capabilities. Courts are slow to respond when it comes to evaluating the constitutional implications of new technology.[11] Supreme Court case law on aerial surveillance has only considered manned aircraft flying at relatively low altitudes, which is

---

States' international borders helped seize 7,600 lbs of narcotics and arrest 467 individuals engaged in illicit activities, http://www.dhs.gov/xlibrary/assets/mgmt/dhs-budget-in-brief-fy2013.pdf.

[9] Somini Sengupta, *U.S. Border Agency Allows Others to Use Drones*, NY TIMES, http://www.nytimes.com/2013/07/04/business/us-border-agency-is-a-frequent-lender-of-its-drones.html?pagewanted=all&_r=0 (July 3, 2013). Federal, state, and local agencies that have received CBP's assistance with drone surveillance include the FBI, US Immigration and Customs Enforcement, US Marshalls, the US Coast Guard, FEMA, DHS Office of Intelligence and Analysis, US Secret Service, DHS Office for Infrastructure Protection, DEA, Interagency Remote Sensing Coordination Cell, DOD, NOAA, FAA, US Forest Service, US Bureau of Land Management, US Department of Energy, Minn. and N.D. Bureaus of Criminal Investigation, North Dakota Army National Guard, and the TX Dept. of Pub. Safety, and the TX Rangers *See* Office of Air & Marine, U.S. Customs & Border Prot., Assistant Comm'r's Rep., Flight logs (Feb. 2, 2010 – Dec. 31, 2012) *available at* https://www.eff.org/deeplinks/2013/07/customs-border-protection-significantly-increases-drone-surveillance-other; Dept. of Homeland Sec., Concept of Operations for CBP's Predator B Unmanned Aircraft System, Fiscal Year 2010 Report to Congress, p.9-10. (June 29, 2010) *available at* https://www.eff.org/file/37304#page/1/mode/1up; Office of the Inspector Gen., Dep't Homeland Security, OIG--12--85, *CBPs Use of Unmanned Aircraft Systems in the Nation's Border Security* (May 2012) *available at* http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-85_May12.pdf [hereinafter DHS OIG Report].

[10] Jennifer Lynch, *Customs & Border Protection Logged Eight-Fold Increase in Drone Surveillance for Other Agencies*, ELECTRONIC FRONTIER FOUNDATION, (July 3, 2013), https://www.eff.org/deeplinks/2013/07/customs-border-protection-significantly-increases-drone-surveillance-other. As of May 2012, CBP had flown missions on behalf of other federal, state, and local agencies, but had failed to implement any formal procedure for outside agencies like state and local police to request drone surveillance assistance. The proposed procedure is that DHS will be the agency in charge of sending the drones out, but that state and local agencies can send requests to the to DHS asking for specific missions that they need/want/would like flown. The data on all missions will be sent almost simultaneously from the drone's camera to DHS who can then very quickly distribute the info out to state and local agencies. Dept. of Homeland Sec., Concept of Operations for CBP's Predator B Unmanned Aircraft System, Fiscal Year 2010 Report to Congress., p.20 (June 29, 2010). available at https://www.eff.org/file/37304#page/1/mode/1up.

[11] *See* Orin S. Kerr, The Fourth Amendment and New Technologies: Constitutional Myths and the Case for Caution, 102 Mich. L. Rev. 801, 868-69 (2004) ("Consider the hurdles that must be overcome before the courts resolve how the Fourth Amendment applies to a new technology. Because the Fourth Amendment applies only to actual searches, not to technologies that merely have the potential to conduct searches, courts generally cannot pass on how the Fourth Amendment applies to a technology until long after a technology has been introduced. For a trial court to address the Fourth Amendment implications of a technology, the technology must be used by the government in the course of investigating a criminal offense; the use of the technology must yield evidence of a crime; it must lead to an arrest; and then it must lead to a constitutional challenge requiring judicial resolution. ")

not equivalent to the characteristics and capabilities of drones. At least in the short term, legislative regulation will likely provide more substantive protection for individual privacy interests in the face of the ever-increasing presence of unmanned aerial surveillance. [12] Congress has held a series of hearings to investigate the future of drones and the privacy and safety issues they present.[13] There is bipartisan concern over how and by whom drones will be used.[14] Yet, progress has been slow. On the other hand, states are moving rapidly to regulate or ban the commercial use of drones as well as place restrictions on government use without a warrant.[15] More than eighty bills or resolutions have been introduced in 42 states.[16] Eight states have enacted laws regulating drone use.[17]

Technological change disrupts the balance of power between people and government -- the very thing the Fourth Amendment regulates. Some anticipate that drone surveillance will eventually enable law enforcement to gather unprecedented amounts of information about individuals, making it virtually impossible to shield oneself from government watch.[18] The very

[12] States are passing laws at alarming speed in response to concern over intrusions on personal privacy. See infra part X.

[13] *Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing before S. Judiciary Comm.*, 113 Cong. (2013).

[14] See e.g., The Drone Aircraft Privacy & Transparency Act , H.R. Res. 1262, 113 Cong. (2013); Preserving Freedom from Unwanted Surveillance Act, S. 3287, 112 Cong (2012).

[15] See infra part X

[16] Jay Stanley and Catherine Crump, ACLU report: Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft, December 2011.

[17] Florida, Idaho, Illinois, Montana, Oregon, Tennessee, Texas, and Virginia.

[18] Michael McAuliff, *FBI's Robert Mueller: Drones Are In Use In America*, (Aug. 2, 2013, 12:39 PM), http://www.huffingtonpost.com/2013/06/19/robert-mueller-drones_n_3466400.html (Reporting that, in a U.S. Senate on the Judiciary Committee Hearing, Sen. Dianne Feinstein (D-Calif.) stated that " the greatest threat to the privacy of Americans is the drone, and the use of the drone and the very few regulations that are on it today, and the booming industry of commercial drones".); http://epic.org/2013/02/epic-foia---us-drones-intercep.html, (Reporting that "[n]ew records obtained by EPIC under the Freedom of Information Act indicate that the Bureau of Customs and Border Protection is operating drones in the United States capable of intercepting electronic communications. The records also suggest that the ten Predator B drones operated by the agency have the capacity to recognize and identify a person on the ground."); see also, statement of Bob Goodlatte, Judiciary Comm. Chairman *available at* http://judiciary.house.gov/news/2013/05172013.html ("While there are many useful applications for UAS, there are also many reasons to be concerned about the privacy implications of UAS. Unchecked law enforcement use of UAS

essence of drone surveillance enables users to track the movements of large numbers of people simultaneously. Drones can provide police with the details of a person's daily routine, easily allowing them to create a profile of the person's associations, religious affiliation, health conditions, professional and recreational activities, and family and economic status.[19] When all this information concerning hundreds, if not thousands, of people can be gathered from a distance of thousands of feet in the sky, it is hard to resist the claim that society has succumbed to an Orwellian vision far beyond George Orwell's imagination.

As with any technology, there is always the potential for abuse. We need look no further than the activities of the National Security Agency (NSA) in obtaining phone records of millions of Americans with no particularized suspicion.[20] In the arena of unmanned aerial surveillance, some privacy rights groups are equally concerned about privacy intrusions by commercial users and law enforcement.[21] Certainly journalists, curious neighbors, and the paparazzi can benefit

---

could lead to violations of U.S. citizens' Constitutional rights. Overly aggressive bureaucrats behind the controls of UAS could lead to an expansion of the federal government's footprint, harassment and serious violations of privacy.") *Eyes in the Sky: Domestic Use of Unmanned Aerial Systems, Subcommittee on Crime, Terrorism, Homeland Security and Investigations Hearing*, 113 Cong. (2013); Jay Stanley and Catherine Crump, ACLU report: Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft, December 2011.

[19] Justice Brennan made the point in his dissent in *California v. Greenwood* that rifling through a person's trash could reveal to its collector some of the most personal and intimate details about a person. See *California v. Greenwood*, 486 U.S. 35, 50-51 (1988)("A trash bag like any of the above-mentioned containers [paper bags, locked trunks, lunch buckets, etc.] 'is a common repository for one's personal effects' and even more than many of them, is 'therefore . . . inevitably associated with the expectation of privacy.' . . . '[A]lmost every human activity ultimately manifests itself in waste products . . . .' A single bag of trash testifies eloquently to the eating, reading, and recreational habits of the person who produced it. A search of trash, like a search of a bedroom, can relate intimate details about sexual practices, health, and personal hygiene. Like rifling through desk drawers or intercepting phone calls, rummaging through trash can divulge the target's financial and professional status, political affiliations and inclinations, private thoughts, personal relationships, and romantic interests. It cannot be doubted that a sealed trash bag harbors telling evidence of the 'intimate activity associated with 'the sanctity of a man's home and the privacies of life,'' which the Fourth Amendment is designed to protect. Brennan, J., dissenting)(internal citations omitted).

[20] See Ellen Nakashima, *NSA gathered thousands of Americans' emails before court ordered it to revise its tactics*, Washington Post (August 21, 2013) http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html.

[21] See John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 Harv. J.L. & Pub. Pol'y 457 (2013).

immensely from being able to spy on their targets without concern for the hazards of physical trespass. Though unmanned aerial surveillance can intrude upon the private lives of citizens in numerous ways, the biggest threat it poses is the nearly limitless expansion of police power. Information that once required expenditure of significant resources will become readily attainable with the assistance of drones.[22] This article is concerned with law enforcement's use of unmanned aerial surveillance and the limits that regulations as well as the Fourth Amendment can place on this new technology.

This article begins with a current look at the deployment of drones domestically, both in terms of their use and the procedure for attaining approval for flight. Part II examines the capabilities of drones. Part III considers the Supreme Court's current Fourth Amendment jurisprudence and its application to law enforcement's use of drones. Part IV reviews existing and proposed federal and state regulation of drones. Part V offers constitutional and legislative prescriptions for regulating drones.

I. Current Deployment of Domestic Drones

Unmanned aerial vehicles (UAVs), more commonly referred to as drones, can conduct aerial surveillance much the same way a helicopter or other manned aircraft can. One advantage

[22] "Drones present a unique threat to privacy. Drones are designed to maintain a constant, persistent eye on the public to a degree that former methods of surveillance were unable to achieve... Drones are currently being developed that will carry facial recognition technology, able to remotely identify individuals in parks, schools, and a political gatherings. The ability to link facial recognition capabilities on drones operated by the Department of Homeland Security ("DHS") to the Federal Bureau of Investigation's Next Generation Identification database or DHS IDENT database, two of the largest collections of biometric data in the world, further exacerbates the privacy risks. *Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing before S. Judiciary Comm.*, 113 Cong. (2013) (statement of Amie Stepanovich, Dir. of the Domestic Surveillance Proj. Elec. Privacy Info. Ctr.). See also, infra ... I am referring to part of article where I talk about capabilities

UAVs offer for surveillance purposes is their small size and, in some cases, their ability to mimic birds and insects to avoid detection.[23] Because they do not need to accommodate a pilot, UAVs can be very small and access areas that manned aircraft cannot. UAVs are also a more cost effective means for police to carry out their investigative efforts. Whether the purpose is to search for missing persons, detect forest fires, or investigate criminal activity, a police department with limited resources can purchase a less expensive UAV that is much more efficient than a helicopter which requires personnel to operate, fuel, and maintain. Eventually, the UAV will replace the helicopter as the preferred method for conducting aerial surveillance.

During 2012, the Department of Homeland Security (DHS) initiated a $4 million "Air-based Technologies Program," for the purpose of facilitating and accelerating the adoption of small unmanned drones by police and other public safety agencies.[24] The program has been described officially as an effort by DHS to work with "state & local partners to develop and promote appropriate use of UASs by law enforcement and first responders."[25] Almost one year

[23] THE BOYER SYNDICATE, INC., http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird (last visited July 23, 2013). supra note X

[24] Andrea Stone, *Drone Program Aims to "Accelerate" Use of Unmanned Aircraft by Police*, (May 22, 2012, 5:39 PM), http://www.huffingtonpost.com/2012/05/22/drones-dhs-program-unmanned-aircraft-police_n_1537074.html. The program is being overseen by DHS's Science and Technology Directorate division of borders and maritime security. See id.

