SILVERMCKENNA
The Internet and Privacy Law Group of STSW

SILVERMAN|THOMPSON|SLUTKIN|WHITE
ATTORNEYS AT LAW

26th Floor
201 North Charles Street
Baltimore, Maryland 21201

Anne T. McKenna, Group Chair
www.silvermckenna.com
Main Phone: 410-385-2225
Direct Dial: 443-909-7496
Fax: 410-547-2432
amckenna@silvermckenna.com

LEGAL MEMORANDUM

Overview of UAS/UAV Technology and Regulation; Analysis of Police Use of UAS/UAV Systems Under U.S. Constitution and Case Law

TO: **The Police Foundation and the U.S. Department of Justice – COPS Office**

FROM: **Anne T. McKenna, Esquire**

RE: ***Community Policing and UAS Guidelines to Enhance Community Trust***
2013-CK-WX-K002

SUBJECT: **Domestic Law Enforcement's Use of UAS/UAV: A Legal Analysis of the U.S. Constitution, Statutory Law, and Case Law, and An Overview of UAS/UAV Technology**

DATE: **April 10, 2014; final edits July 31, 2014**

SUMMARY OF LEGAL MEMORANDUM

This legal memorandum has been drafted pursuant to the principal legal consultant contract entered into between the Police Foundation and Anne T. McKenna to provide legal analysis and memoranda to be used by the Police Foundation, its Project Advisory Group, and the U.S. Department of Justice – COPS Office in the project entitled, *Community Policing and UAS Guidelines to Enhance Community Trust* (the "COPS contract"). Pursuant to the COPS contract Task 1 (detailed description of work appended to the COPS contract) and as discussed with the Police Foundation's Grants Manager, Maria Valdovinos, this first memorandum ("Legal Memo: Police Use of UAVs and the Law") addresses the following:

I. An overview of Unmanned Aerial System (UAS) and Unmanned Aerial Vehicle (UAV) technology;

II. A brief review of Federal Aviation Administration (FAA) regulation of UAS/UAV technology;

III. Task 1's Line Item (1), which includes:

   A. an overview of the U.S. Constitution with a focus on the First and Fourth Amendment considerations in UAS usage

   B. an overview of the existing federal electronic surveillance statutory scheme and how it may govern and apply to UAS usage

IV. Task 1's Line Item (2), which includes research, review and analysis of all Supreme Court decisions and all major U.S. Courts of Appeal decisions that relate to use of various forms of electronic surveillance so that participants may grasp how courts are addressing government use of electronic surveillance and, to a much lesser extent, private industry use of electronic surveillance.

V. Conclusions

SUBJECT INTRODUCTION

Advancements in electronic surveillance technologies in general and UAS/UAV technology in particular, now enable *domestic law enforcement* (collectively referred to as "police") to survey remotely public or open spaces, monitor traffic and air quality, conduct search and rescue missions, identify individuals in open spaces, etc., in non-intrusive and cost-efficient means. Current technology permits UAVs to be outfitted at a relatively low cost with high-powered cameras, thermal imaging devices, license plate readers, and laser radar.[1]

For the most part, however, the legality of police use of such evolving technologies in general and UAS/UAVs in particular has not heretofore been considered by courts. Police want to protect the public and to gather admissible evidence as thoroughly and efficiently as possible; it is fair to say that proper use of UAS/UAV technology would permit just that. But the Supreme Court's hodge-podge of electronic surveillance-related decisions and its openly acknowledged difficulty[2] in applying the framework of existing Fourth Amendment jurisprudence to advancing technologies adversely hampers officers' efforts to understand whether usage of these emerging technologies is permissible under the Fourth Amendment and its state equivalents.

In this memorandum, we attempt to address this conundrum and we provide a framework of analysis to assist police and the communities by whom they have been entrusted with safekeeping.

[1] Congressional Research Service Report, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, Thompson, Richard M., www.crs.gov (April 3, 2013).
[2] *See e.g., United States v. Jones*, 132 S.Ct. 945 (2012).

I. THE TECHNOLOGY: AN OVERVIEW OF UNMANNED AERIAL SYSTEMS (UAS) AND UNMANNED AERIAL VEHICLES (UAVs)

An UAV[3] is only one part of an UAS; the term UAS refers to the entire system, which includes the UAV, the digital network and electronic devices used to operate the UAV and the surveillance systems with which the UAV is equipped, as well as the personnel on the ground operating the UAV and operating the surveillance systems employed on the UAV. [4]

UAVs fly at slower paces and for longer intervals than their manned counterparts. They can fly autonomously, controlled by manned ground stations, or on a pre-programmed path below, in, or above piloted aircraft zones.[5] Current UAS models are incredibly diverse in size, function, and payload. They are generally categorized by size. Most commonly used for reconnaissance, surveillance, and inspection, small UASs weigh under fifty-five pounds (and can weigh as little as nineteen grams),[6] generally fly no higher than 400 feet above ground, and can remain airborne for several hours.[7] Larger UASs weigh more than fifty-five pounds, are capable of flying up to or above 60,000 feet, and can often remain airborne for days. They are most commonly used for data gathering, surveillance, and communications relay.[8]

Advancing technologies have enabled the UAV portion of an UAS to easily and cost-effectively be equipped with various electronic surveillance devices. We next briefly overview the specific and generally available forms of electronic surveillance that are available for use on the UAV portion of an UAS.

A. UAV Surveillance Capabilities: An Overview

Current technology permits UAVs to be outfitted at a relatively low cost with a variety of surveillance tools or payloads. The following electronic surveillance technologies can be employed via UAVs:

---

[3] UAVs come in a wide range of shapes and sizes. At the larger end of the spectrum is the Global Hawk used by the U.S. military: it is as large and nearly as fast as a business jet. At the smaller end, there are UAVs small enough to fit in a backpack or even the palm of a hand. For instance, the video-capable Nano Hummingbird, developed by California-based AeroVironment, weighs only two-thirds of an ounce. OBSERVATIONS FROM ABOVE: UNMANNED AIRCRAFT SYSTEMS AND PRIVACY**,** John Villasenor, 36 Harv. J.L. & Pub. Pol'y 457 (Spring, 2013).

[4] Congressional Research Service Report, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses*, Thompson, Richard M., www.crs.gov (Sept. 2012).

[5] *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat through Interagency Coordination*, Hendriksen, Patrice, 82 Geo. Wash. L. Rev. 205, (December, 2013)

[6] *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Olivito, Jonathan, 74 Ohio St. L.J. 669 (2013)

[7] *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat through Interagency Coordination*, Hendriksen, Patrice, 82 Geo. Wash. L. Rev. 205, (December, 2013)

[8] *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat through Interagency Coordination*, Hendriksen, Patrice, 82 Geo. Wash. L. Rev. 205, (December, 2013)

1. Optical devices:[9]

    a. High resolution visible light imaging (cameras with still photography and video capacity)
    b. Optically enhanced imaging—Night vision/FLIR
    c. Infrared sensors
    d. Electro-optical imagers[10]
    e. License Plate Readers[11]

2. Ultraviolet imaging

3. Synthetic aperture radar

4. Acoustical devices—"Listening In"[12]

5. Tracking devices

6. Thermal Imaging

7. Biometric identification systems: i.e., software and imaging capable of remote identification of individuals from a distance via biometrics, including face recognition, potential use of gait analysis, etc.[13]

8. Olfactory: Bio-surveillance systems[14] or "electronic noses"[15]

9. Weapons systems[16]

[9] *Drones and Privacy*, 14 Colum. Sci. & Tech. L. Rev. 72, Timothy T. Takahashi, Ph.D. (March 2013)
[10] *Unmanned and Unchecked: Confronting the Unmanned Aircraft System Privacy Threat through Interagency Coordination*, Hendriksen, Patrice, 82 Geo. Wash. L. Rev. 205, (December, 2013)
[11] *Watching the Watchmen: Drone Privacy and the Need for Oversight*, Jenkins, Ben, 102 Ky. L.J. 161 (2014)
[12] *Drones and Privacy*, 14 Colum. Sci. & Tech. L. Rev. 72, Timothy T. Takahashi, Ph.D. (March 2013).
[13] Biometrics are discussed in more depth below. For a lengthier discussion of potential biometric identification systems, see *Wiretapping & Eavesdropping: Surveillance in the Internet Age, 3rd Ed.*, Chapter 31—Biometrics, Fishman & McKenna, (West/Thompson 2013).
[14] Biosurveillance systems, with sensors to detect radiation levels and chemicals in the atmosphere, enable situational awareness that may prove critical in the event of chemical or nuclear accident or in the event of a terrorist attack with weapons of mass destruction.
[15] *Drones and Privacy*, 14 Colum. Sci. & Tech. L. Rev. 72, Timothy T. Takahashi, Ph.D. (March 2013)
[16] As noted, the International Association of Chiefs of Police (IACP) in its August 2012 *Recommended Guidelines for the use of Unmanned Aircraft* strongly discourages use of any weapons systems on a UAV.

With respect to weapons systems, The International Association of Chiefs of Police (IACP) in its August 2012 *Recommended Guidelines for the Use of Unmanned Aircraft* strongly discourages use of any weapons systems on an UAV. Key intelligence officials, including the U.S. President, have openly acknowledged that U.S. military operations involving UAS utilize UAVs that are equipped with weapons systems and that such military UAVs are used to conduct targeted strikes of enemy combatants and enemy targets.[17] Use of such military UASs/UAVs by domestic law enforcement would raise clear strong constitutional concerns and violate the *Posse Comitatus* Act, 18 U.S.C. § 1385, which prohibits use of military forces and equipment in domestic law enforcement.[18]

The use of UAVs equipped with weapons systems by police is strongly discouraged by the IACP as such use would likely generate strong public outcry and, in turn, legislative backlash against any type of police use of UAVs. Thus, our analysis of legal issues surrounding police use of UAS does not address police use of UAVs equipped with weapons systems other than to state preliminarily that it is undersigned counsel's legal opinion that police use of UAVs equipped with weapons systems and actual use of such weapons systems is illegal.

B. UAV Applications: Current Use and Potential Use of Surveillance Technologies

UAVs have already been successfully used domestically in search and rescue missions, surveillance during police standoffs, and border control.[19] The Customs and Border Protection Agency has been employing UAVs since 2005 to monitor illegal border crossings and drug trafficking.[20] Some police departments have begun using drones to increase security at large sporting events, assist in crime prevention, and survey private property.[21] NASA and NOAA have both used UAVs for scientific research, data collection, and environmental monitoring. [22] Other current uses by public entities include "law enforcement, firefighting, border patrol, disaster relief, search and rescue, military training, and other government operational missions."[23]

---

[17] See e.g., *Delays in Effort to Refocus C.I.A. From Drone War*, The New York Times, Sunday cover story, April 6, 2014.

[18] Use of Army and Air Force as *posse comitatus*, 18 U.S.C. 1385, provides:
Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.

[19] *Watching the Watchmen: Drone Privacy and the Need for Oversight*, Jenkins, Ben, 102 Ky. L.J. 161 (2014)

[20] *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Olivito, Jonathan, 74 Ohio St. L.J. 669 (2013)

[21] *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Olivito, Jonathan, 74 Ohio St. L.J. 669 (2013)

[22] *Beyond the Fourth Amendment: Limiting Drone Surveillance Through the Constitutional Right to Informational Privacy*, Olivito, Jonathan, 74 Ohio St. L.J. 669 (2013)

[23] *Fact Sheet – Unmanned Aircraft System (UAS)*, FAA Press Release, Duqette, Alison, (January 6, 2014) http://www.faa.gov/about/initiatives/uas/

The FAA's plan to rapidly integrate UASs into the national airspace, discussed in more detail in Section II below, is causing an explosion in the technology and application of UAVs. Possible applications include the detection and observation of forest fires, surveying real estate development, monitoring hostage situations, and observation of oil pipelines.[24]

A brief discussion of the more commonly available electronic surveillance devices capable of use on UAVs is warranted.

