Domestic Drones: Technical and Policy Issues

University of Washington Technology and Public Policy Clinic

Follow this and additional works at: https://digitalcommons.law.uw.edu/techclinic
Part of the Privacy Law Commons, and the Science and Technology Law Commons

Recommended Citation
Available at: https://digitalcommons.law.uw.edu/techclinic/1
Introduction: What are “Domestic Drones”?

Domestic unmanned aerial vehicles (UAVs”) or “drones” are not the drones most commonly associated with tracking and killing targets in overseas operations. Domestic UAVs are autonomous aerial vehicles that are equipped with cameras or other sensors in order to collect assorted data from an aerial vantage point. UAVs have been used for a number of years by hobbyists and other aircraft enthusiasts, but are only recently seeing more widespread use as a result of the Federal Aviation Administration now making available preliminary licenses for law enforcement and other government agencies to make use of domestic UAVs.¹

Domestic drones vary widely in their capabilities and uses, from small, semi-autonomous, rotorcraft that cost around $1,000² up to large, fully-autonomous, fixed wing type aircraft that can cost upwards of $1,000,000.³ While the capabilities and sophistication of drones are not all equal, the basic functions and purpose of domestic drones are all the same, namely to gather information and data from an aerial vantage that can be used by operators on the ground.

Domestic drones have seen use in a number of different fields, including hobbyists, commercial and industrial, agricultural, safety and law enforcement. This paper seeks to address the technical and policy issues specifically surrounding the use of drones in law enforcement.

¹ FAA Modernization and Reform Act of 2012, P.L. 112-95
² See http://diydrones.com/
³ See Boeing Insitu ScanEagle
Figure 1 Photo From a DraganFlyer X6
**Technical**

**Flight Capabilities**

All drones are built to fly through remotes, GPS and other sensors from operators on the ground. Because the drones are not built to hold a human pilot in cockpit, they can be very small and light weight, significantly reducing the cost of operation. However, domestic drones frequently operate on batteries, which can limit their airtime; some have flight times as short as 15 minutes, while others are capable of staying aloft for 12 or more hours.\(^4\)

The autonomy of domestic drones during flight ranges from merely being able to take off and land on their own, with human control over in flight actions and movements\(^5\) to complete autonomous movement in more expensive systems. Drones are generally connected to ground bases which are often handheld computers, allowing an operator to observe the drone’s flight patterns and data gathering through a display screen on the ground connected to a camera or cameras on the drone. This allows an operator to maintain control over the drone in flight even if it leaves the line of sight of the operator, ensuring that the drone does not become lost or crash in the event that it goes off course.

Although many drones are intended to be flown only while in line of sight, the distance that they are capable of flying can still be significant. Although some cheaper models may only go several hundred feet, other more expensive models are capable of flights of 10 or more miles from the base station.\(^6\)

Although all of the drones examined have extremely varying capabilities in flight, the drones that are generally being sought for domestic use by law enforcement fall on the low end of the spectrum for all categories. This is partially because of FAA regulations regarding line of

---


\(^5\) DraganFlyer X6

\(^6\) MLB Superbat
sight use for law enforcement, and partially because of cost considerations in choosing drones for a domestic municipal program.

![Figure 2 MLB Super Bat](image)

**Capabilities of Cameras on Surveillance Drones:**

The sophistication of the camera attachments that can be attached to a domestic surveillance drone depends on the payload capacity of the particular vehicle model in question. That said, camera technology is becoming increasingly lightweight and advanced features are being integrated that make specific object tracking, nighttime recording, and infrared surveillance possible. As an example, this overview will cover the technical capabilities of TASE gimbals, which are stabilized camera systems developed and produced by Cloud Cap Technology, Inc. The Company serves multiple leading aircraft manufacturers including: BAE Systems, Lockheed Martin, Boeing, UAV Solutions, Raytheon, General Dynamics, Griffon Aerospace, and NASA. There are three levels of camera gimbals available from Cloud Cap. On

---

7 Cloud Cap Technology, Inc. is a Hood River, OR based subsidiary of UTC Aerospace Systems. This company produces integrated autopilots, payloads, and sensors for various types of unmanned vehicles. The products sold by this company are used for general representative purposes and should not be considered exclusively representative of the types of features available to local law enforcement agencies interested in surveillance drones. It is important to note, however, the company’s Pacific Northwest roots when considering the economic impact of drone and component acquisition.
the entry level end of the spectrum is the TASE 150. On the high-end is the TASE 400. All of these gimbals can be controlled with the company’s ViewPoint software.