[25] Memorandum from Tamara J. Kessler, Acting Officer, Office for Civil Rights and Civil Liberties, Dept. of Homeland Security to Janet Napolitano, Secretary of Homeland Security (Sept. 14, 2012), http://www.dhs.gov/sites/default/files/publications/foia/working-group-to-safeguard-privacy-civil-rights-and-civil-liberties-in-the-departments-use-and-support-of-unmanned-aerial-systems-uas-s1-information-memorandum-09142012.pdf. (on file with author). Additionally, the DOJ's Office of Justice Programs (OJP) and Office of Community Oriented Policing Services (COPS) have awarded grants to local law enforcement and non-profit organizations for purchasing and researching drone use. See U.S. DOJ Office of the Inspector General Audit Division, Interim Report on the Department of Justice Use and Support of Unmanned Aircraft Systems (September 2013), *available at* http://www.justice.gov/oig/reports/2013/a1337.pdf.

later, DHS has yet to reveal any specifics about the program, but one official described it as creating "a 'middleman' between drone manufacturers and first-responder agencies."[26]

What has been euphemistically labeled the "loan-a-drone program" is drawing criticism from organizations such as the Electronic Privacy Information Center (EPIC). Federal agencies like Custom and Border Protection (CBP) allow state and local police to use their drones for local operations.[27] These partnerships first attracted public attention when a North Dakota Sheriff's department requested assistance from a nearby Air Force base to deploy its Predator B drone to locate three men believed to be rustling cattle.[28] Within hours the drone had detected the suspects and the men were arrested in what is believed to be the first arrest involving a drone on US soil. EPIC has expressed concerns that "CBP's drone program is shrouded in secrecy and legal ambiguity. Despite a specific mission to protect the border from illegal immigration and drug smuggling, CBP continues to let other federal agencies and local law enforcement use [its drones] for unrelated purposes"[29]

In 2007, the Houston Police Department attempted to carry out secret tests of drones using Boeing's ScanEagle, which has the capability to climb to 19,500 feet and stay aloft for

[26] Andrea Stone, *Drone Program Aims to "Accelerate" Use of Unmanned Aircraft by Police*, (May 22, 2012, 5:39 PM), http://www.huffingtonpost.com/2012/05/22/drones-dhs-program-unmanned-aircraft-police_n_1537074.html. The same official acknowledged that the department has "a very tall challenge to change public perception . . . [and reassure the public that] we will not be watching backyards."
http://libertycrier.com/local-law-enforcement-borrowing-federal-drones-for-surveillance/ ("CBP's three years of daily flight logs detail when, where and how the agency flew its Predator drones on behalf of other agencies. These logs show a marked increase in drone flights over the years. In 2010, CBP appears to have flown its Predators about 30 times on behalf of other agencies, but this number increased to more than 160 times in 2011 and more than 250 times in 2012.")

[28] In 2011, a sheriff in North Dakota was investigating a report of cattle rustling at a nearby ranch only a few miles from an Air Force base. At the Sheriff's request, the Air Force deployed one of its Predator drones to detect the suspects. *Within an hour or so the drone had detected the three men believed to be stealing the cattle.* See defendant's motion to dismiss:
http://www.nacdl.org/uploadedFiles/files/news_and_the_champion/DDIC/Brossart%20Order.pdf. See also;
http://www.usnews.com/news/articles/2012/04/09/first-man-arrested-with-drone-evidence-vows-to-fight-case

[29] Kimberly Dvorak, *Homeland Security increasingly lending drones to local police*, The Washington Times (Dec. 10, 2012). http://www.washingtontimes.com/news/2012/dec/10/homeland-security-increasingly-loaning-drones-to-l/

twenty-four hours. Local television reporters used hidden cameras to tape the undercover operation and, when aired, the story caused great controversy. As a result, the Houston police department was forced to slow the program.[30] More recently law enforcement agencies around the country are seeking to use drones for more routine police operations.[31] In Ogden, Utah the police department proposed using an unmanned blimp for surveillance purposes to deter crime.[32] In Houston the police sought to use drones to detect vehicles committing traffic violations.[33]

Because law enforcement's interest in drones is growing so quickly, the government needs to establish criteria for how long and how high drones can fly in navigable airspace so as not to disrupt air traffic control. Right now any entity interested in operating a drone in public airspace must obtain a certificate of authorization (COA) from the FAA.[34] Since 2006 when this application procedure was first created, the FAA has issued more than 1,000 authorizations.[35]

---

[30] Jay Stanley and Catherine Crump, Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft (December 2011) at 37. While the Mayor of Houston stressed the need for public input on the program, he also made it clear that he was not telling the Houston PD not to pursue further drone testing. *Pilots Worry that HPD Drones Could Cause Danger in Air*, (Dec. 5, 2007), http://www.click2houston.com/news/Pilots-Worry-HPD-Drones-Could-Cause-Danger-In-Air/-/1735978/2873996/-/n4u2jmz/-/index.html

[31] See https://www.eff.org/deeplinks/2013/07/customs-border-protection-significantly-increases-drone-surveillance-other

[32] James Nelson, *Utah city may use blimp as anti-crime spy in the sky*, REUTERS (Jan. 16, 2011, 10:53 AM), http://www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116. According to Ogden, Utah mayor, Matthew Godfrey, the blimp would be almost undetectable and would have a very low operating cost and minimal maintenance expenses. The blimp is capable of operating on its own programming without a human operator on the ground.

[33] Stephen Dean, "Police line up to use drones on patrol after Houston secret test," Houston Examiner, Jan. 11, 2010, online at http://www.examiner.com/page-one-in-houston/police-line-up-to-use-drones-on-patrol-after-houston-secret-test

[34] The COAs last as long as two years and "defines the operational conditions, emergency landing procedures, airworthiness requirements, area of operations, and ground crew proficiency required to operate the UAS." Department of Justice Use and Support of Unmanned Aircraft Systems (September 2013), *available at* http://www.justice.gov/oig/reports/2013/a1337.pdf.

[35] The FAA reports that from 2009 to 2012, the agency issued 1,014 public COAs with 327 still active as of Feb. 15, 2013. See FAA Fact Sheet – Unmanned Aircraft Systems (UAS) (Feb. 19, 2013), http://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=14153.
See more at: http://cnsnews.com/news/article/faa-has-authorized-106-government-entities-fly-domestic-drones#sthash.qrIOAlKh.dpuf ("Between January 1, 2012 and July 17, 2012," said Dillingham, "FAA had issued 201 COAs to 106 federal, state and local government entities across the United States, including law enforcement

Currently, certificates have been issued to public agencies including the FBI, US Army, Defense Advanced Research Projects Agency (DARPA), state and local law enforcement agencies, and universities. None have been issued for commercial purposes.[36] That is expected to change dramatically by 2018 when the FAA estimates that as many as 7,500 commercial drones could be in use.[37]

II. UAV Capability

In this age of rapid technological growth, society has an insatiable appetite for the newest tool that offers slightly more convenience than the last device. The speed at which technology progresses is exponential.[38] The newest iPhone outdoes its predecessor and soon after anticipation builds for the next innovation. Some new devices threaten individual privacy

---

entities as well as academic institutions.") According to a list of entities that have applied for drone authorization from the FAA, as of February 2013 there were 81 entities on this list. https://www.eff.org/document/2012-faa-list-drone-applicants.

[36] Peter Finn, "Domestic use of aerial drones by law enforcement likely to prompt privacy debate," *Washington Post*, Jan. 23, 2011, online at http://www.washingtonpost.com/wp-dyn/content/article/2011/01/22/AR2011012204111.html. The FAA sometimes also grants the military swaths of restricted airspace where UAVs can be freely flown. For the private sector, getting permission to fly a UAV is much harder; they are only granted for research and development, demonstrations, and crew training. Although rules permit their operation by hobbyists, commercial uses of UAVs are not permitted. Government entities wishing to fly drones (from law enforcement at all levels to state universities to the Department of Defense) must obtain a certificate from the FAA (a "Certificate of Waiver or Authorization," or COA). The permit available to non-government parties is called the "Special Airworthiness Certificate—Experimental Category." The FAA's regulations, "Unmanned Aircraft Operations in the National Airspace System," effective March 28, 2011, are online at http://www.faa.gov/documentLibrary/media/Notice/N7210.766.pdf. above quoted from ACLU report fn. 46.

[37] Paul D. Shinkman, *Military Drones in U.S. Skies Could Pave Way for Thousands of Civilian Ones*, U.S. News & World Rep. (July 3, 2013), http://www.usnews.com/news/articles/2013/07/03/military-drones-in-us-skies-could-pave-way-for-thousands-of-civilian-ones.

[38] See Paul Rosenzweig, Privacy and Counter-Terrorism: The Pervasiveness of Data, 42 Case W. Res. J. Int'l L. 625, 627 (2010)(The exponential progress of computing technology "is most familiarly characterized as Moore's Law—named after Intel computer scientist Gordon Moore, who first posited the law in 1965. Moore's Law predicts that computer chip capacities will double every eighteen to twenty-four months. Moore's law has been remarkably constant for nearly thirty years".) "The Extent of [drones] potential domestic application is bound only by human ingenuity." Allison Dolan and Richard Thompson II, Integration of Drones into Domestic Airspace: Selected Legal Issues, CRS Report for Congress, R42940 (Jan. 30, 2013).

because they enable their users to either accomplish things they could not have done before or complete tasks more efficiently.[39]

In 2012, nearly fifty companies developed approximately one hundred fifty different UAV systems,[40] resulting in a worldwide expenditure of six billion dollars specifically for drones each year.[41] It's predicted that by 2020, 11.4 billion dollars each year will be spent on UAV sales.[42] The drone industry is expected to create 70,000 new jobs in the first three years of drone integration into the national airspace and over 100,000 jobs by 2025.[43]

Since their inception, UAVs have become smaller, more sophisticated and cheaper.[44] Their main use both oversees and domestically is surveillance. All drones can be fitted with high-resolution cameras and imaging technologies, the capabilities of which advance year after year.[45] The research and development arm of the drone industry is growing exponentially.[46]

Presently there are hundreds of types of drones, ranging in size from a small insect to a commercial aircraft. Aerovironment, a southern California company, was commissioned by the

---

[39] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV 476, 486 (2011).

[40] http://online.wsj.com/article/SB10001424052702304331204577354331959335276.html?mod=googlenews_wsj

[41] http://www.foxnews.com/us/2012/06/19/talk-drones-patrolling-us-skies-spawns-anxiety/#ixzz21m9CZywj

[42] http://www.azcentral.com/12news/news/articles/2012/07/07/20120707arizona-unmanned-drones-concerns.html#ixzz21YZ7M4z ("according to defense-industry analysts at the Teal Group in Virginia.")

[43] Association for Unmanned Vehicle Systems International, The Economic Impact of Unmanned Aircraft Systems Integration in the United States, 2 (March 2013) *available at* http://qzprod.files.wordpress.com/2013/03/econ_report_full2.pdf.

[44] Id.

[45] "Soon drones will be able to operate with facial recognition or soft biometric recognition equipment that can recognize and track individuals based on attributes such as height, age, gender, and skin color." *Eyes in the Sky: Domestic Use of Unmanned Aerial Systems, Subcommittee on Crime, Terrorism, Homeland Security and Investigations Hearing*, 113 Cong. (2013) (statement of Tracy Maclin), http://judiciary.house.gov/hearings/113th/05172013/Maclin%2005172013.pdf.

[46] *See* Yochi J. Dreazen, *From Pakistan with Love: the technology used to monitor the skies over Waziristan is coming to your hometown.* National Journal, March 10, 2011, online at http://www.nationaljournal.com/magazine/drones-may-be-coming-to-your-hometown-20110313 "The nation's aerospace contractors, meanwhile, are stepping up efforts to market low-cost drones to police departments across the country: The California-based MLB Co. says that its $52,000 Bat 3 drone is perfect for "urban monitoring. It may take a few years, but drones will become a common sight in American skies. The steady march of technology can be slowed, but, for better or worse, it probably can't be stopped."