GPS Tracking[25]

GPS stands for Global Positioning System; GPS devices are commercially available and readily affordable.[26] Typically, when one refers to "GPS" he or she is actually contemplating a GPS receiver.[27] The Global Positioning System is actually a constellation of twenty-seven Earth-orbiting satellites.[28]

In simplistic terms, the GPS receiver, which is the actual, electronic tracking device attached or used, locates no less than four of these orbiting satellites and computes the distance between itself and each satellite by analyzing high-frequency, low-power radio signals from the GPS satellites.[29] Using a mathematical principle known as trilateration, the GPS receiver uses these combined calculations to determine its own location.[30]

GPS reveals far more than a traditional electronic tracking device; a standard GPS receiver provides not only a particular location, but it can also, in real time, trace the person or thing's path, movement, and speed of movement.[31] GPS devices also maintain historical data recording the person or object's movements.[32] If a GPS receiver is left in "on" mode, it stays "in constant communication with GPS satellites."[33]

Thus, GPS can serve both passive tracking purposes (to locate a person or an object) as well as real-time tracking purposes (to track the real-time movement of a person or object as it is

---

[24] *Watching the Watchmen: Drone Privacy and the Need for Oversight*, Jenkins, Ben, 102 Ky. L.J. 161 (2014)
[25] Portions of this discussion have been excerpted from CLIFFORD S. FISHMAN & ANNE TOOMEY MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (Thomson Reuters, 4th ed. 2012).
[26] GPS devices are available for less than $100. For that amount of money, a consumer can purchase a pocket-sized or smaller gadget that discerns your exact location on Earth at any moment. Marshall Brain & Tom Harris, *How GPS Receivers Work*, HOWSTUFFWORKS (Aug. 1, 2013, 3:49 PM), http://electronics.howstuffworks.com/gps.htm.
[27] *Id.*
[28] Twenty-four of these satellites are in constant operation and three extra satellites are maintained in space in the event of failure with one of the other twenty-foursatellites. *Id.*
[29] *Id.*
[30] *Id.*
[31] *Id.*
[32] *Id.*
[33] *Id.*

actually occurring).[34] This distinction is referred to as passive monitoring (which describes location-only purposes monitoring) and active monitoring (which is described as real-time monitoring).[35]

As utilized on UAVs, GPS tracking can both permit the UAV operator to locate the UAV in the event line of sight or loss of control occurs while operating the UAV[36] and enable a UAV to locate and track a device equipped with GPS, including a particular phone, vehicle equipped with GPS, or other electronic device.

For government purposes, the use of GPS devices and GPS evidence is generally governed by the same statutes and case law progeny as traditional electronic tracking devices (see Section III below).[37] However, federal tracking laws typically do not apply to private industry's use of GPS tracking technology.[38]

License Plate Readers

Automated license plate readers (ALPR) are standard issue on many police vehicles and most large cities and states routinely employ ALPR. Some ALPR are mounted and stationary, often at toll booths or tunnel entrances such as the I-95 Harbor tunnel and tollbooth in Baltimore, others are moved throughout an area by officers.

The case law generally provides strong support for the legality of plate readers, but the public does not seem to appreciate the scope of the data collected and how long the data is retained. When the public does learn this, there is often a privacy outcry.[39] Given the concurring opinions in *U.S. v. Jones,* which are discussed in detail below, it is unclear how the current Supreme Court would react to government fusion centers, where data from plate readers, CCTV, and other forms of open space surveillance are merged together to create a comprehensive database that would easily enable police to review a 24/7 history of a citizens' travels and activities. We address questions of UAV-obtained data and data retention in a separate legal memorandum per Task 1's Line Item (6).

Surveillance Cameras; CCTV; Body Cameras

---

[34] See, Fredericks v. Koehn, 2007 WL 2890466 (D. Colo. 2007), adhered to on reconsideration, 2008 WL 3833775 (D. Colo. 2008), for discussion of active and passive monitoring.
[35] *Id.*
[36] http://www.satnews.com/story.php?number=915693999
[37] THE SPY WHO GPS-TAGGED ME, www.slate.com/articles/technology/2012/11/gps_trackers_to_monitor_cheating_spouses_a_legal_gray_area_for_private_investigators.html (last visited Aug. 8, 2013) [pull source].
[38] *Id.*
[39] The Minneapolis plate reader scandal story demonstrates this.

A discussion of the use of cameras in open spaces is beyond the scope of this memo. Suffice it to say, cameras—in many forms, shapes and sizes—are routinely employed in open spaces. Such surveillance is cost-effective, poses a deterrent to crime, and provides extremely valuable evidence.

Where the legal quandary arises is when cameras are capable of sound recording, and when cameras are connected to or merged and equipped with other identification systems, such as biometric identification software like face recognition, and connected to databases that provide comprehensive information about the subject and or individual being recorded. Google glass provides an illustrative example.

Thermal Imaging

The Supreme Court has spoken about the warrantless use of thermal imaging devices on homes and private properties: it is unlawful. But thermal imaging devices that record far more data than the device at issue in *Kyllo* are becoming commonplace. Thermal imaging-like devices that detect far more than a heat emission and thus outline will become readily available. Is use of such devices permissible? Should law enforcement be able to detect an individual's rising heart rate or blood pressure without the individual knowing?

Biosurveillance Systems

Biosurveillance systems, with sensors to detect radiation levels and chemicals in the atmosphere, enable situational awareness that may prove critical in the event of chemical or nuclear accident or in the event of a terrorist attack with weapons of mass destruction.[40]

These electronic noses have not yet faced any serious challenges in the courts.

Biometric Identification Systems[41]

"Biometrics" is a general term that is used interchangeably to describe a characteristic or a process.[42] As a *characteristic*, biometrics is defined as "a measurable biological (anatomical and physiological) and behavioral characteristic that can be used for automated recognition."[43]

---

[40] *Drones and Privacy*, 14 Colum. Sci. & Tech. L. Rev. 72, Timothy T. Takahashi, Ph.D. (March 2013)
[41] Portions of this discussion have been excerpted from CLIFFORD S. FISHMAN & ANNE TOOMEY MCKENNA, WIRETAPPING AND EAVESDROPPING (Thomson Reuters, 4th ed. 2012).
[42] For a definition of "biometrics," developed by the National Science & Technology Council's (NTSC) 2006 Subcommittee on Biometrics, see *Biometrics Glossary*, BIOMETRICS.GOV, http://www.biometrics.gov/documents/glossary.pdf (last visited Aug. 8, 2013).
[43] *Id*.

As a *process*, biometrics is defined as "[a]utomated methods of recognizing an individual based on measurable biological (anatomical and physiological) and behavioral characteristics."[44]

In 1907, the Department of Justice (DOJ) established a Bureau of Criminal Identification, which was based upon fingerprints.[45] In 1924, the DOJ tasked the precursor of the Federal Bureau of Investigation (FBI) with creating a national identification and criminal history system.[46] This led to today's Criminal Justice Information Services (CJIS) of the FBI.[47] By the 1960s, the United States had created automated technology for the storage and comparison of prints.[48] Digitization in the 1980s and early 1990s further increased the ease and efficiency of finger prints as a biometric identifier, and by the end of the twentieth century, fingerprint identification had become the norm for governments around the world. [49]

In the 1990s, private industry and the United States Government earnestly invested in developing new biometric identification technologies.[50] The early 1990s saw the beginnings of face recognition software development, and in 1993, the Department of Defense initiated its Face Recognition Technology program.[51] In 1994, "[t]he first patent granted for automated iris recognition was issued."[52] In 1996, the United States Army implemented real-time video face identification.[53]

In 2000, the Defense Advanced Research Projects Agency (DARPA) initiated the Human Identification at a Distance Program.[54] "The goal [of this program] was to develop algorithms for identifying individuals up to 150 . . . meters away [by combining] face and gait recognition technologies".[55] The stated "purpose of [this] program was to provide early warning . . . for force protection . . . terrorism, and crime."[56]

---

[44] *Id*.
[45] NAT'L SCIENCE & TECH. COUNCIL, THE NATIONAL BIOMETRICS CHALLENGE 5 (2011), *available at* http://www.biometrics.gov/Documents/BiometricsChallenge2011_protected.pdf.
[46] Kenneth R. Moses et al., *Chapter 6: Automated Fingerprint Identification System (AFIS), in* NAT'L INST. OF JUSTICE, THE FINGERPRINT SOURCEBOOK 6-1, 6-4 (Alan McRoberts ed., 2011), https://ncjrs.gov/pdffiles1/nij/225320.pdf.
[47] NAT'L SCIENCE & TECH. COUNCIL, THE NAT'L BIOMETRICS CHALLENGE 5 (2011).
[48] Moses et al., *supra* note 86 at 6-1, 6-4.
[49] *Biometrics Glossary*, NSTC, (2006), http://www.biometrics.gov/Documents/BioHistory.pdf (last visited 7/23/2012).
[50] *See* Laura K. Donohue, *Technological Leap, Statutory Gap, and Constitutional Abyss: Remote Biometric Identification Comes of Age*, 97 MINN.L. REV. 407, 419 (2012).
[51] *Id*. at 423.
[52] *Id*. at 419 n. 39.
[53] *Id*. at 423.
[54] *Id*. at 423-24.
[55] *Id*. at 424.
[56] *Id*. This program is one of the first examples of transition to biometric identification via remote technology. *See* NAT'L SCI. & TECH. COUNCIL, BIOMETRICS IN GOVERNMENT POST-9/11: ADVANCING SCIENCE, ENHANCING OPERATIONS 18 (Heather Rosenker & Megan Hirshey eds., 2008), *available at* www.biometrics.gov/documents/biometrics_in_Government_Post-9/11.pdf.

The events of September 11, 2001 ushered in dramatic changes in the use of biometrics and in funding for advancements in biometric technology.[57] 9/11 also provided the impetus for homeland security-related legislation that, with little constitutional consideration, funded the development and implementation of biometric identification systems and authorized the collection (by both overt and covert means), retention, and sharing[58] of individual biometric data.[59] In describing the impact of 9/11 on government-conducted electronic surveillance, one commentator noted:

> In this process, there is a widening of surveillance, with a range of personal data being collected for the purposes of securitized immigration control and a wide range of government agencies (and not only immigration agencies) having access to such data, as well as a deepening of surveillance (via the collection of extremely sensitive categories of personal data, including biometrics) .. . . Great emphasis [is] placed on the widening and deepening of information collection and sharing (including . . . biometrics) from a variety of sources.[60]

The astonishingly rapid developments in biometric identification systems have revolutionized government, military and private industry's security systems and means of identification of persons.[61] The use of biometrics and emerging biometric technologies continues to alter and change the way persons are and can be identified and, in turn, the way persons can be tracked and subjected to surveillance.[62] For instance, the technological advances in the biometric identification system known as face or facial recognition and the corresponding relatively recent ability of government and private industry to surreptitiously collect, retain and access hundreds of millions of individuals' facial biometric data have coalesced to permit the almost immediate identification of individual "faces in a crowd and three-dimensional face recognition."[63] Government and private industry have developed a variety of handheld mobile devices that permit collection and wireless verification of identity via fingerprint biometrics, face biometrics and iris scanning.[64]

---

[57] *See id*. at 425.
[58] *Id*. at 427-28. As a result of post-9/11 legislative changes, this sharing of data amongst government agencies occurs both horizontally (between federal agencies) and vertically (between federal and state and local governments). *See id.* at 45.9-61.
[59] *See* Valsamis Mitsilegas, *Immigration Control in an Era of Globalization: Deflecting Foreigners, Weakening Citizens, Strengthening the State*, 19 IND. J. GLOBAL LEGAL STUD. 3, 12 (2012).
[60] *Id*. at12-13.
[61] *See* Donohue, *supra* note 90, at 410.
[62] *See id*. For instance, in Israel, a security technology firm partnered with an Israeli company, i-Mature, to create Age-Group Recognition (AGR) software that requires a computer user to submit to a scan of a finger bone to determine age prior to accessing certain websites. *See* Press Release, EMC Corporation, RSA Security and i-Mature Partner on Next-Generation Biometric Technology to Further Protect Children on the Internet (Feb. 7, 2005), http://www.rsa.com/press_release.aspx?id=5497.
[63] NAT'L SCI. & TECH. COUNCIL SUBCOM. ON BIOMETRIS & IDENTITY MGMT., *supra* note 54, at 12.
[64] *Id.* at 13.