**Technical Specifications for TASE 150:**

The TASE 150 is a small gimbal mounted camera that weighs 1.98 pounds in a 5-inch package. The camera used by this system is a Sony FCB-EX 1020, which has a 36X optical zoom lens and has 380k pixels image resolution. The camera is capable of functioning in temperature ranging from -20 degrees Celsius to 70 degrees Celsius. To operate the camera requires 10 Watts of power. Low-wave infrared capabilities can be installed even on this low-weight basic camera system, which would provide an ability to track at night. Also, it is possible to mount a laser range pointer that would enable this unit to track the speed and distance of surveyed objects. The gimbal comes with a sealed camera enclosure.

![Figure 3 Tase 150 Gimbal](image)

**Technical Specifications for TASE 400:**

The TASE 400 is a significantly heavier and larger unit capable of sophisticated surveillance. Weighing 7.5 pounds in a 7-inch package, this gimbal and camera system would need a more robust aerial vehicle capable of handling the increased payload. Though the basic
camera has the exact same specifications as the TASE 150, it is supplemented with a mid-wave infrared system that provides more significant surveillance capabilities. This type of thermal camera allows for both nighttime imaging as well as surveillance through fog, haze, smoke, and clouds during daytime. The TASE 400 also comes equipped with a laser range pointer, which allows the unit to determine the distance, speed, and trajectory of objects on the ground. At 40 Watts, this advanced unit requires significantly more power than its sibling and can be operated in temperature conditions ranging from -20 degrees Celsius to 60 degrees Celsius. The gimbal is sealed and is fully rain and dust proof.

**ViewPoint Software Details:**

ViewPoint is the ground based control software that displays video feeds from the surveillance drone and allows users to control and command the TASE series gimbals. The software is sophisticated and allows for (1) the camera to be controlled via joystick, (2) real-time image mosaic (picture-in-picture from camera, infrared camera, and laser range tracker); (3) geographic stamping that will automatically orient the camera to the selected object on a map; (4) object tracking; and (5) path tracking. Between the software and the actual physical units, the surveillance possibilities are quite sophisticated and allow for the tracking of people and objects in a variety of different environments.

**Training for Drone Flight:**

The amount of training required to pilot surveillance drone systems depends on the individual manufacturers, which often include a training program with the purchase of the
vehicle. Currently, there are no FAA guidelines as to what kind of training is required for drone flight, but experts expect that some sort of graduated licensing system will be eventually implemented for different types of aerial vehicles.\textsuperscript{8} Some institutions of higher learning, however, have begun to offer courses for drone operation. For example, the University of North Dakota has begun to offer both degree and certificate programs in drone operation. Community colleges and other institutions have also either considered or begun training programs. Schools plan to teach students about the operation of drones and are also offering courses on the drone regulatory environment. Generally, these programs start with extensive time in simulators before more advanced classes move on to flight.\textsuperscript{9} Additionally, online degree programs have sprung up. Notably, Unmanned Vehicle University now offers a Master Degree in Engineering for drone flight.\textsuperscript{10} This program is completed over two years in eight consecutive quarters. Tuition is set at $1600 per quarter and a bachelor’s degree in math, science, or engineering is required as a prerequisite.


\textsuperscript{10} See generally http://www.uxvuniversity.com/ for details on the degree offerings.
Legal & Policy

UAS Usage and Certification

There are two ways to obtain the Federal Aviation Administration (FAA) certification necessary to operate an Unmanned Aircraft System (UAS). Private sector (civil) operators are granted an “experimental airworthiness certificate” to do research and development, flight demonstrations, and training. Public sector (public) operators are granted a Certificate of Authorization (COA), usually for the purpose of law enforcement, firefighting, border patrol, disaster relief, military training, search and rescue, and other governmental operational missions. UAS are prohibited from routinely operating over densely populated areas.

Applicants for COAs request authorization online with operation proposals. The FAA then evaluates these proposals to determine whether the operation can be conducted safely. The COA defines the blocks of airspace that operators can use and includes special provisions unique to each proposed operation. COAs are issued for specific periods of time, often up to two years. An authorization usually requires coordination with an air traffic control facility and may require a transponder on the UAS depending on the airspace it will occupy. When the UAS operates outside airspace restricted from other users, a visual observer or “chase plane” is required to maintain visual contact with the UAS.