DARPA to develop a drone the size of a small bird for stealth surveillance.[47] The Hummingbird, as it has been named, can fly up to 11 miles per hour and hover and fly sideways and backwards for about eight minutes. Its wingspan is six-and-a-half inches, and it weighs nineteen grams.[48] Aerovironment also manufactures a drone called the Raven, designed to fit inside a backpack and capable of operation by a single person.[49] The Raven weighs four pounds, has a wingspan of four-and-a-half feet, and is three feet long.[50] The Raven can reach altitudes of 14,000 feet and stay aloft for one hundred ten minutes.[51] This particular size drone is quite common among manufacturers and hobbyists who design and build drones. "You can literally pull this out of your pocket, throw it into the air, and it can start flying" said Bill Borgia, the head of Lockheed Martin's Intelligent Robotics Laboratory talking about the size of a UAV being developed by his company.[52] The project was inspired by a DARPA defense program called "Nano Air."[53] The defense program is trying to go even smaller than Lockheed Martin's design, making an aircraft "less than 15 centimeters and less than 20 grams."[54] Some drones at the other end of the spectrum, such as Israel's four-and-a-half ton "Eitan" have a wingspan of eighty-six feet and can rival commercial aircraft in size.[55]

[47] Jay Stanley and Catherine Crump, ACLU report "Protecting Privacy From Aerial Surveillance: Recommendations for Government Use of Drone Aircraft, December 2011.

[48] THE BOYER SYNDICATE, INC., http://www.avinc.com/resources/press_release/aerovironment_develops_worlds_first_fully_operational_life-size_hummingbird (last visited July 23, 2013).

[49] THE BOYER SYNDICATE, INC., http://www.avinc.com/uas/small_uas/raven/ (last visited July 23, 2013).

[50] THE BOYER SYNDICATE, INC., http://www.avinc.com/uas/small_uas/raven/ (last visited July 23, 2013).

[51] THE BOYER SYNDICATE, INC., http://www.avinc.com/uas/small_uas/raven/ (last visited July 23, 2013).

[52] http://idealab.talkingpointsmemo.com/2012/07/maple-seed-drones-will-swarm-the-future.php

[53] http://www.darpa.mil/Our_Work/DSO/Programs/Nano_Air_Vehicle_(NAV).aspx "The Nano Air Vehicle (NAV) program is developing an extremely small, ultra lightweight air vehicle system (less than 15 centimeters and less than 20 grams) with the potential to perform indoor and outdoor military missions." http://www.darpa.mil/NewsEvents/Releases/2011/11/24.aspx

[54] http://www.darpa.mil/Our_Work/DSO/Programs/Nano_Air_Vehicle_(NAV).aspx

[55] http://www.popularmechanics.com/technology/military/planes-uavs/4346921

In 2005, CBP selected the Predator B drone for its operations. The Predator B is "equipped with state-of-the-art electro-optic sensors, communications payloads, and sophisticated on-board sensors, all of which can provide unparalleled surveillance capability."[56] Its wingspan is fifty-five feet long.[57] The Predator B is so surreptitious and clandestine that drug smugglers reportedly call it "el mosco," or the mosquito.[58]

The range in cost is as great as the range in size. Basic autonomous UAVs can be purchased for less than 600 to 700 dollars.[59] Drones for Peace, a recent technology startup, is engineering drones that they hope will cost as little as one hundred dollars.[60] The first model is likely to sell for 250 dollars. [61] At 300 dollars, the Parrot AR drone is available for purchase on amazon.com.[62] The Parrot AR 2.0 Quadricopter is equipped with a 720 megapixel camera, provides live video streaming, hovers and flies in all directions, and is controlled by any smartphone or tablet.[63] The surveillance capabilities of UAVs with a price point of over $100,000 dollars are much greater and currently not available at retail. For instance, the ShadowHawk, already being used by some police departments, can take high-resolution photographs and conduct surveillance from heights of 10,000 feet.[64] The ShadowHawk and its

---

[56] http://www.cbp.gov/xp/cgov/newsroom/news_releases/archives/2005_press_releases/082005/08302005.xml. In a CPB surveillance operation above Arizona, a Washington Post article said the Predator B was "unseen and silent as a hunting owl" from 15,000 feet with "all-seeing eyeball swiveled and powerful night-vision infrared cameras." See id.

[57] http://www.af.mil/information/factsheets/factsheet.asp?id=122

[58] http://articles.latimes.com/2012/apr/28/nation/la-na-drone-bust-20120429.

[59] http://www.npr.org/2012/02/03/146350507/drone-technology-reaches-new-heights

[60] http://masschallenge.org/profile/drones-peace

[61] http://bigthink.com/ideafeed/soon-a-100-drone-will-do-your-bidding

[62] http://www.amazon.com/Parrot-AR-Drone-Quadricopter-Controlled-Android/dp/B007HZLLOK/ref=sr_1_1?ie=UTF8&qid=1375439859&sr=8-1&keywords=parrot+drone.

[63] http://www.azcentral.com/12news/news/articles/2012/07/07/20120707arizona-unmanned-drones-concerns.html#ixzz21lyR6tGk

[64]

counterparts are often equipped with other high-resolution technology such as license plate readers, thermal imaging devices, and non-lethal weaponry.[65]

The capabilities of onboard instruments like cameras and other sensory-enhancing technologies collecting data and processing information are immense. The United States Army recently unveiled a UAV that carries a 1.8-gigapixel color camera known as Argus-IS, named after the one-hundred-eyed giant in Greek mythology.[66] With resolution of over 1,800 times that of most phone cameras, the Argus-IS, "the largest video sensor ever used to conduct tactical missions," can cover almost twenty-five square miles from 20,000 feet overhead.[67] Also known as "wide-area persistent stare,"it can autonomously track sixty-five separate targets.[68] The United States Army is currently developing an infrared system which could track up to one hundred thirty "dismounted personnel at night."[69] Some UAVs can even autonomously track and follow targets.[70] Other capabilities include radar[71], heat sensors[72], facial recognition cameras, or open Wi-Fi sniffers.[73]

[65] http://news.cnet.com/8301-17938_105-57472321-1/flying-drones-getting-smaller-smarter-cheaper-and-scarier/. The ShadowHawk, for example, focuses on what Michael Buscher, the CEO of the drone's manufacturer, calls "less lethal systems" like " a stun baton [that fires bean bags] where you can actually engage somebody at altitude with the aircraft [which] would essentially disable a suspect."[65] The ShadowHawk can also be equipped with Tazers, and some other drones are capable of using pepper spray on a target.

[66] http://www.army.mil/article/49594/

[67] See id.

[68] The Argus-IS camera is attached to the underside of a drone and, with the click of a button, can zoom in and track every single moving object, including cars, humans, and even small birds. The Argus can see objects as small as six inches in length and stores over a million terabytes of information per day, the equivalent of 5,000 hours of surveillance. See http://video.pbs.org/video/2325492143/

[69] http://www.darpa.mil/Our_Work/I2O/Programs/Autonomous_Real-time_Ground_Ubiquitous_Surveillance_-_Infrared_(ARGUS-IR).aspx

[70] http://www.azcentral.com/12news/news/articles/2012/07/07/20120707arizona-unmanned-drones-concerns.html#ixzz21lymft5o

[71] http://security.blogs.cnn.com/2012/07/03/marines-betting-big-on-new-small-drone/

[72] Brian Bennett, "Police Employ Predator Drone Spy Planes on Home Front," L.A. Times (Dec. 10, 2011) http://articles.latimes.com/2011/dec/10/nation/la-na-drone-arrest-20111211 (describing Predator drones used to aid local law enforcement that contain "high-resolution cameras, heat sensors and sophisticated radar" as well as live video feed).

[73] http://www.npr.org/2011/12/05/143144146/drone-technology-finding-its-way-to-american-skies

How long can a drone stay in the air? For some, the sky is the limit. Lockheed Martin unveiled a power system that recharges drones in midair. Previously, a UAV called the Stalker, used by special operations since 2006, was only able to stay aloft for two hours on its battery. A 2012 test using the new laser system kept the Stalker in the air for forty-eight hours in a wind tunnel.[74] By the end of that test, the "Stalker's battery actually held more stored energy than it did at the beginning."[75] Through GPS, the UAV directed itself back to a laser to recharge when its battery ran low.[76] One solar-powered UAV is capable of staying airborne for weeks at a time.[77] Another method of extending drone flight time beyond that of any manned aircraft is changing the batteries midflight with the assistance of other drones.[78]

UAS technology has beneficial applications in situations where delay or human error could cost lives – detecting forest fires, monitoring oil spills, predicting severe weather, and searching for missing persons. UAV technology also provides a safer, cheaper alternative to the manpower needed for law enforcement responsibilities from simple traffic monitoring to complex surveillance of an individual suspect or a large-scale crime operation.

A drone equipped with a high resolution camera and facial recognition technology could have aided law enforcement in the Boston Marathon bombing investigation. In the initial phases of the investigation when police were attempting to determine the identity of the suspects, aerial images may have helped identify the suspects more quickly without having to rely on the public.[79] Similarly, the pursuit of the suspects and eventual apprehension of Dzhokhar Tsarnaev

[74] http://articles.economictimes.indiatimes.com/2012-07-18/news/32730648_1_laser-light-drone-laser-power
[75] http://www.huffingtonpost.com/2012/07/16/laser-powered-drone-aircraft-stalker_n_1677455.html
[76] http://losangeles.cbslocal.com/2012/07/18/drones-that-may-fly-indefinitely-can-be-recharged-by-lasers/
[77] http://www.npr.org/2012/04/17/150817060/drones-move-from-war-zones-to-the-home-front
[78] http://www.innovationnewsdaily.com/1407-flying-batteries-electric-plane.html
[79] As it happened, the images from a department store's surveillance camera across the street from the bomb site captured the images that the FBI disseminated to the public. Once the FBI had the images of the suspects and disseminated them to the public, it was not more than 24 hours before the police knew the identities of both suspects. *FBI: Help Us ID Boston Bomb Suspects*, CNN (Apr. 19, 2013, 5:44 AM).

in the boat could have been aided by unmanned aerial surveillance. A drone would have been able to track the suspects during the pursuit, reducing the likelihood of losing track of them during the car chase. Moreover, the vivid images of Tsarnaev hiding under the opaque tarp, which were captured by a thermal imaging camera operated by a police officer in a helicopter over the backyard of the Watertown home, could have been taken by a drone. [80] The infrared device, called a FLIR, [81] was able to locate Tsarnaev in a boat covered with opaque shrink wrap. [82] One could see the outline of Tsarnaev's body, any objects in his vicinity, and even the trace of blood on the floor of the boat believed to be from an injury he had sustained during the pursuit. [83] Immediately following his capture, television stations were airing the view from the thermal imaging device. [84]

The rapid development and versatility of UAV technology comes at a cost and creates the potential for widespread abuse by users. The pace of drone development and commensurate potential for invasion of privacy outpaces judicial response and has legislators at both state and federal levels hurrying to create regulations limiting public and commercial use of UAVs.

III. Fourth Amendment and Aerial Surveillance

---

http://www.cnn.com/2013/04/18/us/boston-blasts; Valencia, Milton J, *FBI Releases Images of Two Bombing Suspects*, The Boston Globe (Apr. 18, 2013), http://www.bostonglobe.com/metro/2013/04/18/authorities-have-clear-video-images-two-suspects/YejgNWAcmChcx2IUXigs5I/story.html; *102 Hours in Pursuit of Marathon Suspects*, The Boston Globe (Apr. 28, 2013), http://www.bostonglobe.com/metro/2013/04/28/bombreconstruct/VbSZhzHm35yR88EVmVdbDM/story.html

[80] Smee, Sebastian. *The Marathon Bombing Images We Can't Forget*, The Boston Herald (May 25, 2013), http://www.bostonglobe.com/arts/theater-art/2013/05/25/the-marathon-bombing-images-can-forget/BQ8PZgwQQB2WUSHrlQ2UbI/story.html

[81] a forward-looking infrared device.

[82] See id.

[83] See id.