Thus, low cost "biometric handheld devices now make it possible to obtain rapid identification virtually anywhere."[65] Most people seem unaware of how private industry uses biometrics to identify and track individuals' location, preferences and associates.[66]

II. FEDERAL AVIATION ADMINISTRATION'S REGULATION OF UASs

The Federal Aviation Administration (FAA), a division of the US Department of Transportation, authorized the first UAS usage in 1990.[67] The FAA is the primary regulatory agency of UAS usage, but their domain of regulation is safety, not privacy.[68] For this reason, there have been recent pushes to include the Department of Justice and the Department of Homeland Security in determining privacy regulations for the usage of UASs.

---

[65] *Id.*
[66] *Cf.* Lisa Vaas, *Apple's Siri Voiceprints Raise Privacy Concerns*, NAKED SECURITY, SOPHOS (June 28, 2012), http://nakedsecurity.sophos.com/2012/06/28/apples-siri-voiceprints-raise-privacy-concerns/ (IBM employees unaware of security risks from use of mobile device apps).
[67] *Fact Sheet – Unmanned Aircraft System (UAS)*, FAA Press Release, Duqette, Alison, (January 6, 2014) http://www.faa.gov/about/initiatives/uas/
[68] *Drones in the Homeland: A Potential Privacy Obstruction Under the Fourth Amendment and the Common Law Trespass Doctrine*, Oyegunle, Ajoke, 21 CommLaw Conspectus 365 (2013)

A. Current FAA Regulations

The FAA Modernization and Reform Act of 2012, signed into law by President Obama on February 14th, 2012,[69] provides funding to the FAA and requires the FAA to achieve the safe integration of UASs into the national airspace by September 30, 2015. This would include the development of acceptable standards of operations and certification, licensing of operators, air traffic requirements, and designation of safe national airspace. The law also states that the FAA will make recommendations and projections on "the best methods to enhance the technologies and subsystems necessary to achieve the safe and routine operation of civil unmanned aircraft systems in the national airspace system." [70]

Some components of the law have garnered intense opposition. Under this legislation, the FAA is required to remove much of the bureaucratic red tape that hinders government agencies from receiving COAs quickly.[71] The FAA is also required to allow "'a government public safety agency' to operate any drone weighing 4.4 pounds or less as long as certain conditions are met (within line of sight, during the day, below four hundred feet in altitude, and only in safe categories of airspace)." [72]

The FAA allows for the usage of UASs in very controlled conditions. Depending on the type of UAV, most operations must occur under 55,000 feet of elevation, and most operations are currently not authorized to operate in Class B airspace, which "exists over major urban areas and contains the highest density of manned aircraft in the National Airspace System."[73]

Presently, there are two ways to obtain permission to legally operate an UAS within the national airspace system. Civil operators must obtain a Special Airworthiness Certificate in the Experimental Category (SAC-EC), which allow for the performance of "operations for research and development, market survey, and crew training." [74]

---

[69] *Drones in the Homeland: A Potential Privacy Obstruction Under the Fourth Amendment and the Common Law Trespass Doctrine*, Oyegunle, Ajoke, 21 CommLaw Conspectus 365 (2013)
[70] FAA Modernization and Reform Act of 2012, Pub L. No. 112-95
[71] *The Sentinel Clouds Above the Nameless Crowd: Protecting Anonymity from Domestic Drones*, Burow, Matthew L., 39 New Eng. J. on Crim. & Civ. Confinement 427 (Spring, 2013)
[72] *The Sentinel Clouds Above the Nameless Crowd: Protecting Anonymity from Domestic Drones*, Burow, Matthew L., 39 New Eng. J. on Crim. & Civ. Confinement 427 (Spring, 2013)
[73] *Fact Sheet – Unmanned Aircraft System (UAS)*, FAA Press Release, Duqette, Alison, (January 6, 2014) http://www.faa.gov/about/initiatives/uas/
[74] *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implication*, Hiltner, Philip J., 3 Wake Forest L.J. & Pol'y 397 (June, 2013)

Governmental agencies, including law enforcement, may attain a Certification of Waiver or Authorization (COA) in order to legally operate a UAS.[75] COAs may be filled out online, and the number of COAs being issued is rapidly increasing.[76] COAs impose certain requirements on those who obtain them.[77] According to the FAA's publications, these requirements include: 1. COAs should define the airspace in which the UAV is permitted to fly; 2. COAs must mandate coordination with air traffic control facilities; 3. COAs mandate UAV operation within eyesight of the operator when flown in public airspace; and 4. COAs may include special provisions relevant to the operation of the specific UAS.

B. FAA's UAS Test Sites

In a press release on December 30, 2013, the FAA announced their selection of six UAS research and test sites around the country, including the University of Alaska, State of Nevada, New York's Griffiss International Airport, North Dakota's Department of Commerce, Texas A&M University, and Virginia Polytechnic Institute and State University (VA Tech).[78] The goal of these test sites is to conduct research on "certification and operational requirements necessary to safely integrate UAS into the national airspace over the next several years."[79] The FAA will assist operators in setting up safe testing environments and ensuring the operators' adherence to strict safety standards.

Police should look to the data coming from these test sites and from the FAA studies into UAS usage as an ongoing source of information to assist in state and local law enforcement use of UASs and as a source of information for the public.

C. Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS): the FAA Roadmap

[75] *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implication*, Hiltner, Philip J., 3 Wake Forest L.J. & Pol'y 397 (June, 2013)
[76] *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implication*, Hiltner, Philip J., 3 Wake Forest L.J. & Pol'y 397 (June, 2013)
[77] *The Drones are Coming: Use of Unmanned Aerial Vehicles for Police Surveillance and its Fourth Amendment Implication*, Hiltner, Philip J., 3 Wake Forest L.J. & Pol'y 397 (June, 2013)
[78] *Press Release – FAA Selects Unmanned Aircraft Systems Research and Test Sites*, Duquette, Alison, (December 30th, 2013) http://www.faa.gov/about/initiatives/uas/
[79] *Press Release – FAA Selects Unmanned Aircraft Systems Research and Test Sites*, Duquette, Alison, (December 30th, 2013) http://www.faa.gov/about/initiatives/uas/

In accordance with the FAA Modernization and Reform Act of 2012, the FAA published in December of 2013 a roadmap that outlines the actions and considerations the FAA will take in order to ensure the safe integration of UAS into the National Airspace System (NAS). The following list of regulations is directly from that publication, and pertains to all UASs integrated into the NAS—police departments wishing to utilize UASs should necessarily be familiar and in compliance with these FAA UAS regulations:[80]

1. UAS operators comply with existing, adapted, and/or new operating rules or procedures as a prerequisite for NAS integration.
2. Civil UAS operating in the NAS obtain an appropriate airworthiness certificate while public users retain their responsibility to determine airworthiness.
3. All UAS must file and fly an IFR flight plan.
4. All UAS are equipped with ADS-B (Out) and transponder with altitude-encoding capability. This requirement is independent of the FAA's rule-making for ADS-B (Out).
5. UAS meet performance and equipage requirements for the environment in which they are operating and adhere to the relevant procedures.
6. Each UAS has a flight crew appropriate to fulfill the operators' responsibilities, and includes a pilot-in-command (PIC). Each PIC controls only one UA.*
7. Autonomous operations are not permitted.** The PIC has full control, or override authority to assume control at all times during normal UAS operations.
8. Communications spectrum is available to support UAS operations.
9. No new classes or types of airspace are designated or created specifically for UAS operations.
10. FAA policy, guidelines, and automation support air traffic decision-makers on assigning priority for individual flights (or flight segments) and providing equitable access to airspace and air traffic services. Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap.
11. Air traffic separation minima in controlled airspace apply to UA.
12. ATC is responsible for separation services as required by airspace class and type of flight plan for both manned and unmanned aircraft.
13. The UAS PIC complies with all ATC instructions and uses standard phraseology per FAA Order (JO) 7110.65 and the Aeronautical Information Manual (AIM).
14. ATC has no direct link to the UA for flight control purposes.

III. ELECTRONIC SURVEILLANCE LAW

A. <u>The U.S. Constitution: The First Amendment and the Fourth Amendment</u>

[80] *Integration of Civil Unmanned Aircraft Systems (UAS) in the National Airspace System (NAS) Roadmap*, US Department Transportation, Federal Aviation Administration. First Edition, 2013.

1. The Right to Privacy: Development of the Concept and U.S. Common Law[81]

The word "privacy" does not appear in the United States Constitution, [82]but in their seminal 1890 Harvard Law Review article, *The Right to Privacy*, Samuel Warren and Louis Brandeis framed our modern constitutional and common law concepts of privacy.[83] In large part due to Warren and Brandeis's article, the U.S. Constitution—despite missing the magic *privacy* word—is the cornerstone of modern privacy law.[84] Common law privacy concepts and the common law right to privacy have flowed therefrom and, as evidenced by the amount of civil ligation cases asserting invasion of privacy-based claims, the U.S. common law provides for a robust right to privacy.

There are some marked similarities between today's societal and legal privacy struggles and those of the 1890s. At the time Warren and Brandeis's article was published, American society was facing aggressive, sensationalistic press (the term "Yellow Journalism" was coined to describe private press activities of the time);[85] there was incredible growth in newspaper circulation rates[86] (which fueled the financial rewards reaped from more invasive, intrusive newsgathering activities);[87] and technological developments, including readily available and affordable photography devices (this era saw the mass market introduction of Kodak's small snap camera)[88] and recording devices,[89] which permitted individuals to be recorded and photographed at an unprecedented rate.[90] These factors—(1) legally unfettered gathering of personal data (2) by private industry for commercial gain (3) enabled through advanced technologies—combined to foster invasions of individual privacy on a scale heretofore unimaginable.[91] When boiled down to the aforementioned factors, which spurred Warren and Brandeis to write their article and advocate for a new legal right, connecting the dots further is unnecessary: the similarity of these privacy issues in 1890 and the privacy concerns surrounding police use of UAS is strikingly similar.