The proposed purposes for UAS are usually public in nature such as law enforcement, firefighting, border patrol, disaster relief, search and rescue, military training, and other government operational missions. Private sector uses for UAS involve research and development, training, and flight demonstrations. As of February 15, 2013, there are 327 active COAs.11

Organizations Applying for FAA Approval to operate UAS

There are many organizations, both private and public, that have applied to the FAA for approval to operate UAS. The proposed uses vary, but mainly involve government operational missions for the public sector COAs, or research and development for the “experimental” certifications granted to private sector groups.


The public organizations that have submitted proposals to the FAA include the Departments of Agriculture, Commerce, Defense, Energy, Homeland Security, Interior, and Justice; NASA; state universities including Texas State, Texas A&M, Kansas State, Mississippi State, University of Alaska, University of Colorado, Utah State; Federal/State law enforcement; and state National Guard offices from California, Illinois, Iowa, Louisiana, Michigan, Minnesota, New Mexico, Ohio, Texas, and Oregon.

---

12 https://www.eff.org/sites/default/files/filenode/20120416_FAADrones COA 0.pdf
13 https://www.eff.org/deeplinks/2013/02/faareleases-new-list-drone-authorizations-your-local-law-enforcement-agency-map;
15 https://www.eff.org/sites/default/files/filenode/20120416_FAADrones SAC.pdf
Current UAS Legislation

There are UAS Test Site Proposals in 24 States. All applications were by public organizations, which are permitted to have private companies operate as part of their teams. Of the 24 states where Test Sites have been proposed, 16 have introduced legislation related to the regulation of UAS, with 8 of those states having UAS-related bills which are dead as of this writing or having nothing introduced at all. California, Georgia, Maryland, Minnesota, Michigan, Nevada, North Carolina, and New York have all introduced UAS-related legislation. Alabama, Arizona, Missouri, and Texas have had UAS-related legislation successfully pass at least one legislative committee. Alaska adopted a resolution creating a task force charged with recommending UAS policy and legislation. Florida, Idaho, Montana, and Virginia have all enacted legislation that will go into effect in 2013. North Dakota, Oklahoma, Washington, and Wyoming have all introduced UAS legislation which did not become law. Only Utah, Ohio, and Mississippi have not introduced any UAS-related legislation yet.

Examples of Unmanned Aircraft Systems

UAS that have been proposed to the FAA for operation include the ALTAIR UPB97010-1, GMAV, COBRA, UPA97000-32, SKYBUS (30K), PREDATOR B UHK97000-10, SHADOW 200B, UWA-97000-1, UHK97000-10, SANDSTORM, VIKING 100, POLAR 400, GOLDENYE 50, KESTREL-T, TR 918, UPA 97000-30, and the CYBER BUG "B." Another popular type with several models, one of which was purchased by the Seattle Police Department, is the Draganflyer UAS.

---

16 http://www.faa.gov/about/initiatives/uas/media/UAS_testsite_map.pdf
18 https://www.eff.org/deeplinks/2013/02/just-how-many-drone-licenses-has-faa-really-issued
The State of Washington Aircraft Laws

Washington’s Revised Code deals with some state issues regarding aircraft operating within the state. However, since the FAA has oversight of all US airspace and regulations, the Washington laws are relatively simple and limited in their overall impact. RCW Title 14 deals with aeronautics generally though Chapter 16 specifically dealing with aircraft and flight regulations. RCW 14.16 requires all pilots or aircraft owners be in compliance with FAA rules and be licensed under the FAA in order to operate in Washington. This state’s laws and regulations simply require that all safety and other requirement of the FAA be followed at all times, leaving relatively little room for unique requirements pursuant to state laws with respect to drone rules and regulations.

Most recently, however, a piece of legislation was proposed to Washington’s state legislative body in order to provide guidance on domestic drone usage, particularly with respect to privacy. House Bill 1771 would have required: warrants for the majority of surveillance conducted through domestic drone use; regulated when drones could be used, and regulated the storage of data captured in this manner. However, despite partisan support for the bill, an effort led by Boeing Company lobbyists ultimately resulted in a rejection of the bill.20

Privacy

The preamble of the Washington State Constitution expressly recognizes the right to privacy. Further, the Fourth Amendment of the U.S. Constitution (“Fourth Amendment”), which guards against unreasonable searches and seizures, applies to Washington State through

19 https://www.eff.org/deeplinks/2012/04/faa-releases-its-list-drone-certificates-leaves-many-questions-unanswered
the due process clause of the Fourteenth Amendment. Article I Section 7 of the Washington State Constitution is the state counterpart to the Fourth Amendment. Generally, the Washington State Constitution has higher standards than the Fourth Amendment against unreasonable searches and seizures.