[84] Need a cite to some news stations

Fourth Amendment jurisprudence places minimal limitation on aerial surveillance. It is well settled that we do not have an expectation of privacy in public or from a public vantage point.[85] Supreme Court cases on aerial surveillance from the 1980s deal with manned aircraft flying at altitudes of 400 – 1000 feet, taking pictures of private property concealed from ground observation but not from the sky. The Supreme Court found no reasonable expectation of privacy under these circumstances because the observations were made from a public vantage point. The court treated navigable airspace like a public thoroughfare, open to anyone who abided by the regulations governing air travel.[86] Hence the view of one's curtilage from an altitude of 400 or even 1000 feet was not considered a violation of the Fourth Amendment.

Katz v. United States & Reasonable Expectation of Privacy

The 1960's marked an important shift in the approach toward assessing government intrusion into a person's constitutionally protected space. *Katz v. United States* involved law enforcement officers placing a recording device on the outside of a public phone booth.[87] FBI agents were able to capture Katz' end of the conversation and subsequently used his statements to convict him of transmitting wagering information via the telephone.[88] Prior to Katz, a Fourth Amendment violation would not have been found because there was no physical intrusion into the phone booth.[89] The *Katz* decision departed from a long-standing property rights based test and formulated a reasonable expectation of privacy analysis. The Court concluded that the

[85] See [85] California v. Ciraolo, 476 U.S. 207, 213, 106 S. Ct. 1809, 1812, 90 L. Ed. 2d 210 (1986); Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986); Florida v. Riley.

[86] California v. Ciraolo, 476 U.S. 207, 213, 106 S. Ct. 1809, 1812, 90 L. Ed. 2d 210 (1986)("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.")

[87] Katz v. United States, 389 U.S. 347, 352-53 (1967).

[88] Katz, at 348.

[89] See Olmstead v. United States, 277 U.S. 438, 466 (1928)(wire-tapping predicated on physical intrusion), Goldman v. United States, 316 U.S. 129, 134-35 (1942) (holding that the attachment of a detectaphone to a wall did not constitute a Fourth Amendment violation).

Constitution "protects people not places".[90] In this instance, Katz made a concerted effort to protect his conversation from the "uninvited ear" and hence the government's interception of the communication was a violation of Katz' reasonable expectation of privacy.[91] For decades that followed, the *Katz* decision transformed the way courts assess whether police conduct constitutes a search under the Fourth Amendment. The following cases illustrate the application of the reasonable expectation of privacy test to aerial surveillance.

Dow Chemical, Ciraolo, and Riley: Observations from the Air

When Dow Chemical prevented the Environmental Protective Agency (EPA) from physically inspecting a chemical manufacturing plant, the EPA hired a commercial photographer to take pictures from above within lawfully navigable airspace.[92] Fences obstructed the public's view of the plant from the ground, the plant had security, and many of the plant's operations took place under the cover of buildings.[93] Ultimately, the Supreme Court found "that the taking of aerial photographs of an industrial plant complex from navigable airspace is not a search prohibited by the Fourth Amendment."[94] In reaching its conclusion, the Court considered the quality of detail revealed in the photos,[95] the technology utilized, and the place being surveilled. The Court acknowledged hypothetical limits by saying that "surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as

[90] Katz v. United States, 389 U.S. 347, 351, 88 S. Ct. 507, 516, 19 L. Ed. 2d 576 (1967) ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.").

[91] Katz v. United States, 389 U.S. 347, 352, 88 S. Ct. 507, 511-12, 19 L. Ed. 2d 576 (1967)("One who occupies it, shuts the door behind him, and pays the toll that permits him to place a call is surely entitled to assume that the words he utters into the mouthpiece will not be broadcast to the world.")

[92] Dow Chem. Co. v. United States, 476 U.S. 227, 229 (1986).

[93] Id.

[94] Dow Chem. Co. v. United States, 476 U.S. 227, 239 (1986).

[95] Dow Chemical 476 U.S. 227, 238, 106 S.Ct. 1819, 1826-27 (1986). ("But the photographs here are not so revealing of intimate details as to raise constitutional concerns. Although they undoubtedly give EPA more detailed information than naked-eye views, they remain limited to an outline of the facility's buildings and equipment. The mere fact that human vision is enhanced somewhat, at least to the degree here, does not give rise to constitutional problems.")

satellite technology, might be constitutionally proscribed absent a warrant."[96] There was a partial concurrence and dissent written by Justice Powell that criticized the majority approach.[97] Justice Powell framed the majority as holding that "the photography was not a Fourth Amendment 'search' because it was not accompanied by a physical trespass and because the equipment used was not the most highly sophisticated form of technology available to the Government."[98] Powell claimed that the majority's approach abandoned *Katz* principles by hinging its decision on the method of search rather than the scope of the right being protected. Justice Powell argued that this rationale would lead to the erosion of privacy.

In *Ciraolo*, police received an anonymous tip that the defendant was growing marijuana in his backyard. The backyard was surrounded by a fence and unobservable at ground level. Without a warrant, police flew an airplane over the defendant's house at 1000 feet, within navigable airspace. Although the Court recognized that the defendant possessed a subjective expectation of privacy in his backyard because he had taken measures to block it from public view by erecting a fence, the Court deemed his expectation to be one society was not willing to recognize. Ciraolo's expectation of privacy was unreasonable in light of the fact that his backyard could be viewed by any member of the public from an elevated position or an aircraft in navigable airspace.[99] The Court did note, however, that the "state acknowledges that '[a]erial observation of curtilage may become invasive, either due to physical intrusiveness or through

[96] Dow Chemical 476 U.S. 227, 238, 106 S.Ct. 1819, 1826-27

[97] The concurrent in part and dissent in part believed that the majority's approach is mistakenly based on the type of surveillance, not the right to be protected. They suggested that with the improvement of technology, a standard based on the technology utilized will erode the interests that the Katz test was meant to protect. Sotomayor, in Jones, compares the majority's approach here to privacy rights which are based on an unchanging standard, such as the bedroom in Lawrence.

[98] Dow at 240.

[99] California v. Ciraolo, 476 U.S. 207, 213, 106 S. Ct. 1809, 1812, 90 L. Ed. 2d 210 (1986)("The Fourth Amendment protection of the home has never been extended to require law enforcement officers to shield their eyes when passing by a home on public thoroughfares.")

modern technology which discloses to the senses those intimate associations, objects or activities otherwise imperceptible to police or fellow citizens."'[100]

Ciraolo was found to control *Florida v. Riley*[101], another case involving aerial surveillance with the naked eye. In *Riley*, the question was "whether surveillance of the interior of a partially covered greenhouse in a residential backyard from the vantage point of a helicopter located 400 feet above the greenhouse constitutes a 'search' for which a warrant is required under the Fourth Amendment".[102] The Court analogized to *Ciraolo*, finding that the aircraft was observing curtilage from navigable airspace. Under the *Katz* analysis[103], the Court stated that Riley had no reasonable expectation of privacy under the circumstances of this case.

Kyllo and *Caballes: Enhanced technology and its availability to the public*

The next case from the Supreme Court that could be applied to UAVs and potential privacy threats involved activities observed from the ground rather than from the sky. In *Kyllo v. United States* As mentioned earlier, UAVs have tremendous capabilities for surveillance based on features such as signal interception, optics, and even thermal imaging.

In *Kyllo*, a federal agent used a thermal-imaging device to determine whether the amount of heat emanating from the home was consistent with the high-intensity lamps typically used for indoor marijuana growth.[104] The agent, under suspicion there was marijuana growing inside the home, sat in his vehicle across the street from the defendant's house at 3:20 am and pointed his thermal imager at the defendant's house.[105] The device revealed that, compared to the rest of the

[100] California v. Ciraolo, 476 U.S. 207, 226 n. 3 (1986) quoting the Brief for Petitioner 14-15.
[101] 488 U.S. 445, 447-48, 109 S. Ct. 693, 695, 102 L. Ed. 2d 835 (1989)
[102] See id.
[103] See 389 U.S. at 361 ("[T]here is a twofold requirement, first that a person have exhibited an actual (subjective) expectation of privacy and, second, that the expectation be one that society is prepared to recognize as 'reasonable.")
[104] *Kyllo v. U.S.*, 533 U.S. 27 (2001).
[105] *Id.* at 29-30.

home, relatively hot areas existed. Based on informant tips, defendant's utility bills and the thermal imager readings, a Federal Magistrate Judge issued a warrant to search Kyllo's home.[106] The Supreme Court held that the use of sense enhancing technology to obtain information from the interior of a home that could not be obtained through visual observation constitutes a search, at least where the technology is not typically used by the public.[107] In this close case, Justice Scalia, writing for a five person majority, held that the officer's actions constituted a violation of the defendant's reasonable expectation of privacy. A crucial fact in support of the Court's finding was the general public's lack of access to this type of sophisticated technology.[108]

Today of course these devices can be purchased on Amazon or eBay.[109] So what does this mean for drones? If, as anticipated, the FAA relaxes its ban on commercial use of drones by 2015 and 30,000 drones are occupying national airspace by 2020, it will be difficult under existing case law to find a reasonable expectation of privacy from unmanned aerial surveillance in navigable airspace. Presently, one can purchase a recreational unmanned aerial vehicle for less than five hundred dollars that is equipped with a 720 megapixel camera and can fly at altitudes of approximately 300 feet while being operated by a remote control device such as an iPad or iphone.[110] It is anticipated that by the end of the decade, unmanned aerial vehicles equipped with greater intensity cameras and other sensory-enhancing technology will be available to the general public.[111]

Kyllo was read slightly differently in *Illinois v. Caballes*, another case that has relevance to drones and privacy. In *Caballes*, police stopped a car for speeding and, with no reasonable

[106] *Id.* at 30.
[107] *Id.* at 34.
[108] *Id.* at 40.
[109] See www.amazon.com/
[110] Supra cite to $350 drone on amazon
[111]

articulable suspicion of drug activity, a drug-sniffing dog was brought to sniff around the car.[112] The issue was whether "the Fourth Amendment requires reasonable, articulable suspicion to justify using a drug-detection dog to sniff a vehicle during a legitimate traffic stop."[113] *Caballes* is significant in two somewhat contradictory ways: how it reads *Kyllo* may be favorable to privacy and drones and second, the holding of *Caballes* may be read to reduce privacy when it comes to drones. The Court in *Caballes* distinguished between the thermal imaging in *Kyllo* and the drug-sniffing dog. Thermal imaging, the Court said, was an intrusion because it could observe protected activity and lawful activity such as when a person takes a bath.[114] Drug-sniffing dogs, on the other hand, can *only* sense the presence of illegal contraband.[115] Because possessing illegal contraband is not a legitimate expectation of privacy, a drug sniffing dog may be used. This distinction is significant because it allows for the argument that drone optics and sensors are an intrusion because they detect lawful activity or legitimate privacy interests. In other words, unless the drone can distinguish between lawful and unlawful activity, the observation should be considered a Fourth Amendment intrusion or search. On the other hand, this case also has some negative implications for privacy and drones. Read more broadly, *Caballes* says that a drug-sniffing dog does not intrude on a reasonable expectation of privacy. For drones that have the ability to sense particles of drugs or explosives, similar to the way dogs do on the ground, the Court may find that there is no legitimate expectation of privacy.

GPS, Trackers and other forms of surveillance

[112] *Illinois v. Caballes*, 543 U.S. 405, 406 (2005).
[113] Id. at 407.
[114] *Id.* at 409-410.
[115] *Id.* at 410.

If we look for protection under existing Fourth Amendment jurisprudence, the case law on aerial government surveillance will disappoint. Our only precedents are from cases dealing with manned aircraft at low altitudes.[116] How will courts evaluate whether unmanned aerial surveillance in navigable airspace constitutes a search under the Fourth Amendment? Is there a permissible duration where surveillance need not implicate the Fourth Amendment? Who can use the information collected and for how long can it be stored? Some of these questions were triggered in the Court's most recent consideration of whether government use of GPS tracking technology violated the defendant's expectation of privacy.