---

[81] Portions of this discussion of the origins of U.S. privacy have been excerpted from Anne T. McKenna's law review article, *Pass Parallel Privacy Standards or Privacy Perishes*, 66 Rutgers L. Rev. 1041 (2013)
[82] *See* U.S. CONST.; *see also* Mark Silverstein, Note, *Privacy Rights in State Constitutions: Models for Illinois?*, 1989 U. ILL. L. REV. 215, 218 (1989).
[83] *See* Samuel D. Warren & Louis D. Brandeis, *The Right of Privacy*, 4 HARV. L. REV. 193 (1890).
[84] *See generally id.*
[85] JOSEPH W. CAMPBELL, YELLOW JOURNALISM: PUNCTURING THE MYTHS, DEFINING THE LEGACIES 33 (2001).
[86] James H. Barron, *Warren and Brandeis,* The Right to Privacy, *4 HARV. L. REV. 193 (1890): Demystifying a Landmark Citation*, 13 SUFFOLK U. L. REV. 875, 889-90 (1979).
[87] *See id*. at 891.
[88] History of Kodak Milestones, KODAK, www.kodak.com/ek/us/en/our_company/history_of_kodak/milestones_chronology/1878-1929.htm.
[89] *See* DAVID R. SPENCER, THE YELLOW JOURNALISM: THE PRESS AND AMERICA'S EMERGENCE AS WORLD POWER 54 (David Abrahamson, ed., 2007).
[90] *See, e.g., id.* at 2-3.
[91] *See, e.g.*, Barron, *supra* note 16, at 889-91.

In their introduction to *The Right to Privacy*, Warren and Brandeis considered the Anglo-American jurisprudence system that enables our law's developmental flexibility to keep abreast of social, political, and technological changes.[92] The authors then highlighted how—enabled by developments in technology—the sacred precincts of private and domestic life were being invaded in ways not previously possible.[93] Warren and Brandeis then asked whether existing laws in 1890 were capable of protecting the privacy of the individual.[94] After an analysis of available legal remedies,[95] the two conclude that, while some laws may hinder certain types of privacy invasion, *e.g.*, libel and slander, existing laws were too limited in stopping unwanted personal data gathering by private industry.[96]

Warren and Brandeis looked to the U.S. Constitution itself and found that individual rights preserved by the First Amendment and the Fourth Amendment implicitly reflected a strong and vigorous right to privacy from government surveillance. [97] While Warren and Brandeis's concerns were focused on a privacy right that could protect the individual from private actors as opposed to state actors, their analysis of the First and Fourth Amendments were prescient to the UAV debate.

By providing the factual stage and describing in detail the nature of injury caused by privacy invasions, Warren and Brandeis unequivocally demonstrate the societal need for a new right.[98] The two then persuasively explain how the right to privacy is both derived from and present throughout our common law and historical concepts of "an inviolate personality" and "the right to be let alone."[99] Pointing to privacy protections afforded by tort law, evidence, property rights, contract law, and criminal law, the two establish that the right to privacy is not a new concept but something carried throughout all of these sources of common law, constitutional law, and statutory law.[100] Warren and Brandeis frame what the scope of the right to privacy is, the remedies it should afford, and reject what criticisms they foresee to the recognition of the right to privacy.[101] Warren and Brandeis's proposed common law right to privacy was ultimately recognized and adopted by the United States Supreme Court and by state courts and state legislatures across the nation.[102]

---

[92] Warren & Brandeis, *supra* note 15, at 193-95.
[93] *See id.* at 195.
[94] *See id.* at 197.
[95] *See id.* at 197-207.
[96] *See id.* at 207.
[97] *See id.* at 198.
[98] *See id*. at 197-98.
[99] *See id*. at 193, 197-205.
[100] *See id*. at 197-214.
[101] *See id*. at 214-20.
[102] *See generally* Benjamin E. Bratman, *Brandeis and Warren's* The Right to Privacy *and the Birth of the Right to Privacy*, 69 TENN. L. REV. 623 (2002) (examining the legal impact and legacy of The Right to Privacy); Richard C. Turkington, *Legacy of the Warren and Brandeis Article: The Emerging Unencumbered Constitutional Right to Informational Privacy*, 10 N. ILL. U. L. REV. 479 (1990) (tracing the development of privacy rights from The Right to Privacy).

2. The First Amendment

The First Amendment to the U.S. Constitution provides:

> Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.

Critics of police use of UASs raise the point that such use potentially violates the First Amendment's guarantee of freedom of association because the ability of police to know one's location and travels at all times will have a chilling effect on the freedom of association and free expression. As discussed below, Justice Sotomayor articulated similar concerns, albeit it with respect to police use of a GPS tracking installed on a car rather than police tracking via UAVs, in her concurrence in the Supreme Court's 2012 decision in *U.S. v. Jones*.[103]

In contrast, other commentators note that private use of UAVs as a method of news gathering is a First Amendment right.[104]

The most effective way to address Justice Sotomayor's First Amendment concerns and the public's fear is ensuring that police adhere to clearly specified acceptable use practices for UAVs and clearly expressed data gathering and data retention practices for data gathered via UAVs. A routine UAV patrol that monitors traffic or borders or environmental conditions is very different than the use of a UAV to surreptitiously track a certain individual for an extended period of time without a warrant.

3. The Fourth Amendment

The Fourth Amendment to the United States Constitution states:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly

---

[103] U.S. v. Jones, 132 S.Ct. 945, 956 (J. Sotomayor, concurring):

> Awareness that the Government may be watching chills associational and expressive freedoms. And the Government's unrestrained power to assemble data that reveal private aspects of identity is susceptible to abuse. The net result is that GPS monitoring—by making available at a relatively low cost such a substantial quantum of intimate information about any person whom the Government, in its unfettered discretion, chooses to track—may "alter the relationship between citizen and government in a way that is inimical to democratic society." *United States v. Cuevas–Perez*, 640 F.3d 272, 285 (C.A.7 2011) (Flaum, J., concurring).

[104] http://voxglobal.com/2014/02/privacy-policy-drones-and-the-first-amendment/, Walt Sharp, author, article posted 2/18/14 (site last visited 4/7/14).

> describing the place to be searched, and the persons or things to be seized.[105]

The Fourth Amendment applies only to government search and seizure.[106] It does not apply to private industry or third party search and seizure.[107] Section III.C., below, sets forth the Supreme Court's Fourth Amendment jurisprudence, and the Court's development of the reasonable expectation of privacy test and the third-party doctrine.[108] It specifically considers the Court's more recent, technology-specific Fourth Amendment cases to illustrate the application of the Fourth Amendment, the reasonable expectation of privacy test, and the third-party doctrine to the use of UASs, including emerging surveillance technology and existing digital data collection practices and geolocation tracking.

B. The Federal Legislative Scheme[109]

This section of Legal Memo: Police Use of UAVs and the Law overviews the federal statutory scheme that specifically pertains to electronic surveillance of communications and tracking. It does not address UAS/UAV specific legislation, which is addressed separately by the Police Foundation working with the consultant, per Task 1's Line Items (3) and (4). Pending federal legislation is also briefly discussed.

1. Title III

In 1968, in response to considerable social and political activity on a variety of fronts, Congress enacted the Omnibus Crime Control and Safe Streets Act.[110] Title III of that Act regulates interception of communications by public officials and private persons. In general terms, the electronic surveillance statutory scheme developed by Congress is collectively referred to as Title III.

Congress enacted Title III with two primary goals in mind. First, it sought to safeguard the privacy of wire and oral communications[111]—electronic communications were added to the

---

[105] U.S. CONST. amend. IV.
[106] *See* United States v. Jacobsen, 466 U.S. 109, 113 (1984).
[107] *See id.*
[108] *See generally* Orin S. Kerr, *Four Models of Fourth Amendment Protection*, 60 STAN. L. REV. 503 (2007) (discussing reasonable expectations of privacy test); Stephen E. Henderson, *The Timely Demise of the Fourth Amendment Third Party Doctrine*, 96 IOWA L. REV. BULL. 39 (2011) (discussing third-party doctrine).
[109] Portions of this discussion have been excerpted from CLIFFORD S. FISHMAN & ANNE TOOMEY MCKENNA, WIRETAPPING AND EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (Thomson Reuters, 3rd Ed. 2012), which provides a much more extensive discussion of the federal electronic surveillance legislative scheme.
[110] P.L. No. 90-351, 82 Stat. 197, 211 (1968), codified at 18 U.S.C.A. §§ 2510 et seq.
[111] Pub. L. No. 90-351, § 801(b), 82 Stat. 211 to 212 (1968); Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2177. State v. Gilmore, 201 Wis. 2d 820, 549 N.W.2d 401 (1996) (citing CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE (Thomson Reuters ed., 3rd ed. 2007).)

statute's coverage in 1986[112]—and, in particular, the privacy of innocent persons.[113] Thus, Title III forbids the interception of wire, oral or electronic communications by private persons unless the communication is intercepted by, or with the consent of, a participant, and significantly restricts the authority of law enforcement officials to intercept such communications. Second, it sought to provide law enforcement officials with a much-needed weapon in their fight against crime, particularly organized crime,[114] by empowering them to intercept such communications under carefully regulated circumstances. With regard to the latter goal, Congress endeavored to satisfy the procedural and substantive requirements previously enunciated by the Supreme Court, in *Berger v. New York*[115] and *Katz v. United States*,[116] as constitutional prerequisites to a valid interception-of-communication statute,[117] while defining "on a uniform basis"—applicable to state, as well as federal government—"the circumstances under which the interception of wire and oral communications [and, subsequently, electronic communications] may be authorized" by a judicially issued interception order.[118]

Title III is a detailed legislative scheme. It specifies who may authorize an investigator to apply for a court order, the information an application must contain, the findings a judge must make before issuing the order, how the order is to be executed, how recordings of intercepted conversations are to be secured, who must eventually receive notice that a phone or other communications facility was tapped or a location was bugged, among other details. The statute describes when information obtained from intercepted communications may be disclosed, identifies who may seek to suppress evidence and on what grounds, and sets forth an exclusionary rule. It also created a civil cause of action for those whose communications are unlawfully intercepted.

An in-depth analysis of the federal electronic surveillance legislative scheme is well beyond the scope of Legal Memo: Police Use of UAVs and the Law. For our purposes, however, there are components of this scheme to briefly consider because of the likelihood that electronic surveillance devices employed via UAVs may fall within the scope of the statutes. Specifically, in 1986, the Electronic Communications Privacy Act (ECPA) amended Title III's

---

[112] CLIFFORD S. FISHMAN & ANNE T. MCKENNA, WIRETAPPING & EAVESDROPPING: SURVEILLANCE IN THE INTERNET AGE § 1:15 (Thomson Reuters ed., 3rd ed. 2007).
[113] Pub. L. No. 90-351, § 801(d), 82 Stat. 211 to 212 (1968), Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2177.

[114] Pub. L. No. 90-351, § 801(c), 82 Stat. 211 to 212 (1968) (legislative findings introducing Title III); Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2157, 2177.
[115] Berger v. State of N.Y., 388 U.S. 41, 87 S. Ct. 1873, 18 L. Ed. 2d 1040 (1967).
[116] Katz v. U.S., 389 U.S. 347, 88 S. Ct. 507, 19 L. Ed. 2d 576 (1967).
[117] Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2161 to 62.
[118] Pub. L. No. 90-351, § 801(b), 82 Stat. 211 to 212 (1968), Senate Report (Judiciary Committee) No. 1097, 90th Cong. 2d Sess., Reprinted in (1968) U.S. Code, Cong. & Admin. News 2112, 2153, 2177.

definition of "wire communication" to include "electronic" communications.[119] The broad definition of "electronic" communications brings a host of modern, Internet-based communications, within ECPA's purview. Because ECPA expanded the definition of communications protected from surveillance, police use of any electronic surveillance device on an UAV that would permit interception of protected forms of communication must comply with ECPA.