The Fourth Amendment requires that a warrant is sanctioned by a judge for a search. In order for the warrant to be valid, it must be supported by probable cause. However, for the Fourth Amendment to apply, the act must be considered a search. Under the Fourth Amendment, a search occurs when a state agent physically intrudes on a constitutionally protected area in order to obtain information or the agent’s search of a constitutionally protected area violates an individual’s reasonable and subjective expectation of privacy. However, the Fourth Amendment protects individuals only against actions by publicly paid police officers or officials. Actions by private citizens are not within the scope of this federal protection.

**The Fourth Amendment and Drone use by Public Actors**

Public actors (those acting on behalf of a government body and thus subject to regulation under the United States Constitution), including private citizens acting under the instruction of a public actor, must follow the Fourth Amendment requirements if they are engaged in a search. The use of drones by public actors raises serious questions about the reasonable search requirement. Drones are capable of amassing large amounts of data. They can be equipped with various functions including live-feed video, infrared cameras, heat sensors, and radar. Some of the newer drones are capable of capturing images on super high resolution cameras that can track people and vehicles from high altitudes. Some drones can even eavesdrop on electronic transmissions and crack Wi-Fi networks and intercept text messages and cell phone
conversations. Yet a public actor may be able to argue that the use of a drone does not constitute a search because the actor did not physically intrude on a constitutionally protected area or that the individual did not have an expectation of privacy.

**Home**

The question of privacy within the home becomes murky when we consider the use of powerful technology. The general notion is that whatever is in plain view does not enjoy a right to privacy. For example, if an illegal marijuana supplier grows their plants in front of their window overlooking the street, the grower can be arrested without a search warrant. But with the advancement of technology, drones will be equipped with high powered cameras, thermal imaging, and the capacity to see through walls. If a drone can ‘see’ marijuana growing through reflective tinted windows, was the the marijuana in plain view? Is there a right to privacy? At the moment the general rule is if law enforcement uses technology that is not available to the general public, it must need a warrant for the search. This leaves open the assumption that a drone can use unsophisticated technology to view people and objects in plain view without triggering a Fourth Amendment violation. With the rapid advancement of technology, this entire area of law remains undefined.

**Yards**

Moving beyond the home to the immediately surrounding area, it is unclear what the permissible circumstances for surveillance are. The Fourth Amendment offers less robust restrictions upon government surveillance in areas such as the backyard, swimming pool, deck or porch. While the Supreme Court has reiterated multiple times that the private property around a

---

home receives the same privacy protections as inside the home, their rulings on aerial surveillance cases point otherwise. In *California v. Ciraolo*, the Court found no Fourth Amendment violation when police flew over a house in an airplane to see marijuana plants growing in the backyard when the fence around the yard was too high to see in.\(^\text{22}\) Similarly, in *Florida v. Riley*, when police could not see the contents of a greenhouse over a tall fence, they flew over the backyard at a height of 400 feet and saw marijuana plants growing through a crack in the greenhouse roof.\(^\text{23}\) The Court did not consider this a search for which a warrant was required, and remarked that this helicopter surveillance did not violate the Fourth Amendment because the plane was at all times in navigable airspace. These two cases erode the privacy that individuals enjoy in their own yard. In a world with surveillance drones, it may be that these aerial surveillance cases will be upheld, or reexamined in favor of stronger privacy restrictions in consideration of drones and their current and potential uses.

**Public Areas**

In public areas outside of the home such as open fields or city streets, there is generally no expectation of privacy. Surveillance in public areas with current technology such as helicopters or cameras is not considered a search in relation to the Fourth Amendment. We can expect this to remain the same with the introduction of domestic drones. But although public surveillance is not considered a search, pervasive tracking may go too far: Take, for instance, the Supreme Court’s recent decision in the GPS tracking case *United States v. Jones*, 132 S. Ct. 945 (2012). In the *Jones* case, the Court held that the attachment and month long tracking of a GPS device on an individual’s vehicle constituted a trespass, and hence a Fourth Amendment

---

\(^{22}\) *California v. Ciraolo*, 476 U.S. 207 (1986)

search. *Id.* The Court grounded its decision in the property-based approach to assessing what constitutes a “search” under the Fourth Amendment, which had been more prevalent in the late 19th and early 20th century cases involving relatively unsophisticated technology.