In *United States v. Jones* the Supreme Court considered whether the use of a GPS device to monitor Jones' movements constituted a search within the framework of the Fourth Amendment.[117] The majority limited its rationale to the narrowest set of facts possible – that the GPS device was impermissibly affixed to the car Mr. Jones was using.[118] Writing for the majority, Justice Scalia relied on eighteenth century tort law to explain why the government's actions constituted a trespass, thereby violating Mr. Jones' right to be free from unreasonable search and seizures.[119] According to Justice Alito's critique of the majority opinion in his concurrence, "the Court's reliance on the law of trespass will present particularly vexing problems in cases involving surveillance that is carried out by making electronic, as opposed to physical, contact with the item to be tracked."[120] Other justices did view this case with the same

[116] See Ciraolo, Riley, Dow

[117] Police attached a GPS device to the undercarriage of defendant Antoine Jones' car without his consent or knowledge. The police monitored Jones' movement s in the car for a four week period. The data revealed multiple trips to a suspected drug house. Police used the location data from the GPS device, along with other intelligence to obtain search warrants which recovered drug paraphernalia and cash. Following his indictment jones moved to suppress the information gained from the GPS tracking device. The trial court denied the motion finding that all the information gained from the movement of the car on public roads was admissible.

[118] Majority opinion rests on finding of physical trespass.

[119] *United States v. Jones*, 132 S. Ct. 945, 949 (2012).

[120] *See id.* at 962.

import as many scholars and court watchers believed it to be – as a precursor for the Court's response to the challenges newer technologies pose to existing Fourth Amendment jurisprudence.[121] Five justices expressed a willingness to reassess the legal framework for evaluating long-term electronic monitoring of a person in public.[122] Both concurring opinions recognized the "quantum of intimate information about a person" that can be obtained from a global positioning system with relative ease and little expense.[123] In his concurrence, Justice Alito, opined that the level of monitoring in this instance exceeded a reasonable duration, thereby unreasonably infringing on Mr. Jones' expectation of privacy.[124] But Alito failed to answer the question raised in his opinion: At what point does electronic monitoring require a warrant?[125] We will have to wait for a future case to see if the justices are willing to re-calibrate the standard for determining when surveillance crosses the line from reasonable to unreasonably intrusive.

Justice Sotomayor, for her part, expressed concern for even the short-term monitoring of a person's public activities.

> "GPS monitoring generates a precise, comprehensive record of a person's public movements that reflects a wealth of detail about her familial, political, professional, religious, and sexual associations..... The Government can store such records and efficiently mine them for information years into the future.

[121] *See id.* at 961. (Alito, J.)("First, the Court's reasoning largely disregards what is really important (the use of GPS for the purpose of long term tracking) and instead attaches great significance to something that most would view as relatively minor.... By contrast, if long term monitoring can be accomplished without committing a technical trespass – suppose for example that the Federal Government required or persuaded auto manufacturers to include a GPS tracking device in every car – the Court's theory would provide no protection.")

[122] *See id.* at 954 (Sotomayor, J., concurring); *Id.* at 957 (Alito, J., joined by Ginsburg, J., Breyer, J., and Kagan, J. concurring).

[123] "With increasing regularity, the Government will be capable of duplicating the monitoring undertaken in this case by enlisting factory- or owner-installed vehicle tracking devices or GPS-enabled smartphones." *Id.* at 955. (Sotomayor, J., concurring).

[124] *Id.* at 964. ("In this case, for four weeks, law enforcement agents tracked every movement that respondent made in the vehicle he was driving. We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark").

[125] "We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark. Other cases may present more difficult questions. But where uncertainty exists with respect to whether a certain period of GPS surveillance is long enough to constitute a Fourth Amendment search, the police may always seek a warrant." Id.

> *Pineda-Moreno*, 617 F. 3d, at 1124 (opinion of Kozinski, C. J.). And because GPS monitoring is cheap in comparison to conventional surveillance techniques and, by design, proceeds surreptitiously, it evades the ordinary checks that constrain abusive law enforcement practices:"limited police resources and community hostility.""[126]

Moreover, she warns of the limitations of the third party doctrine in this new age of modern technology.[127] In a digital age, more and more people are all but forced to relinquish personal information to third parties just to accomplish routine tasks.[128] For instance, on-line banking, on-line payment systems, renewing a driver's license or registration, making airline reservations, paying bar dues – all these necessary tasks require disclosure of confidential information. Hence, Sotomayor contemplates an even more central question: whether it is reasonable that one's disclosure of information to third parties will alter the expectation of the privacy of that information.

Global positioning systems (GPS) allow anyone to track another person's location without conducting a dragnet-style operation, which requires expenditure of greater resources and personnel. Similar to GPS devices, UAVs are cost effective ways for police to conduct pervasive surveillance.[129] It is far from certain that *Jones* would apply to unmanned aerial surveillance when UAVs are not affixed to anything and travel in public airspace.[130] Attitudes

---

[126] Id at 955.

[127] *See Id.* at 956 (Sotomayor urges the court in the future to think critically about the inconsistency between our modern use of technology and the expectation of privacy test. Under our existing reasonable expectation of privacy test, living in a modern society today reveals an extensive amount of information to third parties that citizen's largely want to be kept from government interference and other private users).

[128] "I would not assume that all information voluntarily disclosed to some member of the public for a limited purpose is, for that reason alone, disentitled to Fourth Amendment protection. See *Smith*, 442 U. S., at 749 (Marshall, J., dissenting) ("Privacy is not a discrete commodity, possessed absolutely or not at all. Those who disclose certain facts to a bank or phone company for a limited business purpose need not assume that this information will be released to other persons for other purposes"); see also *Katz*, 389 U. S., at 351–352 ("[W]hat [a person] seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected")." *Jones*, 132 S. Ct. at 957.

[129] See supra X

[130] See supra X

toward domestic use of unmanned aerial surveillance run the gamut. A leading concern is the erosion of personal privacy that can occur with these sensory enhancing devices. On the other end of the spectrum is their use in preventing harm and detecting crime.[131] Lawmakers and scholars share two distinct concerns: the means by which information is collected and how the information is being used and stored. The former is a constitutional issue, the latter more of a regulatory matter. The concern over how drones can be used and how long the information they collect can be kept is addressed in the Drone Aircraft Privacy & Transparency Act introduced in the United States Senate in March 2013.[132] In our global economy, where large quantities of data are sold to private users, it is reasonable to require those seeking to operate drones to provide details about how the information collected will be stored and used. Otherwise, there will be no limits on the duration of data storage or how and to whom the acquired data is disseminated.[133]

IV. Efforts to Regulate on the Federal Level:

[131] The New York Times conducted a study and created an article entitled "Poll Finds Strong Acceptance for Public Surveillance." This survey was conducted right after the Boston Marathon bombing sparked by the video footage that revealed the two suspects. This was a nationwide poll of 965 adults on landlines and cell phones from April 24 to April 28, five days after the manhunt for Tsarnaev. This poll ultimately shows that any polls taken after a terrorist attack often result in 78% of people said surveillance cameras were a good idea in public places. However, the public was divided on whether the information collected could actually be beneficial and prevent harm. Specifically, 41% said they could prevent harm, and 45% said they had not. The poll further suggested that Americans are willing to tolerate more heightened security measures by the government to prevent future attacks. 66% said information about how to make explosives should not be allowed on the Internet, and 30% said it should be because of the liberty of speech. This survey doesn't specifically talk about demographic and different age groups, but it may be useful, especially since it is closely tied to the Boston Marathon bombing. See http://www.nytimes.com/2013/05/01/us/poll-finds-strong-acceptance-for-public-surveillance.html?pagewanted=all&_r=0

[132] H.R.1262 — 113th Congress (2013-2014), Drone Aircraft Privacy and Transparency Act of 2013.

[133] Ken Dilanian, http://www.post-gazette.com/stories/business/news/nsa-google-facebook-and-formerly-nordstrom-are-watching-you-695592/, *NSA, Google, Facebook and formerly Nordstrom are watching you* (Mark Herschberg, chief technology officer at Madison Logic, a New York-based company that provides data for advertisers stated that "[t]here are thousands of companies out there collecting information on customers… Google is reading through your email. Amazon is looking at not just what you buy, but what you shop for.");

The FAA Modernization and Reform Act of 2012 directs the FAA to promulgate regulations so airways can accommodate drones by 2015.[134] It is estimated that by end of this decade 30,000 drones will be operating in national airspace.[135] Some members of Congress are calling on the FAA to take privacy into account as part of its mandate to integrate drones into domestic airspace. Legislation before Congress, the Drone Aircraft Privacy & Transparency Act, sponsored by Sen. Edward Markey (D -MA) and introduced March 2013, would require as part of the FAA licensing process that the entity seeking permission to use the drone would have to disclose where it is going to fly the drone; who will operate it; what type of data it will collect; how the data will be used; and whether information will be sold to third parties.[136]

At present there is no federal statute providing safeguards to protect privacy against drones used by government agencies and officials. In 2012, Senator Rand Paul (R-KY) introduced the Preserving Freedom from Unwanted Surveillance Act, which called for a sweeping prohibition of drone usage for surveillance by any person or entity affiliated with the U.S. government.[137] Paul re-introduced the bill in May 2013.[138] The legislation currently resides in the Senate Judiciary Committee.[139]

Another bill, the Safeguarding Privacy and Fostering Aerospace Innovation Act of 2013, introduced by Senator Mark Udall (D-CO), prohibits private individuals from using drones to conduct surveillance on other individuals.[140] The Act makes a broad exception for surveillance

[134] See PL 112-95, February 14, 2012, 126 Stat 11.
[135] Patrick Leahy comments from hrg on March 20, 2013 US Senate Committee on the Judiciary "The Future of Drones in America: Law Enforcement & Privacy Considerations"

[136] The Drone Aircraft Privacy & Transparency Act, H.R. Res. 1262, 113 Cong. (2013).
[137] Preserving Freedom from Unwanted Surveillance Act, S. 3287, 112 Cong (2012).
[138] Preserving Freedom from Unwarranted Surveillance Act, S. 1016 (113 Cong. (2013).
[139] Preserving Freedom from Unwanted Surveillance Act, S. 1016, 113th Cong. (2013).
[140] The Safeguarding Privacy and Fostering Aerospace Innovation Act, S. 1057, 113th Cong. (2013).

of individuals who are "in a place of public use where surveillance would not be highly offensive to a reasonable person."[141] Introduction of the bills is a legislative response to what many perceive as the inevitability of drone usage by private individuals.[142]

An absence of comprehensive federal legislation will certainly lead to injustices for defendants charged in federal court. One example may arise where state officials violate a state statute on drone surveillance. Those state officials could then turn illegally obtained information over to federal authorities for use in federal prosecution because the defendant will not be able to challenge the admissibility of the evidence. This example of federal authorities using information obtained in violation of a state statute creates a "reverse silver platter doctrine" situation.[143] Second, federal authorities can ignore state protections relevant to drone surveillance. In that second case, there is no exclusion remedy for the defendant in federal court because there is no corresponding federal statute to create such a remedy.

Legislation in the States –

States have outpaced federal lawmakers when it comes to regulating the use and scope of drone surveillance. Since early 2013, there has been significant momentum among states to regulate the use of UAVs.[144] Much of this momentum is spurred by local concern over the

[141] The Safeguarding Privacy and Fostering Aerospace Innovation Act, S. 1057, 113th Cong. (2013

[142] Drone technology is already being used, albeit illegally, for small-scale commercial activities like selling aerial images and films. See Steve Henn, *Under the Radar: Some Pilots of Small Drones Skirt FAA Rules*, NPR (June 13, 2013, 5:28 PM), http://www.npr.org/blogs/alltechconsidered/2013/06/13/190369460/Guidelines-For-Commercial-Drones-Expect-To-Come-By-2015. The FAA is aware of these small-scale "black market" drone operations, which use relatively inexpensive drone technology and have even begun to advertise their services on the internet. Tom Spring, *Illegal Drone Business Thrives in US*, TechNewsDaily (June 18, 2013), http://www.technewsdaily.com/18370-illegal-drones-thrive-despite-ban.html.

[143] Can imagine many uses of drone intelligence by federal authorities & many crimes with concurrent jurisdiction between state & federal laws that would involve use of information gathered by drone surveillance.