In terms of tracking devices, there are only two federal statutes that directly address the use of tracking devices, and these only apply to law enforcement.[120] The Pen/Trap Statute regulates the use of pen/trap devices,[121] and the Stored Communications Act (SCA) also regulates storage of and access to stored electronic communications.[122]

The ECPA's SCA authorizes government access to stored communications in the hands of third party providers.[123] The SCA categorizes different types of stored communications (information) and outlines what the government must do to obtain access to those different types of communications.[124] The protection afforded by the SCA to these different types of information is based upon the type of stored information sought, i.e. addressing or dialing information—which by system design is in the hands of the third party provider for routing purposes—is afforded the least protection), whereas "content" information—which refers to the actual substance of the communication (whether email or voice call)—is afforded the greatest protection from surveillance).[125]

The Communications Assistance for Law Enforcement Act (CALEA) forbids the communications service providers, such as Verizon or Sprint, from producing "any information that may disclose the physical location of the subscriber" when the provider is producing call identifying information pursuant to the Pen/Trap Statute.[126] Thus, CALEA specifically limits information that providers may produce to law enforcement pursuant to the Pen/Trap Statute.

While this complex federal legislative scheme regulates both private actors and government, it regulates private and government actors in different ways.[127] The scheme does not limit what personal information and geolocation data the private actor or provider may collect, but it limits what information the private actor may give the government in the absence of court order.

---

[119] 18 U.S.C. § 2510 (2006).
[120] *See id*.§ 3117; 47 U.S.C. § 1002 (2006).
[121] 18 U.S.C.§§ 3121-3127,
[122] *Id.* § 2703.
[123] 18 U.S.C.§§ 2701 *et seq.*
[124] *Id*.
[125] *Id.*
[126] 47 U.S.C.§ 1002(a)(2)(B).
[127] *Id*.

Depending upon the purpose for which UAV based electronic surveillance may be employed, it is likely that Title III and related tracking device legislation will govern usage.

Corresponding State Wiretapping Statutes

The majority of states have mini-wiretapping acts and in some cases, such as Maryland and California, the corresponding state legislation is greater in its privacy protections. Police in such jurisdictions are strongly urged to be familiar with state and local electronic surveillance legislation, particularly in jurisdictions where there are variants from federal law.

2. Pending Legislation

Federal Proposed or Pending Legislation

The following are recently proposed Congressional bills that, if enacted, will impact the use of UAVs and other electronic surveillance devices at a domestic law enforcement level:

a. *Preserving Freedom from Unwarranted Surveillance Act of 2012 (S. 3287, H.R. 5925).* Would require law enforcement to obtain a warrant before using drones for domestic surveillance.
b. *Preserving American Privacy Act of 2012 (H.R. 6199).* Would permit law enforcement to conduct drone surveillance pursuant to a warrant, but only in investigation of a felony.
c. Other pending legislation includes multiple proposed electronic tracking laws passed in response to *US v. Jones*, and growing privacy concerns over tracking via geolocation data.

State Proposed or Pending Legislation

According to the NCSL, forty-three states have introduced 96 bills and resolutions concerning UAVs and UASs. As noted above, six bills have been enacted and resolutions have been adopted in six states.[128]

IV. FEDERAL COURT DECISIONS: GUIDANCE FOR POLICE USE OF UASS

A. Supreme Court Decisions

While the United States Supreme Court has yet to specifically consider whether the domestic law enforcement's use of many advancing technologies, in general, and UAVs, in particular, raises constitutional concerns, there is a complex and long-standing Fourth Amendment jurisprudence that can be applied to the use of UAVs and electronic surveillance devices with which a UAV may be equipped. By considering and familiarizing themselves with

[128] www.ncsl.org/issues-reserach/justice/unmanned-aerial-vehicles.aspx

the Court's prior Fourth Amendment rulings, police can ascertain what types of emerging electronic surveillance technologies may be legal.

The Fourth Amendment to the United States Constitution prohibits unreasonable search and seizure. For decades, the United States Supreme Court has considered the constitutionality of searches conducted with technology that enhances a human's own ability to see, follow, feel, hear or smell. The framework of this Fourth Amendment jurisprudence guides our discussion today, and the following layman-styled overview of that jurisprudence provides the necessary framework for police to gauge how such technologies may be appropriately used:

1. Katz v. United States (1967)—Listening Device in Public Phone Booth

In *Katz*,[129] the Court held that it violated the Fourth Amendment to attach a listening device to a public telephone booth. This reflected a significant development in the Court's Fourth Amendment rationale: the Court explicitly recognized that the Fourth Amendment protects people, not places. And Justice Harlan's Concurrence set the stage for a major development in our modern day concept of privacy, which is that one must have a reasonable expectation of privacy (RXP) for society and the law to recognize it and protect it.

The concept of RXP fundamentally changed privacy law, but technological advances have called the RXP analysis into question. When considering whether a person has an RXP in any given situation, courts consider this subjectively and objectively—so disclosure to a 3rd party takes on greater significance as policy and laws develop around how we protect privacy in our lives…so if you knowingly expose something to the public or voluntarily turn information over to someone else (a third party)…then you cannot be said to have a reasonable expectation of privacy.

Usage of UAVs in open spaces has not yet faced challenge in federal court, and for now, police may rely in good faith upon this RXP test.

2. Maryland v. Smith (1979) – Disclosure and the Third Party Doctrine

In *Smith v. Maryland*, 442 U.S. 735 (1979), the defendant had disclosed the phone numbers he dialed out to the telephone provider. The Court held that this voluntary disclosure to the telephone provider was third party disclosure, and thus it was no longer afforded them Fourth Amendment protection. If blindly applied to the Internet, *Smith v. Maryland*'s third party doctrine would result in the vast majority of our electronic information being unprotected by the Fourth Amendment.[130]

3. United States v. Knotts (1983)—Tracking Beeper

[129] Katz v. U.S., 389 U.S. 347 (1967)
[130] *See id*.

In *Knotts*,[131] the Court ruled that law enforcement did not violate the Fourth Amendment when, without a warrant, officers attached a tracking beeper to a container of chloroform. The beeper was placed in the container with the owner's consent prior to the defendant's taking possession of the container. The development in rationale is that a person travelling on a public thoroughfare has no RXP in his movements from one place to another.

This will be significant when a court considers the use of UAV enabled with a license plate reader to track an individual on a public roadway.

4. United States v. Karo (1984)—Tracking Beeper

In *Karo*,[132] the Court added a complicated nuisance: the Court ruled that installation of a tracking device without a warrant but with the consent of the original owner did not constitute a search—but—the Court held that once officers turned the tracking beeper on without a warrant, officers had conducted a search in violation of the Fourth Amendment.

5. Dow Chemical Co. v. United States (1986); California v. Ciraolo (1986) and Florida v. Riley (1989) —the Aerial Surveillance Photography Cases

In *Dow*,[133] the Court considered the Environmental Protection Administration's ("EPA") use of a commercial aerial photographer to photograph a Dow Chemical facility that Dow refused to allow the EPA to inspect. Claiming that the photographs might reveal valuable trade secrets that it had gone to considerable lengths to protect (particularly with regard to several open-air plants), Dow argued that the EPA's action constituted a search that violated the Fourth Amendment.[134]

Dow, like *Ciraolo*[135] and *Riley*[136]—two other Supreme Court cases involving the constitutionality of aerial surveillance—poses questions concerning the applicability of the Fourth Amendment to aerial surveillance. The cases differ, however, in two significant respects:

- First, unlike the naked-eye surveillance in *Ciraolo* (photos taken from a plane at 1000 feet of the fenced yard of a private residence) and *Riley* (photos taken from helicopter at 400 feet of the fenced yard of a private residence), the *Dow* surveillance was conducted with an aerial mapping camera that recorded on film far more than an observer in the

[131] 460 U.S. 276 (1983)
[132] United States v. Karo, 468 U.S. 705 (1984)
[133] Dow Chemical Co. v. U.S., 476 U.S. 227, 106 S. Ct. 1819, 90 L. Ed. 2d 226, 24 Env't. Rep. Cas. (BNA) 1385, 16 Envtl. L. Rep. 20679 (1986), Fishman and McKenna, Wiretapping and Eavesdropping § 30:13
[134] Fishman and McKenna, Wiretapping and Eavesdropping § 30:13
[135] In *Ciraolo*, 476 U.S. 207 (1986), the Supreme Court ruled that there was no Fourth Amendment violation when Officers flew over a private residence at 1000 feet and took photographs after receiving a tip about a marijuana grow operation.
[136] In Florida v. Riley, 488 U.S. 455 (1989), the Court again ruled that photographs taken from a helicopter at 400 feet over a private residence did not constitute a search.

plane could have seen with the naked eye. Thus, the surveillance in *Dow* was far more revealing than that in *Ciraolo* and *Riley*.

- Second, while *Ciraolo* and *Riley* involved surveillance of a curtilage of a private home, *Dow* involved surveillance of a huge multi-building industrial complex.[5]

The Court in *Dow* focused most of its Fourth Amendment attention on the question of whether the Dow complex should be likened to residential curtilage or an open field. A five-to-four majority opinion written by Chief Justice Burger, concluded that "for purposes of aerial surveillance," the latter analogy is more apt, and rejected Dow's claim.

Under the *Dow* case, the question of whether an UAV is employed in public airspace versus non-public airspace will be critical in determining the constitutionality of the usage.

6. NY v. Class (1986)—Exterior of Automobile

In *Class*,[137] the Court held that the exterior of an automobile is necessarily thrust into the public eye, so there is no RXP in that exterior and to visually examine it without a warrant does not constitute a search.

This is significant for UAV use because it supports the position that what is visible to any person standing in public is not protected by the Fourth Amendment. This strongly supports the argument that use of a UAV to see people, objects and activities that are knowingly exposed to the public does not raise Fourth Amendment concerns. Thus, the use of UAVs to monitor traffic conditions, weather conditions, a suspect publically fleeing police, a border crossing, an open field, etc., is permissible.

7. Kyllo v. United States (2001)—Thermal Imaging Devices

Resolving a split in the Circuits, the Supreme Court in *Kyllo*[138] held that the warrantless use of a thermal imaging device on a private residence constituted a search that violated the right to privacy afforded by the U.S .Constitution. *Kyllo* reflects a development in the Court's modern day privacy policy rationale: despite advances in technology, the Court will protect Constitutional concepts of privacy.

But the dissent in *Kyllo* presciently argued that Justice Scalia's rule—"firm but bright line of privacy at the door of the home"—would become problematic and defunct when the thermal imaging technology at use in *Kyllo* became readily available to the general public. And now we are there: thermal imaging devices are cheap and readily available to the public.

[137] NY v. Class, 475 U.S. 106 (1986).
[138] Kyllo v. US, 533 U.S. 27 (2001)

Thermal imaging devices are commonly available for installation and use on UAVs. Thus, the prudent officer who needs to employ thermal imaging via an UAV will seek a warrant.

8. Illinois v. Caballes (2005)—Dog Sniff No. 1—a traffic stop

In *Caballes*,[139] the Court ruled that officers did not violate the Fourth Amendment when they used of a drug-sniffing canine during a routine traffic stop where the sniff search did unreasonably prolong the length of the stop.

9. City of Ontario v. Quon (2010)—Text Messages

Having personally attended oral arguments in *Quon*,[140] I witnessed firsthand the Justices' discomfort with, understanding of, and difficulty in applying traditional RXP concepts to technological advances.[141] The Court in *Quon* determined that a SWAT team officer's superiors did not violate the Fourth Amendment when the supervising officer reviewed Officer Quon's text messaging to determine whether data overages were a problem under the City's data contract with a wireless provider. In the process of that pager audit, the supervisor saw Quon's lurid sexual text messages. But the Court ruled purely on the reasonableness of the pager audit, explicitly refusing to consider "far-reaching issues" it raised on the grounds that modern technology and its role in society was still evolving.[142]

The Court's struggle with understanding the capabilities of advancing technologies was uncomfortably on display during oral arguments in *City of Ontario v. Quon*.[143]. In *Quon*, the Court considered whether Special Weapons and Swat Team ("SWAT") members have an expectation of privacy in personal text messages sent on pagers issued by the city that employs them.[144] The Justices' struggle with the pager technology involved in the case was awkward. Chief Justice Roberts asked what would happen if a text message was sent to an officer at the same time he was sending a text to someone else,[145] at which point Justice Kennedy asked whether the officer in that situation would receive "a voice mail saying that your call is very important to us; we'll get back to you."[146] Both Justices Roberts and Scalia were openly grappling with the concept of a service provider when they stated they did not know that text

---

[139] Illinois v. Caballes, 543 U.S. 405 (2005)
[140] City of Ontario v. Quon, 130 S.Ct. 2619 (2010).
[141] The reporters' galley actually laughed out loud when one of the Justices asked during oral argument if someone could somehow print out and see Quon's text pages from his SWAT team pager.
[142] Justice Scalia harshly criticized the Court's rationale in his concurrence. He considered the majority opinion "vague" and charged his fellow justices with "disregard of duty" for their refusal to address the Fourth Amendment issues. A month after *Quon* was handed down, an appellate panel in a Georgia case similarly criticized it for "a marked lack of clarity" as it narrowed an earlier ruling to remove a finding that there was no expectation of privacy in the contents of email.
[143] *See* Transcript of Oral Argument at 44, *Quon*, 130 S. Ct. 2619 (No. 08-1332).
[144] *See Quon*, 130 S. Ct. at 2627.
[145] Transcript of Oral Argument at 44, (Roberts, C.J) ("What happens, just out of curiosity, if you're – he is ont the pager and sending a message and they're trying to reach for him, you know, a SWAT team crisis? Does he – does the one kind of trump the other, or do they get a busy signal?")
[146] *Id.*

messages are sent to a service provider before going to the intended receiver.[147] Such questions are particularly concerning because the Justices lack an understanding that, by design, today's technology discloses all of one's personal information to third parties.[148] Accordingly, under the third party doctrine in *Smith v. Maryland* in 1979, the vast majority of our electronic information would be unprotected.[149]

10. United States v. Jones (2012)—Warrantless Use of a Tracking Device

In 2012, the Court unanimously affirmed a 2010 decision from the United States Court of Appeals for the D.C. Circuit wherein the lower appellate court had ruled that law enforcement's warrantless attachment of a GPS device to a car and subsequent warrantless use of that GPS device to track defendant Jones for a period of 28 days constituted an unlawful search in violation of the Fourth Amendment. Although unanimous in their decision to affirm the D.C. Circuit, the Justices arrived at their unanimous holding through two sharply and evenly divided camps of rationale, with Justice Sotomayor striking out on her own.

For purposes of analysis, the *Jones* decision reflects a hard step backwards in considering law enforcement's use of advanced tracking in open spaces. Why? Because in this case, the Supreme Court took on law enforcement's warrantless use of GPS tracking devices.[150] The majority opinion based its holding on the act of trespass that occurred when police physically attached the GPS device to the suspect's vehicle.[151]

The *United States v. Jones* decision is remarkable in many respects, but for purposes of our discussion, there are three notable aspects of the decision. First, given earlier beeper and GPS-based location tracking decisions, it is striking that all nine Justices unanimously agreed that the warrantless installation of a GPS tracking device on a suspect's car and subsequent tracking for twenty-eight days constituted an impermissible search.[152] Second, although the

---

[147] *See id*. at 48-49 ("MR DAMMEIER: Well, they --they expect that some company, I'm sure, is going to have to be processing the delivery of this message. And --
CHIEF JUSTICE ROBERTS: Well, I didn't --I wouldn't think that. I thought, you know, you push a button; it goes right to the other thing. (Laughter).
MR. DAMMEIER: Well --
JUSTICE SCALIA: You mean it doesn't go right to the other thing? (Laughter)."),
[148] *See* Smith v. Maryland, 442 U.S. 735, 743-44 (1979).
[149] *See id*.
[150] United States v. Jones, 132 S. Ct. 945 (2012).
[151] *See id*. at 953. There were three opinions issued with the ruling: Justice Scalia authored the majority opinion, which was joined by Justices Roberts, Kennedy, Thomas, and Sotomayor; Justice Sotomayor also filed her own concurring opinion; and Justice Alito, joined by Justices Ginsburg, Breyer, and Kagan, filed a concurring opinion as well.
[152] For example in United States v. Knotts, the Court held that the use of a beeper to track Knotts's location was constitutional because a person does not have a reasonable expectation of privacy on public thoroughfares because one's movements are exposed to the public. 460 U.S. 276, 281-82 (1983). Additionally, police use of the beeper to supplement their visual surveillance did not result in a Fourth Amendment violation. *Id*. at 282. Rather, the Court stated: "Nothing in the Fourth Amendment prohibited the police from augmenting the sensory faculties bestowed upon them at birth with such enhancement as science and technology afforded them in this case." *Id*.

Justices were unanimous in their conclusion, the differences in the Justices rationales was stunning.[153] And third, the Justices' open struggle with certain issues reflects the increasing quagmire at the intersection of advancing technologies, privacy and reasonable expectations of privacy.[154]

In *Jones*, while the majority held the use of a GPS device to conduct prolonged surveillance was unconstitutional, it did so only because it found the police's physical act of attaching a GPS device to Jones's car was a trespass on Jones's property.[155] As Justice Sotomayor notes in her concurring opinion, a search occurs "at a minimum" where the government physically intrudes on a constitutionally protected area.[156] Her concurrence and Justice Alito's concurrence acknowledge very problematic limitations of the Court's decisions: advanced capabilities of new technologies enable the collection of vast amounts of data without a physical trespass.[157]

11. Florida v. Jardines (2013)—Dog Sniff No. 2—on the Front Porch

In *Jardines*,[158] the Court surprised some legal scholars: it ruled that a dog sniff at the front door of a house where officers suspected drugs were being grown constituted a Fourth Amendment search. Justice Scalia, who wrote the majority opinion, decided it purely on property grounds. While at first blush, the decision reflects a problem for UAV usage, the rationale is purely non-technology based. Justice Kagan's concurrence provides more useful guidance for our analysis of electronic surveillance devices: she describes the dog as a form of enhanced technology—a "super sensitive instrument, which the police deployed to detect things inside that they could not have perceived unassisted."

In *Florida v. Jardines*, police took a drug sniffing dog to the front porch of Jardines's home where police suspected Jardines was growing marijuana.[159] The dog tracked a scent he had been trained to detect and eventually sat, indicating that he had discovered the odor's

---

[153] Compare *Jones*, 132 S. Ct. at 949 (Scalia, J.) ("The Government physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a "search" within the meaning of the Fourth Amendment when it was adopted."), *with id*. at 955 (Stomayor, J., concurring) ("In cases of electronic or other novel modes of surveillance that do not depend upon a physical invasion of property, the majority opinion's trespassory test may provide little guidance."), *with id*. at 958 (Alito, J., concurring) ("I would analyzing the question presented in this case by asking whether respondent's reasonable expectations of privacy were violated by the long term monitoring of the movements of the vehicle he drove.").
[154] *See id*.
[155] *Jones*, 132 S. Ct. at949,
[156] *Id*.at 954 (Sotomayor, J., concurring).
[157] *Id*. at 959 (Alito, J., concurring) ("'[T]he search of one's home or office no longer requires physical entry, for science has brought forth far more effective devices for the invasion of a person's privacy than the direct and obvious methods of oppression which were detested by our forebears and which inspired the Fourth Amendment.'" (quoting Goldman v. United States, 316 U.S. 129, 135 (1942))).
[158] Florida v. Jardines, 569 U.S. ___ (2013).
[159] Florida v. Jardines, 133 S. Ct. 1409, 1413 (2013).

strongest point.[160] The Court considered whether using a drug sniffing dog on Jardines's porch to investigate the contents of his home constituted a search.[161]

In a 5-4 decision, Justice Scalia and the majority held that the use of the dog on the front porch constituted a search within the meaning of the Fourth Amendment because the police learned what they learned only by physically intruding onto Jardines's property.[162] The majority did not consider the *Katz* analysis or the use of a drug sniffing dog as technology.[163]

Justice Kagan joined the majority, but in her concurrence adds that she would have found the same outcome using the *Katz* analysis and precedent in *Kyllo v. United States*,[164] which held that where the government uses technology "not in general public use to explore details of the home that would previously have been unknowable without physical intrusion, the surveillance is a search…"[165] Justice Kagan says she would have found that the police used technology not in general public use (the drug sniffing dog) to explore details of the home.[166]

The dissenting Justices in *Jardines*, including the Chief Justice and Justice Kennedy, found there was no physical trespass. Notably, the dissent did not consider the dog to be technology; rather the dissenters said there was nothing that constituted trespass by bringing the dog to Jardines's front porch because "dogs have been domesticated for about 12,000 years."[167]

Jardines, like the *Jones* decision before it, provides little guidance to the electronic surveillance quagmire because it uses a property based approach, and thus, arguably does not apply to technology capable of determining information without physical intrusion upon property. Additionally, Justice Kagan's concurrence and reliance on *Kyllo*, where the Court relied upon the consideration of whether the thermal imaging technology at issue was readily available to the public, demonstrates another weakness in the Court's privacy jurisprudence: today, technology in general public use evolves so rapidly that previously expensive, highly invasive electronic surveillance technologies rapidly become cheap, readily available, and mainstream. This rule cannot form the basis of whether a form of surveillance technology is constitutionally permissible because it does not take into account the astounding pace of technological developments. It creates an unsustainable and uncertain legal rule if followed, because it would hold in one year a technology not in general public use to be constitutionally impermissible, yet advancements that made the technology readily available to the public one

---

[160] *Id*. The Court noted that "[t]he dog had been trained to detect the scent of marijuana, cocaine, heroin, and several other drugs, indicating the presence of any of these substances through particular behavioral changes recognizable by his handler." *Id*.
[161] *Id*.
[162] *Id*. at1417.
[163] *Id*. at 1417.
[164] 533 U.S. 27 (2001).
[165] *Jardines*, 133 S. Ct. at XX (Kagan, J. concurring) (quoting Kagan *Kyllo*, 533 U.S. at40).. *Kyllo* involved the warrantless use of a thermal imaging device on one's home, which the Court found to be unconstitutional.
[166] *Id*. at 1420
[167] *Id*.

year later would render that same illegal form of surveillance because the technology had become widely available to the public. UAVs are a perfect example of this. Five years ago, UAVs were not generally available for private commercial purchase on the Internet. Today, run a Google search using "drones for sale" as your search term—any 12-year old with an Internet connection and some babysitting money can find a drone readily available for inexpensive purchase on the Internet.