[144] The eight states with existing state regulation of aerial surveillance introduced their bills as late as March 2013. Among the 41 states with pending legislation, California had the first bill proposed, although not passed, in December 2012.

intrusive nature of the surveillance capabilities embedded in this new technology.[145] As of August 2013, eight states have passed legislation regulating how drones may be used by private individuals and law enforcement.[146] Each one of these states evinces a legislative intent to create an enforceable privacy interest, and the particular scheme illustrates how the collection and retention of information can be effectively regulated. For instance, Florida's statute, the Freedom from Unwanted Surveillance Act, prohibits state and local law enforcement from using a drone to gather evidence or other information except in certain limited circumstances: (1) when police have a warrant; (2) to counter a high risk of a terrorist attack deemed credible by DHS; or (3) when there is reasonable suspicion that swift action is needed to prevent escape of a suspect, prevent imminent danger to life, serious damage to property or search for a missing person.[147] Virginia's response to drone surveillance was to place a moratorium on all domestic drone use until 2015.[148] Within this period legislators have committed to developing protocols for UAV use.[149] Idaho's act, the Preserving Freedom from Unwanted Surveillance Act, took effect on July 1, 2013.[150] The law prohibits any person, entity, or state agency from using unmanned aerial surveillance without a warrant to conduct surveillance on, gather evidence or information

[145] *See e.g.* titles of drone surveillance legislation: Citizens Protection From Unwarranted Surveillance Act – AZ; Freedom from Unwanted Surveillance Act- FL; Preserving Freedom from Unwanted Surveillance Act – ID; An Act to Protect the Privacy of Citizens from Domestic Unmanned Aerial Vehicle Surveillance – ME. Response has been rapid to quell anxiety about the very real and sensitive privacy concerns/issues raised by deployment of drones.

[146] Florida, Idaho, Illinois, Montana, Oregon, Tennessee, Texas, and Virginia. Freedom from Unwanted Surveillance Act, S. 92, 2013 Cong. (Fl. 2013)(enacted); S. 1134, 62d Cong. (Id. 2013)(enacted); S.1587, 98th Cong. (Il. 2013)(enacted); S. 196, 63d Cong. (Mt 2013)(enacted); H. 2710, 77th Cong. (Or. 2013)(enacted); Freedom from Unwanted Surveillance Act, S. 796, 108th Cong. (Tn. 2013)(enacted): Texas Privacy Act, H. 912, 83d Cong (Tx. 2013)(enacted); and S. 276, 85th Cong. (Ia. 2013); S. 1331, 2013 Cong. (Va. 2013)(enacted).

[147] Freedom from Unwanted Surveillance Act, S. 92, 2013 Cong. (Fl. 2013)(enacted).

[148] S. 1331, 2013 Cong. (Va. 2013)(enacted). Exceptions: Amber alert; Senior alert; Blue alert; search or rescue; training exercises of the Virginia National Guard; damage assessment, traffic assessment, flood stages, wildfire assessment.

[149] See id.

[150] S. 1134, 62d Cong. (Id. 2013)(enacted).

about, or photograph or record specifically targeted persons or property without consent.[151] Violation of the statute gives the aggrieved party a civil cause of action against the violator. Exceptions under the statute include drug investigations, search and rescue missions, and allowance for an owner of a business to monitor the premises.[152]

Thirty-four other states have introduced legislation to regulate the use of drone surveillance, and the proposed bills share common elements.[153] Most have a warrant requirement and an exigent circumstances exception. Massachusetts authorizes drone use with a warrant but limits the surveillance to only the subject of the warrant.[154] The proposed bill contains specific language instructing the police to avoid data collection on other individuals, homes, and areas other than those related to the target of the investigation.[155] Maine's proposed legislation allows for drone surveillance with a court order if police demonstrate specific and articulable facts demonstrating that there is reasonable suspicion of criminal activity that the UAV can uncover, and that alternative methods of information gathering are too costly or pose a serious risk to a person's bodily safety.[156] Virtually all states with proposed unmanned aerial surveillance legislation have exceptions that arguably erode the privacy protections of their citizens. For instance, Texas, which passed its law in June 2013, has nineteen exceptions for allowing drones, including permitting realtors to use drones to take pictures of real estate and oil

[151] See id.
[152] S. 1134, 62d Cong. (Id. 2013)(enacted).
[153] Proposed legislation in nine of the thirty-four states is no longer active for the current legislative session: Arkansas, Georgia, Maine, New Hampshire, New Mexico, North Dakota, Oklahoma, Washington, and Wyoming.
[154]
[155] See S.No. 1664, 188th Gen. Court (Mass. 2013)(" Under no circumstances shall unmanned aerial vehicles be used to track, collect or maintain information about the political, religious or social views, associations or activities of any individual, group, association, organization, corporation, business or partnership or other entity unless such information relates directly to investigation of criminal activity, and there are reasonable grounds to suspect the subject of the information is involved in criminal conduct".
[156] An Act To Protect the Privacy of Citizens from Domestic Unmanned Aerial Vehicle Use, S. 236, 126th Cong, (Me 2013); , Freedom from Drone Surveillance Act, S. 1587, 98th Cong. (Il. 2013)(enacted). New Hampshire also allows for a reasonable, articulable suspicion standard whereby law enforcement or "employees of governmental agencies or other entities, public or private" may proceed to use a drone without getting a court order first. See An Act prohibiting images of a person's residence to be taken from the air, H. 619 (NH 2013).

companies to use them to monitor their rigs.[157]

The most common remedies for a violation of these statutes are exclusion of the evidence from criminal prosecution and grounds for civil action by the aggrieved party. Legislatures in a small number of states have proposed that an entity or person can be charged with a crime for violating the law.[158] Maine prohibits drone use by anyone other than law enforcement.[159] Illinois is seeking to require reporting and retention requirements for all drone users (private and public).[160] Some states prohibit weaponry and enhanced technologies such as facial recognition technology.[161] Iowa and Virginia permit use for amber alerts, and natural disasters.[162]

Legislatures are likely going to move more quickly than the courts. Regulation is imperative if there is any promise of curtailing the slow demise of a citizen's right to privacy in the face of these powerful aerial observers. Consumer protection laws illustrate the ability of state legislatures to craft protections for consumers even in the face of threats to personal privacy. The Massachusetts consumer protection statute,[163] along with a general statute that protects privacy,[164] has been used to protect consumers against the sharing of private information

[157] *See* Sara Kellogg, *Drones: Coming to the Skies Near You*, Washington Lawyer, July/Aug. 2013.

[158] See An Act prohibiting images of a person's residence to be taken from the air, H. 619 (NH 2013). "A person is guilty of a class A misdemeanor if such person knowingly creates or assists in creating an image of the exterior of any residential dwelling in this state where such image is created by or with the assistance of a satellite, drone, or any device that is not supported by the ground."

[159] Act to Protect the Privacy of Citizens from Domestic Unmanned Aerial Vehicle Surveillance, S. 236, 126th Cong. (Me. 2013).

[160] Freedom from Drone Surveillance Act, S. 1587, 98th Cong. (Il. 2013)(enacted).

[161] Among others, *See* S. 783, 27th Cong. (Hi. 2013); S. 4839 (NY 2013); Aerial Privacy Protection Act, S. 411 (RI 2013).

[162] *See* S. 276, 85th Cong. (Ia. 2013); S. 1331, 2013 Cong. (Va. 2013)(enacted).

[163] Mass. Gen. Laws Ann. ch. 93A, § 2 (West)(Under this statute, "[u]nfair methods of competition and unfair or deceptive acts or practices in the conduct of any trade or commerce are hereby declared unlawful.")

[164] Mass. Gen. Laws Ann. ch. 214, § 1B (Under this statute, "[a] person shall have a right against unreasonable, substantial or serious interference with his privacy.")

or intrusions into privacy in the commercial context.[165] Mass. Gen. Laws, ch. 214, § 1B provides general protections "against unreasonable, substantial or serious interference with his privacy."[166] The purpose of 214 § 1B is to prevent the "disclosure of facts ... that are of a highly personal or intimate nature when there exists no legitimate, countervailing interest."[167] These laws were erected to prohibit intrusions to privacy in both specific and broad contexts.

V. Recommendations --

A. Shifting the Focus from Privacy to Power in the Fourth Amendment Analysis

Some scholars argue that new technologies that challenge our longstanding reasonable expectation of privacy test reveal that privacy is no longer a legitimate proxy for what the Fourth Amendment protects.[168] Professor Ohm observes that given how rapidly technology is changing our everyday lives and our notions about what is considered "private", a more appropriate way to understand the purpose of the Fourth Amendment is as a restraint on police power.[169] This paradigm shift is a dramatic move away from how we have thought about privacy and its relationship to the Fourth Amendment for over half a century. But it is not without precedent.

[165] One such case arose where the Massachusetts Attorney General objected to private sale of information regarding bankrupt telecom service provider's customer base, including credit card and phone history. See In re Essential.com, Inc., No. 01-15339 (D. Mass. Bankr. Aug. 9, 2001). See the Massachusetts Attorney General's objection, available at http://web.archive.org/web/20040804065025/http://www.fenwick.com/About_Fenwick/Privacy_Documents/Essential_AG_2d_Objection_8-7-01.pdf (last visited August 13, 2008), relied on the following authority as a basis for a potential violation of Mass. Gen. Laws Ann. ch. 93, § 105 and Mass. Gen. Laws Ann. ch. 93A, § 2. See also, *Weld v. Glaxo Wellcome Inc.*, 434 Mass. 81, 746 N.E.2d 522 (2001), where the Court affirmed the certification of a class action for alleged privacy abuses due to transfer of consumer information by CVS Pharmacy and others.

[166] Mass. Gen. Laws ch. 214, § 1B.

[167] Dasey v. Anderson, 304 F.3d 148, 153-54 (1st Cir. 2002) quoting Bratt v. Int'l Bus. Machs. Corp., 392 Mass. 508, 467 N.E.2d 126, 133-34 (1984) (citations omitted)

[168] See Paul Ohm, The Fourth Amendment in a World Without Privacy, 81 Miss. L.J. 1309., Daniel J. Solove, Nothing to Hide,: The False Tradeoff Between Privacy and Security 114 (2011), Thomas Clancy, What Does the Fourth Amendment Protect: Property, Privacy or Security? 33 Wake Forest L Rev. 307, 361 (1998).

[169] See Ohm at 1336-38.