It is these discrepancies which demonstrate that the property based approach and other judicial precepts to determine whether use of surveillance technology is constitutional (such as the third party doctrine or the readily available to the public consideration) are not capable of creating clear precedent for courts; more importantly they fail to give clear guidance to law enforcement on appropriate uses for emerging technologies. These approaches have been acknowledged to be inadequate by the very judges struggling to address and limit the capabilities of rapidly evolving modern surveillance technologies that permit highly invasive, intrusive and surreptitious electronic surveillance.

12. Maryland v. King – DNA check swab following arrest

This June 2013 in a 5-4 decision, the Supreme Court ruled in *Maryland v. King* that taking and analyzing a cheek swab of an arrestee's DNA following an arrest based upon probable cause was reasonable under the Fourth Amendment.[168] The Court weighed the government interest in collecting the DNA against the privacy intrusion. Justice Kennedy, writing for the majority, found there to be a legitimate government interest in law enforcement's need "to process and identify persons and possessions taken into custody" and to be able to do so "in a safe and accurate way."[169] The majority compared the taking of DNA as a routine booking procedure, similar to fingerprinting.[170]

The majority described the collection of DNA by buccal swab as one requiring "no surgical intrusion beneath the skin" and one that poses no threat to the arrestee's health or safety.[171] Such a distinction will apply to many existing and emerging technologies, including importantly, almost all other biometric identification technology. Merely because a method of collection has improved or become less intrusive does not necessarily negate or diminish the intrusively private nature of the data collected. Fingerprinting for instance, provides a markedly sure and non-intrusive method of identifying an individual. But it does not also provide the government with intimate details about a detainees's familial blood relations, who the detainee's parents and siblings are, what a detainee's genetic makeup is, what a detainee's ancestry and country of origin is, and whether a detainee is more likely to have cancer than another individual

[168] *Maryland v. King*, 133 S. Ct. 1958, 1962 (2013).
[169] *Id*. at 1963.
[170] *Id*. at 1964.
[171] *Id*. at1963 (quoting Winston v. Lee, 470 U.S. 753, 760 (1985

due to their genetic makeup. DNA collection can permit all of this to be accomplished using existing technologies.

The dissent, written by Justice Scalia, firmly and correctly condemns. He acknowledges that solving crime is a noble objective, but with this quote emphasizes the scope of search the majority has now permitted law enforcement.[172]

> Today's judgment will, to be sure, have the beneficial effect of solving more crimes; then again, so would the taking of DNA samples from anyone who flies on an airplane (surely the Transportation Security Administration needs to know the identity of the flying public), applies for driver's license, or attends a public school. Perhaps the construction of such a genetic panopticon[173] is wise. But I doubt that the proud men who wrote the charter of our liberties would have been so eager to open their mouths for royal inspection.[174]

King is yet another recent case wherein the Court struggles with rapidly involving electronic surveillance and tracking technologies and with defining protections that should be afforded individual privacy in the face of a legislative void. The Justices could not be clamoring more openly for legislative guidance.

13. ***Riley v. California*** **(June 2014) – Search of Cellphone Incident to Arrest**

In *Riley v California*,[175] the Supreme Court unanimously held that the "search incident to arrest" doctrine, which allows a police officer to search any physical object in the possession of and closely associated with the person of an arrestee, does not apply to cell phones.[176] Barring exigent circumstances, police may search an arrestee's cell phone only if they first obtain a search warrant based on probable cause.

The *Riley* Court properly based its conclusion on the nature and vast quantity of information that the typical smart phone contains – including historical cell site location information. Although neither *Jones* (discussed above) nor *Riley* squarely holds that a warrant

---

[172] *Id*. at 1989.
[173] The Panopticon was first conceived by Jeremy Bentham. The idea is a prison designed with a central guard tower that may view all inmates housed there. At the same time, the prisoners have no view of who is watching them. Eventually, the inmates modify their behavior to be in line with those who watch them. *See* Ron Collins, "*Panopticon"? –You're your eyes on the word!*, SCOTUSblog (Aug. 1, 2013, 2:02 PM), http://www.scotusblog.com/2013/06/panopticon-keep-your-eyes-on-the-word/.
[174] See *King*, 133 S. Ct. at 1989.
[175] *Riley v. California*, 573 U.S. ___ (2014).
[176] For a more thorough discussion of Riley v. California, see Chapter 28 of *Wiretapping & Eavesdropping: Surveillance in the Internet Age, 3rd Ed.*, Fishman & McKenna, Thomson/West (2014 Supplement).

is needed to access either real time or historical cell phone information, those decisions point very clearly toward that conclusion.

B. U.S. Court of Appeals Decisions

1. Decisions Related to Data Collected Via Wireless

In ***Joffe v. Google***,[177] Plaintiffs filed putative class actions alleging that Google, an internet-based service provider, violated Federal Wiretap Act and state law by collecting data from unencrypted wireless local area (Wi–Fi) networks. In the course of capturing its "Street View" video for Google maps, Google's "street view" cars were equipped with sophisticated technology that not only captured video and still images, but the Google street cars also collected all unencrypted Wi-Fi data. As the Ninth Circuit described it:

> Between 2007 and 2010, Google also equipped its Street View cars with Wi–Fi antennas and software that collected data transmitted by WiFi networks in nearby homes and businesses. The equipment attached to Google's Street View cars recorded basic information about these Wi–Fi networks, including the network's name (SSID), the unique number assigned to the router transmitting the wireless signal (MAC address), the signal strength, and whether the network was encrypted. Gathering this basic data about the Wi–Fi networks used in homes and businesses enables companies such as Google to provide enhanced "location-based" services, such as those that allow mobile phone users to find nearby restaurants and attractions or receive driving directions.
>
> But the antennas and software installed in Google's Street View cars collected more than just the basic identifying information transmitted by Wi–Fi networks. They also gathered and stored "payload data" that was sent and received over unencrypted Wi–Fi connections at the moment that a Street View car was driving by. Payload data includes everything transmitted by a device connected to a Wi–Fi network, such as personal emails, usernames, passwords, videos, and documents.[178]

Google publicly apologized, but plaintiffs brought suit under federal and state law, including the Wiretap Act, 18 U.S.C. § 2511, *et seq.*. Google contended that data transmitted over a Wi–Fi network is a "radio communication" and that the Act exempts such communications by defining them as "readily accessible to the general public," 18 U.S.C. §

[177] Joffe v. Google, 729 F.3d 1262 (9th Cir. 2013), opinion amended and superseded, 2013 WL 6905957.

[178] Joffe v. Google, 729 F.3d 1262

2511(2)(g)(i), so long as "such communication is not ... scrambled or encrypted," 18 U.S.C. § 2510(16)(A). Google argues that its data collection did not violate the Act because data transmitted over a Wi–Fi network is an "electronic communication" that is "readily accessible to the general public" and exempt under the Act. 18 U.S.C. § 2511(2)(g)(i).

A federal district court in California rejected Google's argument,[179] and Google appealed to the Ninth Circuit, where it argued again that the unencrypted Wi-Fi data its street view cars collected were communications that were "readily accessible to the general public." In affirming the lower court's ruling, the Ninth Circuit ruled as follows:

> We hold that the phrase "radio communication" in 18 U.S.C. § 2510(16) excludes payload data transmitted over a Wi–Fi network. As a consequence, the definition of "readily accessible to the general public [ ] with respect to a radio communication" set forth in § 2510(16) does not apply to the exemption for an "electronic communication" that is "readily accessible to the general public" under 18 U.S.C. § 2511(2)(g)(i).

The *Joffe* case is a civil suit, and Google is a private entity not a state actor. But the message from *Joffe* is clear: in the Ninth Circuit, police that use a UAS/UAV to intercept and collect unencrypted or encrypted Wi-Fi data without a warrant are engaging in wiretapping.

2. Decisions Related to Cellular Tracking

Since the *U.S. v Jones* GPS tracking decision, courts have grappled with cellular tracking. In *U.S. v. Skinner*, the Sixth Circuit distinguished law enforcement's cellular tracking of defendant Skinner—accomplished by continuously "pinging" Skinner's cell phone—from *Jones* because there was no physical intrusion upon Skinner's personal property. Relying on *U.S. v. Knotts*,[180] the Sixth Circuit determined that Skinner did not have a reasonable expectation of privacy in inherent location data broadcast from his cell phone.

Because Skinner was traveling on public thoroughfares and stopped at a public rest stop, the court said he had no reasonable expectation of privacy.[181] Moreover, the Sixth Circuit found no difference between trailing Skinner through physical surveillance and tracking him via cellular technology. "Law enforcement tactics must be allowed to advance with technological changes, in order to prevent criminals from circumventing the justice system."[182]

---

[179] In re Google Inc. St. View Elec. Commc'n Litig., 794 F.Supp.2d 1067, 1073–84 (N.D.Cal.2011).
[180] *U.S. v. Knotts*, 460 U.S. 276 (1983).
[181] *United States v. Skinner*, 690 F.3d 772, (6th Cir. 2012) cert. denied, 12-7971, 2013 WL 3155276 (U.S. June 24, 2013).
[182] *United States v. Skinner*, 690 F.3d 772, 778 (6th Cir. 2012) cert. denied, 12-7971, 2013 WL 3155276 (U.S. June 24, 2013).

After the *Skinner* opinion was issued, Judge Ellen Huvelle of the United States District Court for the District of Columbia heard the *U.S. v. Jones* case on remand from the Supreme Court's remand of *U.S. v. Jones*.[183] While the case was before the Supreme Court, it ruled that the government's warrantless use of a GPS-tracking device was a physical search because of the physical intrusion/trespass involved in attaching the "slap-on" tracker to the car. But defendant Jones also argued that the government needed a warrant for his real-time, prospective cellphone data, which included location and time data, incoming and outgoing numbers dialed, but not content. The Supreme Court did not rule on this question, and Judge Huvelle considered this question on remand.

In her opinion, Judge Huvelle noted the unsettled state of the law with respect to cellphone location surveillance, and pointed out that, unlike the "slap-on" GPS tracker, cellphone location tracking does not involve physical trespass. Closely analyzing the events, Judge Huvelle noted in 2005 during the course of the Jones' investigation two federal magistrate judges in the District of Columbia had previously issued orders permitting the law enforcement to collect this data from the cellular provider without warrants. Thus Judge Huvelle ruled that the government reasonably relied upon this authority and the good faith exception applied to the warrantless. Under the good faith exception, law enforcement's warrantless collection of Jones' real-time cellphone data was permissible under the Stored Communications Act.