Prior to *Katz*[170] we associated property with that which the Fourth Amendment was created to protect. But *Katz* changed that by replacing privacy for property as a proxy for Fourth Amendment protection.[171] Ohm and others suggest that in this era of rapid technological growth, we substitute power as the proxy for that which the Fourth Amendment was created to restrain.[172] Ohm's proposition makes sense when one considers how new technologies have made it easier (and cheaper) to obtaininformation. Users willingly relinquish some of their privacy to avail themselves of these new devices.[173] For instance, most smartphones are equipped with tracking software that records the user's location with great precision.[174] Cellular systems update and record location data every few minutes of all phones on their networks.[175] Cell phone companies typically retain this data for a year or longer.[176] In June 2011, more than 322 million wireless devices were in use in the United States.[177] Most users are aware of the phones' tracking capability, yet most opt for the convenience of having their phone with them and choose to ignore concerns of being tracked.[178] As Ohm argues, the prevalence of people with phones equipped with this technology may make location data "public" no matter how it is retrieved.[179]

---

[170] Katz v. United States, 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).
[171] See Jones, 132 S. Ct. at 957 (Alito, J., concurring).
[172] Ohm at 1336.
[173] See, *e.g.*, NPR, The End of Privacy, http://www.npr.org/series/114250076/the-end-of-privacy (all Internet materials as visited Jan. 20, 2017, and available in Clerk of Court's case file); Time Magazine, Everything About You Is Being Tracked—Get Over It, Joel Stein, Mar.21, 2011, Vol. 177, No. 11. See also, Jones at 10.
[174] Peter Maass and Megha Rajagopalan, *"That's No Phone. That's My Tracker"*, NY Times. July 15, 2012. GPS tracking software 5 years ago could locate a phone to a level of accuracy within 50 feet. See Kevin McLaughlin, The Fourth Amendment and Cell Phone Location Tracking: Where are We?, 29 Hastings Comm. & Ent. L. J. 421, 427 (2007); Adam Cohen, What Your Cell Phone Could be Telling the Government, TIME, Sept. 15, 2010.
[175] See id.
[176] See id.
[177] See Jones at 963, citing to CTIA Consumer Info, 50 Wireless Quick Facts, http://www.ctia.org/consumer_info/index.cfm/AID/10323.
[178] Maybe a cite to Solove's nothing to Hide?
[179] Courts could also treat this information as unprotected because those using such devices are legally considered consensually sharing their data with third parties and therefore assume the risk that third parties will share it with the government. See e.g., Smith v. Maryland, 442 U.S. 735, 743-44 (1979), the United States Supreme Court reiterated

As technology has rapidly advanced in the past decade, social norms concerning what is considered private have changed as well.[180] According to a Pew Research study teens share more information about themselves than they have in previous years, minimizing the scope of what is considered private. [181] This is likely the result of growing up in an age of handheld devices that allow younger generations to communicate more by texting than talking on the phone or even emailing.[182] With the increasing use of cell phones, marketers are turning to practices called behavioral advertising and location-based-marketing. Behavioral advertising is the targeting of ads to persons based on the web pages they visit and the searches they perform.[183] Companies like Google and Amazon save the user data of persons who use their services.[184] Location-based advertising is the targeting of ads to persons based on their physical location.[185] Companies like

---

previous holdings that "a person has no legitimate expectation of privacy in information he *744 voluntarily turns over to third parties." E.g., United States v. Miller, 425 U.S., at 442–444, 96 S.Ct., at 1623–1624; Couch v. United States, 409 U.S., at 335–336, 93 S.Ct., at 619–620; United States v. White, 401 U.S., at 752, 91 S.Ct., at 1126 (plurality opinion); Hoffa v. United States, 385 U.S. 293, 302, 87 S.Ct. 408, 413, 17 L.Ed.2d 374 (1966); Lopez v. United States, 373 U.S. 427, 83 S.Ct. 1381, 10 L.Ed.2d 462 (1963).

[180] See Jones at 958 (Alito concurrence)

[181] Teens are sharing more personal information about themselves as the concept of "sharing" has become commonplace. On social media websites, 91% of teens now post a photo of themselves, up from that of 79% in 2006. Further, 20% of teens now post their phone number, up from a mere 2%. Information sharing among teens is influenced by a number of factors. Over the last six years, new social media sites have developed, giving users the opportunity to post more personal information, such as photos, cell phone numbers, and school locations. The increased use of and advanced technology makes it easier to post personal information, thus making it easier for the scope of the definition of privacy to minimize. See http://pewinternet.org/Reports/2013/Teens-Social-Media-And-Privacy/Main-Report/Part-1.aspx.

[182] In a 2012 study, Pew Research Center found that texting and cellular device use dominates a teen's choice of communication. Only 19% of teens talk on landlines and only 6% exchange emails, in comparison to 63% of teens who communicate through text messaging. See http://www.pewinternet.org/Reports/2012/Teens-and-smartphones/Communication-choices/Texting-dominates-teens-general-communication-choices.aspx.

[183] *See* FED. TRADE COMM'N, ONLINE BEHAVIORAL ADVERTISING: MOVING THE DISCUSSION FORWARD TO POSSIBLE SELF-REGULATORY PRINCIPLES 2 (2007), *available at* http://www.ftc.gov/os/2007/12/P859900stmt.pdf [hereinafter "FTC BEHAVIORAL ADVERTISING REPORT"].

[184] Ken Dilanian, http://www.post-gazette.com/stories/business/news/nsa-google-facebook-and-formerly-nordstrom-are-watching-you-695592/, *NSA, Google, Facebook and formerly Nordstrom are watching you* (Mark Herschberg, chief technology officer at Madison Logic, a New York-based company that provides data for advertisers stated that "[t]here are thousands of companies out there collecting information on customers… Google is reading through your email. Amazon is looking at not just what you buy, but what you shop for.");

[185] Patricia Covington, Meghan Musselman, Privacy and Data Security Developments Affecting Consumer Finance in 2008, 64 Bus. Law. 533, 544 (2009).

AT&T, Verizon, and Foursquare are selling the GPS location data of their users.[186] In 2010, businesses spent $42.8 million on location-based advertising.[187] That figure is projected to rise to $1.8 billion by 2015.[188]

In the past decade there has been a rise in the use of surveillance in public places such as malls, parks, schools, streets and highways.[189] Chicago for instance is considered to have the nation's most "extensive and integrated" network of government video surveillance cameras, according to former U.S. Homeland Security Secretary Michael Chertoff.[190] Just in the downtown area there are over 10,000 publicly and privately owned cameras, making it virtually impossible to avoid being identified and tracked while on a public way in the city.[191] Another example of the use of tracking devices is the toll roads equipped with automatic collectors that keep records of the path of travel of those users availing themselves of that convenience.[192] The prevalence of surveillance cameras capturing our images and our movements in public has changed attitudes about what is and should be considered an intrusion on one's expectation of privacy.[193]

---

[186] AT&T joins Verizon, Facebook in selling customer data, available at http://rt.com/usa/at&t-selling-personal-information-725/

[187] Nicole A. Ozer, Putting Online Privacy Above the Fold:Building A Social Movement and Creating Corporate Change, 36 N.Y.U. Rev. L. & Soc. Change 215, 237 (2012)

[188] Nicole A. Ozer, Putting Online Privacy Above the Fold:Building A Social Movement and Creating Corporate Change, 36 N.Y.U. Rev. L. & Soc. Change 215, 237 (2012)

[189] See Jones at 963.

[190] *See* CHICAGO'S VIDEO SURVEILLANCE CAMERAS: A PERVASIVE AND UNREGULATED THREAT TO OUR PRIVACY *a report from the* ACLU of Illinois (February 2011).

[191] Only approximately 1000 cameras are visible, the remaining 9,0000 are unmarked or invisible. Under a program known as "Operation Virtual Shield," all of these public and private cameras are integrated together, and monitored by the City's Office of Emergency Management and Communications ("OEMC"). See id.

[192] License plate recognition (LPR) technology automatically identifies the license plate and location of passing vehicles through the use of stationary cameras or cameras mounted on police cruisers. A 2009 national survey of police agencies found that "37% of large agencies (in this case, agencies with greater than 100 officers) already used LPR and that nearly one-third of those remaining planned to acquire it within one year." See Linda M. Merola & Cynthia Lum, Emerging Surveillance Technologies: Privacy and the Case of License Plate Recognition (Lpr) Technology, 96 Judicature 119, 120 (2012).

[193] See Jones at 963.

In this technological age, civil liberations are concerned about a slippery slope leading to an abandonment of privacy rights. Law enforcement officials have available to them a tool to conduct inexpensive, unobtrusive, continuous dragnet-type surveillance. For a moment, visualize a drone equipped with a GPS device, facial recognition software, and a high resolution camera, ascending to a height of10,000 feet above a major metropolitan area. Absent a warrant requirement, the police seemingly can engage in surveillance of law-abiding individuals who present no reasonable ground for suspicion.[194] Domestic drone use could be the nail in the coffin of privacy rights, and those concerned are voicing their objections and disseminating information on the dangers of drone surveillance to as many people as will listen.

A recalibration of police power in response to emerging technologies is consistent with Orin Kerr's "equilibrium adjustment" theory.[195] Kerr posits that when new technologies give the police greater power and make it easier to intrude into the lives of citizens, courts ultimately respond by limiting the use of the technology in order to restore the level of police power to that which existed prior to the advent of the new technology.[196] Ultimately the courts' response recalibrates the norms concerning what society should expect is private -- a type of correction mechanism. One of the early examples of this is the invention of the telephone. Among its many virtues, the telephone introduced a means for people to engage in criminal conduct without actually meeting in person. It enabled co-conspirators to plan their illicit activity over the phone. In many instances such as gambling, crimes could actually be committed by phone as opposed to physically appearing somewhere to conduct the activity. At the same time, it gave police a new

[194] Brief Amici Curiae for the Electronic Frontier Foundation and the ACLU of the National Capital area, United States v. Jones, at 7.
[195] Orin S. Kerr, *An Equilibrium-Adjustment Theory of the Fourth Amendment*, 125 HARV. L. REV 476 (2011).
[196] Kerr argues that for as long as there have been rules that govern the investigatory practices of the police, technological advances have caused courts to make adjustments to the rules to maintain the balance of police power. See Kerr at 485-6.

way to eavesdrop on illicit conversations without expending the resources of using undercover agents or surveillance teams. The wiretap became a common means for police to investigate criminal activity. Once this type of police surveillance became a reliable investigative tool for law enforcement, the Court departed from precedent and found a reasonable expectation of privacy in the telephone.[197] Promptly following *Katz*, Congress enacted a comprehensive statute regulating wiretapping.[198]

A more recent example of equilibrium adjustment involves government use of GPS devices.[199] The police use GPS devices to remotely track the location of persons by physically placing the device on a car or other property of the person under surveillance.[200] This technology makes it easier and cheaper for the police to track a suspect. All an officer has to do while deploying GPS technology is sit in an office and hit the refresh button on the computer to maintain the precise location of his target. There is no concern for detection (if the device is hidden well) and no need for several officers to follow the vehicle day and night. In *United States v. Jones*, the US Supreme Court unanimously agreed that the placement of the GPS device on the defendant's car constituted a search under the Fourth Amendment.[201] In his concurrence written on behalf of himself and three other justices, Justice Alito explained that the twenty-eight day surveillance of Mr. Jones' vehicle was the kind of persistent monitoring that society does not expect the government will conduct without a warrant.[202] The importance of Alito's concurrence is what it foreshadows in terms of recognizing that newer technologies expand the government's

[197] See Katz; *Jones*, 132 S. Ct. at 963
[198] 18 U.S.C. secs. 2510-2522 (2006 ed.); See also, *Jones*, 132 S. Ct. at 963.
[199] Kerr at 496.
[200] Before GPS devices there were radio beepers which acted much the same way as a GPS device but instead gave off a signal to police.
[201] *Jones*, 132 S. Ct. at 949.
[202] *Id.* at 964 ("For such offenses society's expectation has been that law enforcement agents and others would not – and indeed in the main, could not secretly monitor and catalogue every single movement of an individual's car for a very long period").

power and, in this instance, the degree of power is too great to go unchecked by the Fourth Amendment. Nonetheless, Alito cautions that not all government surveillance will implicate the Fourth Amendment. He notes that short-term monitoring of people in public facilities occurs routinely throughout society and will not and should not be subject to Fourth Amendment constraints.[203]

The distinction Justice Alito draws between persistent surveillance such as that used in *Jones* and the ubiquity of public surveillance cameras is important from an equilibrium adjustment perspective. Alito stops short of defining what constitutes long term monitoring, the trigger that would implicate the Fourth Amendment. Rather, in trying to maintain current social norms and practices, his concurrence attempts to recalibrate the balance between police power and personal privacy. Normatively, he observes that a certain degree of surveillance is expected in contemporary society because the public is aware of the prevalence of surveillance cameras throughout public thoroughfares, parks, public transportation facilities, and roads.[204] Importantly, it is not the omnipresence of video surveillance that concerns some justices. The concern regards the duration of the monitoring; the greater the duration, the more intrusive the invasion and the greater the amount of information the government can gather.

When applying the equilibrium adjustment theory to unmanned aerial surveillance, one can surely predict that the focus will be on the depth of the surveillance and the magnitude of information that can be gathered from this new technology.[205] In its prior aerial surveillance cases, the Supreme Court has held that there is no reasonable expectation of privacy in spaces

---

[203] See id.

[204] *Id.* at 962.