In *State v. Earls*, [184] however, New Jersey's Supreme Court took a decidedly different approach to cellular tracking. In *Earls*, police apprehended defendant Earls with the warrantless help of his cell phone provider, T-Mobile, which provided three sets of location data in one evening. The New Jersey Supreme Court unanimously ruled that, absent an exception, a warrant is required to obtain tracking information via cellular tracking data. The court's Judge Rabner noted that, while the text of the New Jersey Constitution is nearly identical to the Fourth Amendment, New Jersey provides greater protection against unreasonable searches and seizures than the Fourth Amendment.[185]

Characterizing cell phones as "an indispensable part of modern life"[186] and using language reminiscent of Justice Sotomayor's concurring opinion in *Jones*, Judge Rabner discussed why application of the third party doctrine[187] is inappropriate to cell phone tracking: "[c]ell phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not

[183] http://www.gpo.gov/fdsys/pkg/USCOURTS-dcd-1_05-cr-00386/pdf/USCOURTS-dcd-1_05-cr-00386-9.pdf
[184] *State v. Earls*, No. A-53, (Sup. Ct. N.J. July, 18 2013).
[185] *State v. Earls*, No. A-53, slip op. at 26 (Sup. Ct. N.J. July, 18 2013).
[186] *State v. Earls*, No. A-53, slip op. at 30 (Sup. Ct. N.J. July, 18 2013).
[187] The third party doctrine articulated in *Smith v. Maryland*, 442 U.S. 735 (1979) says that one does not have a reasonable expectation of privacy in information disclosed to a third party.

using a cell phone."[188] "People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with police." Even though consumers have some level of awareness that their phones can be tracked, one does not reasonably expect their precise location to be available to law enforcement without probable cause.[189]

The Tenth Circuit has addressed the constitutionality of GPS "pinging" of a suspect's cell phone to determine a suspect's location. In ***United States v. Barajas***, (10th Cir. 2013), agents prepared affidavits, which were approved to conduct wiretap surveillance on the defendant. The affidavits, however, did not include or disclose that GPS pinging would occur as to defendant's cell phone. The GPS pinging information was provided to police. The court did not decide whether pinging was a search, but pointed out that the Sixth Circuit had previously held that pinging was not a search (*Skinner)*. The court said there may not have been probable cause because the affidavit did not explain how defendant's location would reveal information about the conspiracy, but determined that the good faith exception applied. Therefore, it ruled that the GPS data was properly admitted.

One state court has taken a different approach. In ***State v. Earls***, police apprehended Earls, with the help of his cell phone provider, T-Mobile, which provided three sets of location data in one evening; a warrant was not obtained for any set of location data. The New Jersey Supreme Court held except when there is an exception, a warrant is required to obtain tracking information through the use of a cell phone. Judge Rabner wrote for a unanimous court. He first noted that while the text of the New Jersey Constitution is nearly identical to the Fourth Amendment, New Jersey provides greater protection against unreasonable searches and seizures than the Fourth Amendment.[190] The court discussed the inapplicability of the third party doctrine, reminiscent of Justice Sotomayor's concurring opinion in *Jones.*[191] "Cell phone users have no choice but to reveal certain information to their cellular provider. That is not a voluntary disclosure in a typical sense; it can only be avoided at the price of not using a cell phone."[192] The court also considered the nature of cell phones, which are now "an indispensable part of modern life."[193] "People buy cell phones to communicate with others, to use the Internet, and for a growing number of other reasons. But no one buys a cell phone to share detailed information about their whereabouts with police." Even though consumers have some level of awareness that their phones can be tracked, one does not reasonably expect their precise location to be available to law enforcement without probable cause.[194]

---

[188] *State v. Earls*, No. A-53, slip op. at 27 (Sup. Ct. N.J. July, 18 2013).
[189] *State v. Earls*, No. A-53, slip op. at 32 (Sup. Ct. N.J. July, 18 2013).
[190] *State v. Earls*, No. A-53, slip op. at 26 (Sup. Ct. N.J. July, 18 2013).
[191] The third party doctrine articulated in *Smith v. Maryland*, 442 U.S. 735 (1979) says that one does not have a reasonable expectation of privacy in information disclosed to a third party.
[192] *State v. Earls*, No. A-53, slip op. at 27 (Sup. Ct. N.J. July, 18 2013).
[193] *State v. Earls*, No. A-53, slip op. at 30 (Sup. Ct. N.J. July, 18 2013).
[194] *State v. Earls*, No. A-53, slip op. at 32 (Sup. Ct. N.J. July, 18 2013).

As the first decision of its kind, the New Jersey decision could affect state and federal court decisions when applying similar questions.

3. Decisions Related to Use of Surveillance Cameras and Videos

UAVs may easily be equipped with surveillance cameras or video recording equipment that surreptitiously capture and record still and video images that are sent back to the UAS operator. The Supreme Court aerial surveillance cases set forth above provide some framework for police in determining proper use of such electronic surveillance equipment on UAV, but lines become increasingly blurred because of the increasing sophistication of videon and audio surveillance equipment deployable via UAV. There are U.S. Court of Appeals decisions that provide some guidance in this gray area.

In ***United States v. Cuevas-Sanchez***,[195] the Fifth Circuit addressed police installation and use of a video camera installed on a utility pole (a "pole camera") overlooking a suspect's 10 foot high fenced in backyard. The officers installed the pole camera without a warrant and, using the camera, were able to observe the suspect remove drugs from the gas tanks of several cars parked in the suspect's yard. Using the evidence from the pole camera, officers obtained a warrant and arrested the defendant/suspect. At trial, the defendant moved to suppress arguing that the warrant was based on evidence obtained in violation of the Fourth Amendment, *i.e.*, the improper video search via the pole camera. The government argued that *Ciraolo* authorized this type of continuous pole camera surveillance. But the Fifth Circuit rejected this contention and found the video surveillance to be a search in violation of the Fourth Amendment. The court noted, "this was not a one-time overhead flight or a glance over the fence by a passer-by…. It does not follow that *Ciraolo* authorizes any type of surveillance whatever just because one type of minimally-intrusive aerial observation is possible."[196]

Because many UAVs, by design, can hover for extended periods of time and record video images, there is a strong analogy to the pole camera at issue in *Cuevas-Sanchez*. The prudent officer is urged to obtain a warrant when using a UAS to conduct targeted surveillance of the curtilage of a suspect's property.

In ***United States v. Wahchumwah***,[197] the Ninth Circuit considered whether an informant's use of a hidden video camera inside a home violated the Fourth Amendment. The Ninth Circuit first reviewed the core jurisprudence, stating:

---

[195] U.S. v. Cuevas-Sanchez, 821 F.2d 248 (5th Cir. 1987).
[196] 821 F.2d at 251.
[197] U.S. v. Wahchumwah, 710 F.3d 862 (9th Cir. 2012)

> "Our Fourth Amendment analysis ... ask[s] whether the individual ... has exhibited an actual expectation of privacy ... [and] whether the individual's expectation of privacy is 'one that society is prepared to recognize as reasonable.' " *Bond v. United States*,529 U.S. 334, 338, 120 S.Ct. 1462, 146 L.Ed.2d 365 (2000) (quoting *Smith v. Maryland*, 442 U.S. 735, 740, 99 S.Ct. 2577, 61 L.Ed.2d 220 (1979)). However, that expectation of privacy does not extend to "[w]hat a person knowingly exposes to the public, even in his own home or office." *Katz v. United States*, 389 U.S. 347, 351, 88 S.Ct. 507, 19 L.Ed.2d 576 (1967) (citations omitted).

The Ninth Circuit concluded in *Wahchumwah* that the invitee informant's use of a hidden spy cam in a suspect's home did not violate the Fourth Amendment. In so doing, the Ninth Circuit joins several other circuits that have reasoned that the one-party consent doctrine developed in audio monitoring cases also applies to secret video recording.

Advances in surveillance technology make it easy for an officer, via an UAV, to engage in audio and visual surveillance of activities and communications occurring inside a private home without an officer being anywhere near the home. Absent exigent circumstances, such use would be illegal and citizens should be assured that such use is deemed unacceptable by law enforcement.

C. Summary and Overview: How Will Courts Treat UAS/UAV Use, Searches and Data

In sum, when faced with questions about the legality of police use of UAS/UAV to monitor, to search, and to gather electronic data, a reviewing court will look closely at the facts of the situation. The reviewing court will attempt to apply the framework of existing electronic surveillance cases and the electronic surveillance statutory scheme set forth above to determine whether the use of the UAS/UAV was reasonable. Thus, police should consider beforehand the facts and circumstances that a reviewing court will review in making a determination as to the constitutionality of UAS/UAV usage, and that includes:

- the location of the search
- the specified purpose of the search or mission (routine or targeted)
- what surveillance technologies were utilized
  - were communications (verbal or electronic) intercepted
    - wiretapping statutes may apply
  - was GPS tracking or its equivalent conducted
    - *U.S. v. Jones*
  - were images taken
    - *Dow* line of cases
  - thermal imaging

- *Kyllo*

- the sophistication of the surveillance technology used
  - what degree of imaging capabilities were employed;
  - did the UAS/UAV engage in eavesdropping of communications;
  - did the UAS/UAV mimic a cell tower and intercept electronic communications;
  - the general availability of the technology in question, etc
- society's conception of privacy and how it would apply to the facts of the particular case.[198]

IV. CONCLUSIONS

A. Police Use of UAVs: Legally Appropriate Uses

Many of the technologies discussed above are used domestically by federal, state and local governments for a wide range of purposes and in a manner consistent with the Fourth Amendment's prohibition against unreasonable search and seizure. Federal agencies that have led the way in using such technologies include (although many scholars and attorneys hotly debate the constitutionality of certain federal agency's surveillance activities, such as the NSA): the Department of Homeland Security (DHS); the Federal Bureau of Investigation (FBI); Department of Defense (DOD); and Immigration and Customs Enforcement (ICE).

States and local police forces that routinely and appropriately employ electronic surveillance technologies include the Texas Rangers; various cities and counties in the State of Texas; various cities and counties in the State of Florida; North Dakota police; and multiple California city and county police forces. Common uses thus far—which typically do not pose constitutional and privacy concerns—include: border patrol; routine aerial patrols in rural areas (particularly effective for small offices responsible for large jurisdictions or territories); crowd surveillance; identification of vehicle via plate reader; biosurveillance; identification of individuals after criminal activities occur (Boston bomber example) and search and rescue.

Use of military UASs/UAVs by domestic law enforcement, however, raises strong constitutional concerns and arguably violates the *Posse Comitatus* Act, 18 U.S.C. § 1385, which prohibits use of military forces and equipment in domestic law enforcement.[199]

---

[198] Thompson, *CRS Drones Report* for Congress, at pg 1.

[199] Use of Army and Air Force as *posse comitatus*, 18 U.S.C. 1385, provides:
Whoever, except in cases and under circumstances expressly authorized by the Constitution or Act of Congress, willfully uses any part of the Army or the Air Force as a posse comitatus or otherwise to execute the laws shall be fined under this title or imprisoned not more than two years, or both.

B. Police Uses of UAVs that Potentially Violate the Fourth Amendment

In the absence of a warrant, use of electronic surveillance devices in a manner that would be considered to be a search under our Fourth Amendment jurisprudence is unconstitutional. There are a myriad of potential uses that would violate the Fourth Amendment. For instance, thermal imaging of buildings in public spaces may constitute a Fourth Amendment search. Listening in with acoustic enhancement to conversations that occur in public spaces but which the conversant is demonstrating a clear intent to remain private, e.g., leaning in, talking quietly or whispering, or covering mouth would likewise constitute a search.

Law enforcement employing or utilizing these devices must be familiar with and consider the Fourth Amendment principles BEFORE deploying such devices in any mission.

C. Uniform Policy and Procedure Guidelines

Advancing and emerging technologies that permit non-intrusive yet comprehensive data-gathering are here to stay. Policy, procedure and use guidelines for domestic law enforcement must consider the existing Fourth Amendment jurisprudence and provide working legal guidelines for officers when using such technologies.

By drafting uniform policy, procedure and use guidelines for domestic law enforcement in the use of such technology, domestic law enforcement can help avoid a legislative showdown, allay public fears of a "big brother" state, and help shape legislation that insures preservation of civil liberties while equipping police with Fourth Amendment compliant use of efficient, cost-effective surveillance technology.

Proactive and uniform policies with respect to: data collection, data processing, data retention, and data sharing with various federal, state and local law enforcement agencies, will reduce liability from improper data usage, improve cooperative law enforcement efforts, protect civil liberties and help shape regulation of the same. Legal Memo 3 addresses uniform data practices.