[205] This was true in Kyllo where the Court was concerned about what the police could learn from the thermal imager about what was happening inside the house and less concerned with the public vantage point from which police were using the device.

viewed from public navigable airspace.[206] According to equilibrium theory principles, when unmanned aerial surveillance at altitudes well into public navigable airspace becomes pervasive enough that it tips the balance of police power too far in the government's favor, courts will respond by erecting new rules that restore government power to its prior level. Notwithstanding, it is unlikely that all forms of unmanned aerial surveillance will be prohibited under the Fourth Amendment. Consistent with Justice Alito's approach in *Jones*, the Court will consider the extent to which society has grown accustomed to unmanned surveillance, including video monitoring of the sort just described. The Court's analysis will focus on the degree of sensory augmentation by unmanned aerial surveillance and the resulting ease of gathering information about people without constraint.[207] Included in the Court's assessment will be the high volume, low cost nature of this type of surveillance and whether there are reasonable limits that can be placed on police use of this technology to arrive at a reasonable balance between personal privacy and law enforcement purposes.

At this juncture, the application of the Fourth Amendment to emerging technologies is far from certain. To be sure, some of the theories expressed by the justices in recent cases predict possible Fourth Amendment approaches for evaluating government power in a world of emerging technologies. Whether courts will respond to restore the equilibrium depends largely on how pervasive the technology becomes and who will have access to it. At present, the availability of drones that have the ability to conduct the type of surveillance that concerns lawmakers has not reached its apex. The technology is evolving quickly and, as with all

---

[206] See Dow, Ciroalo, Riley

[207] See John Villasenor, *Observations from Above: Unmanned Aircraft Systems and Privacy*, 36 Harv. J.L. & Pub. Pol'y 457, 516-517)(predicts that it will not be the pervasiveness of unmanned aerial surveillance technology that will cause Court to create new limits, but the level of detail drones will be capable of capturing as the technology advances. As a result, the Court's previous rulings are "likely to provide more protection from government UAS observations than is commonly assumed").

economies of scale, the drive for demand promotes wider availability.[208] For lawmakers and courts the task is how to regulate the technology so that society can realize the benefits of these inventions without relinquishing the privacy Americans have traditionally relied upon. Recommendations can be made for how information obtained through UAVs should be used.

B. Proposals for Legislative and Regulatory Action

Legislatures must lead the way in balancing the potential of unmanned aerial surveillance with subjective expectations of privacy and societal norms. The tragic bombing at the Boston Marathon this year has fueled the Boston Police Department and Suffolk County District Attorney's push for enhanced surveillance measures in and around the city of Boston. The government's argument is a familiar one – had there been more government surveillance during the event, the police may have been able to prevent this tragedy or minimize the harm. The Boston police commissioner and the District Attorney have since called for a significant increase in police cameras to be installed in more public spaces throughout the city.[209] Commissioner Ed Davis has publicly endorsed the use of drones at next year's marathon.[210] Upon reflection, one can appreciate how drone surveillance could have aided law enforcement in their investigation of the Boston Marathon bombing. If drones had been aloft in the sky over the Boston Marathon, and in particular the crowded finish line, it is conceivable that they could have captured images of the suspects sooner than was made known to police from private surveillance cameras in the area. Arguably, additional resources used by police might have lessened the trauma and possibly

[208] See - draw on examples like GPS devices, thermal images, maybe license plate readers

[209] *Suffolk DA Conley Advocates for More Surveillance Camera Coverage in Boston*, Boston.Com (Apr. 22, 2013, 6:20 PM), http://www.boston.com/metrodesk/2013/04/22/suffolk-conley-advocates-for-more-surveillance-camera-coverage-boston/jmKqAS2cMDb9iF4kxhx9fI/story.html

[210] *Boston Police Ed Davis Wants Drones For Next Marathon*, Huffington Post (Apr. 27, 2013, 10:17 AM), http://www.huffingtonpost.com/2013/04/27/boston-police-drones-marathon_n_3169613.html. See also, http://www.huffingtonpost.com/2013/05/01/boston-bombing-drones_n_3192694.html?utm_hp_ref=politics.

saved lives lost in this senseless plot. But as was repeated by the Governor and top law enforcement officials during and in the aftermath of this tragedy, this was an unprecedented event - both in scope and duration.[211] Whenever one considers a response to a horrific event, like the senseless killing of innocent bystanders at a sporting event, one should pause long enough to consider whether extending broader powers to the police with few legal safeguards is a reasonable response or too great a cost to American privacy.

Routine unmanned aerial surveillance, without any particularized suspicion of criminal activity, will dramatically alter normative divisions between public and private life in the U.S.[212] Imagine the infrared camera attached to a drone pointed at us; inside our homes - bathing, sleeping, lounging in the backyard. The powerful type of surveillance capabilities of drones ought to be subject to strict regulations to ensure that their use does not erode individual privacy.[213] Suspicionless drone surveillance should be prohibited by state and federal laws. This technology offers concrete benefits, but without a set of rules to ensure that authorities do not abuse their power we tread on the verge of becoming a surveillance society in which people's movements are tracked, recorded and analyzed by authorities.

---

[211] Ryan, Andrew, Amid hunt for 2nd suspect, Boston a 'ghost town', http://www.bostonglobe.com/metro/2013/04/19/metropolitan-boston-awakens-under-siege-police-launch-manhunt-for-marathon-bomber/AcObNkQ5NOJC4Acv2azyZJ/story.html ("An unprecedented manhunt held metropolitan Boston hostage as police searched house by house for a suspect in the Marathon bombings, leaving almost 1 million people under siege.")

[212] The call for enhanced surveillance is not specific to an on-going or future threat. It is a request to continuously survey both from the air and from traffic lights and other public spaces. According to the ACLU 2011 report, psychologists have repeatedly found that people who are being observed tend to behave differently, and make different decisions, than when they are not being watched. This effect is so great that a recent study found that "merely hanging up posters of staring human eyes is enough to significantly change people's behavior. See Sander van der Linden, "How the Illusion of Being Observed Can Make You a Better Person," Scientific American, May 3, 2011, online at http://www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person.

[213]

Advanced technologies and third-party providers are enabling the government to engage in indiscriminate data collection.[214] Recent revelations have exposed the government's surreptitious data collection of millions of people for whom the government has no particularized suspicion.[215] According to authorities, the NSA has been collecting "wholly domestic" phone records and other electronic communications of Americans for the past several years.[216] Pursuant to a controversial collection program approved by Congress in 2008 under Section 702 of the FISA Amendments Act, the NSA collects more than 250 million Internet communications each year.[217] Approximately ninety-one percent of the communications are obtained from Internet providers such as Google, Yahoo and AOL through a program code-named PRISM.[218]

There may be some legal differences between the collection of phone records by the NSA pursuant to a FISA court's issuance of a warrant and warrantless surveillance from drones.[219] But the message worth heeding from the recent disclosure of the NSA's conduct is that the government will gather information about persons not engaged in criminal conduct as well as those who are. Unmanned aerial surveillance offers the government another covert method of

[214] See Megha Rajagopalan, *How Many Millions of Cellphones Are Police Watching?*, http://www.ProPublica.org/article/how-many-millions-of-cellphones-are-police-watching, July 12,2012.

[215] The information being collected is called "telephony metadata," consisting of information about whom you have called and the call length. The NSA secretly ordered Verizon to share its customers' metadata on an "ongoing daily basis" beginning April 25, 2013 and ending July 19, 2013. See Fisher, Max. *Expert: NSA Phone Data Collection Had Likely Been Ongoing Since 2006*, The Washington Post (June 6, 2013, 10:28 AM), http://www.washingtonpost.com/blogs/worldviews/wp/2013/06/06/expert-nsa-phone-data-collection-has-likely-been-ongoing-since-2006/

[216] See Ellen Nakashima, *NSA gathered thousands of Americans' emails before court ordered it to revise its tactics*, Washington Post (August 21, 2013) http://www.washingtonpost.com/world/national-security/nsa-gathered-thousands-of-americans-e-mails-before-court-struck-down-program/2013/08/21/146ba4b6-0a90-11e3-b87c-476db8ac34cd_story.html.

[217] See Glen Greenwald and Ewen MacAskill, *NSA PRISM program taps in to user data of Apple, Google, and others*, The Guardian (June 6, 2013) http://www.theguardian.com/world/2013/jun/06/us-tech-giants-nsa-data (detailing how the NSA created a secret program called PRISM whereby NSA could directly access data available through servers connected with Google, Facebook, Apple, and other internet service providers).

[218] See id.

[219] Although the chief judge of the FISA court has noted a "pattern of misleading statements by the government and hinted that the NSA possibly violated a criminal law against spying on Americans". See id.

collecting information about millions of Americans -- information that when pieced together creates a detailed profile of a person's lifestyle: their habits, recreational activities, family status, affiliations, health and hygiene, profession, economic and social status.

Congress and the states should pass legislation regulating unmanned aerial surveillance that is focused on transparency and accountability. Such recommendations include statutes that require warrants for all drone surveillance by law enforcement.[220] These statutes would recognize only a limited number of exceptions where unmanned aerial observation is necessary to prevent imminent loss of life or destruction of property.[221] It should be noted that this type of protection does little to protect the privacy of a person who is not the subject of the warrant and whose privacy is compromised by the breadth of judicially-approved UAV surveillance. But it would prohibit using unmanned aerial surveillance without a particularized target and probable cause to believe a crime is being committed.

Other legislative prescriptions include restricting the use of sensory enhancing technologies that can be mounted on UAVs. In situations that would authorize law enforcement to use a specific device such as an infrared camera, the law would require logs detailing the device used and the duration of its use. Furthermore, it is necessary to create an independent body to evaluate the impact of unmanned aerial surveillance on individual privacy. Each state should be mandated to create a commission comprised of representatives from the technology

[220] See *Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing before S. Judiciary Comm.*, 113 Cong. (2013) (statement of Amie Stepanovich, Dir. of the Domestic Surveillance Proj. Elec. Privacy Info. Ctr.). *Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing before S. Judiciary Comm.*, 113 Cong. (2013) (Written statement of the American Civil Liberties Union.).

[221] These types of situations include fires, chemical exposures, hostage situations and other instances where conventional surveillance would be inadequate in scope and time to prevent harm. See Troy Roberts, On the Radar: Government Unmanned Aerial Vehicles and Their Effect on Public Privacy Interests from Fourth Amendment Jurisprudence and Legislative Policy Perspectives, 49 Jurimetrics J. 491, 516-18 (2009)

industry, civil liberties organizations, policy advocates, and academics. This group would be assigned the task of measuring the impact drones are having on society's expectation of privacy and make recommendations on how to improve.

Members of Congress have called for the FAA to require operators, as part of the certification for flight, to submit a detailed report on the drones' intended use. Specifically, an operator, public or commercial, would have to document where the UAV will be operated, by whom, what type of data will be collected and how the data will be used and stored.[222] Each report should be made publically available.[223] This adds a layer of transparency to the certification process, which has been veiled in a shroud of secrecy.[224] It also elevates the privacy concerns beyond those of ordinary citizens to a federal regulatory agency. Further recommendations that would help protect privacy interests of individuals against unmanned aerial surveillance include date retention limitations with an emphasis on personally identifiable information and a requirement for all government agencies that operate drones to promulgate privacy regulations, including third party audits and oversight for law enforcement operations.[225]

Conclusion

Unmanned aerial surveillance poses many challenges to individuals' privacy rights while simultaneously offering tangible benefits to society. It is fair to say that drones are in our lives to stay, and the task at hand is to regulate their use. The Fourth Amendment was created to control

[222] See supra Part X.

[223] See, *Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing before S. Judiciary Comm.*, 113 Cong. (2013) (statement of Amie Stepanovich, Dir. of the Domestic Surveillance Proj. Elec. Privacy Info. Ctr.).

[224] See supra part X.

[225] See, *Future of Drones in America: Law Enforcement and Privacy Considerations: Hearing before S. Judiciary Comm.*, 113 Cong. (2013) (statement of Amie Stepanovich, Dir. of the Domestic Surveillance Proj. Elec. Privacy Info. Ctr.).

these types of governmental intrusions into our personal lives. Deference to police power at the exclusion of the Fourth Amendment is at odds with our constitutional protections. There is an ever-increasing awareness of the prevalence of drones on our soil, and we are very much in a nascent period when it comes to figuring out how to regulate them. However, one thing is certain: when the prevalence of drones does compel the Court to act, it will be another Katzian moment.