The court’s focus on whether long term tracking violates Fourth Amendment protections is very applicable to domestic drones. But the concurring opinion may have even more far-reaching implications for domestic drones:

Justice Alito, concurring in the Court’s judgment, and joined by Justices Ginsburg, Breyer, and Kagan, would have held that “the use of longer term GPS monitoring in investigations of most offenses impinges on expectations of privacy. For such offenses, society’s expectation has been that law enforcement agents and others would not—and indeed, in the main, simply could not—secretly monitor and catalog every single movement of an individual’s car for a very long period.”

Drones will certainly bring into question the ability to continuously track individuals. Tracking, along with the expectations of privacy in and around our house will hopefully be reexamined as domestic drones find their way into the skies across the country.

**Publicity rights**

Every individual has a property right to their likeness, including their name, voice, signature, and faceprint - this is called the right of publicity. Drones conducting surveillance on the public will have an expanded ability to collect people’s likenesses; they can fly for longer

---

durations and can reach areas not currently accessible by traditional aircraft. The interest of protecting people’s private identity from intrusive drone surveillance must be weighed against the society’s concern for the free flow of information. The free flow of information and the ability to gather ideas is protected by the First Amendment of the United States Constitution (First Amendment), which grants freedom of the press and other forms of expression. Challenges arise in attempting to find the appropriate balance between newsgathering and privacy interests, and the courts have been divided on the issue. Some courts have ruled that it is not a privacy invasion to surreptitiously record someone, while others have ruled that an individual should not expect to be photographed or recorded while talking with a visitor in their own house. What is clear is that publishers have no special immunity from privacy laws. This issue has arisen with paparazzi photographers, in which courts have stated that “crimes and torts committed in newsgathering are not protected. There is no threat to a free press in requiring its agents to act within the law.” At the moment drone operators will be expected to follow state and local publicity laws, but it is unclear how they will act as a catalyst to shift these policies.

**Criminal Investigations**

When a drone is used by law enforcement to gather evidence for a criminal investigation, the evidence is generally considered public unless the case is active. Information that is gathered by a drone for an ongoing criminal investigation may not be open to the public under many states’ ongoing criminal investigation constraints. The purpose of not making this information public is to prevent the disclosure of information that can impede the investigation or allow a suspect to avoid apprehension. For example, if a drone collects video footage of a suspect’s car

---

25 H.R. 6676, 112th Cong. 2d Sess. (2012), and Dietemann v. Time, Inc., 449 F.2d 245 (9th Cir. 1971), respectively
26 Galella v. Onassis, 487 F.2d 986, 991-92 (2d Cir. 1973)
fleeing through your neighborhood, you will not be able to view the footage in order to see if your rooftop sunbathing was caught in the footage. Only after the criminal investigation is closed can the public request to view the footage.

Private Actors

Although the Fourth Amendment and Article I Section 7 of the Washington Constitution do not protect individuals from searches by a private party, individuals are still afforded some protection. Washington State provides civil and criminal penalties for violations of privacy by private actors for trespass, stalking, harassment, public disclosure of private information, among others. Businesses and private individuals would most likely be allowed to use drones to monitor the interior and exterior of their premises or residence much like CCTV (closed circuit television camera) cameras but the surveillance of places with an expectation of privacy such as bathrooms and changing rooms would not be allowed. The recording of audio along with video is generally not allowed. In most cases, consent by the party being recorded is needed if audio is being recorded.

Other Surveillance Devices in Washington State

Washington State has dealt with other surveillance issues such as video surveillance, dashboard cameras on patrol cars, and red light cameras. Red light cameras are the most limited. Currently, the images captured on red light cameras can only be used to determine red light infractions. However, there has been pressure on the legislature of this state to change the laws so that images captured by red light cameras would be allowed in other criminal investigations.
Regarding the use of surveillance cameras and dashboard cameras by the police, Washington State allows the use of such devices to prevent, detect, and deter crime. Dashboard cameras record both audio and video while most surveillance cameras only record video. The footage can be used as evidence for any crime they capture. Like cameras used by private actors, the footage cannot violate an individual’s expectation of privacy. They are primarily used in public places, which greatly diminishes an individual’s expectation of privacy. A current issue with dashboard cameras on police vehicles is that the police department is allowed to destroy the videos before the public can gain access to the footage. Although there are few legislative limits for the use of cameras by the police, protests by the public have deterred some use. For example, an expansive surveillance project along the Seattle waterfront has been delayed because of privacy concerns by residents. The plan to use drones by the police department was also cancelled because of public outcry.

State Survey on Domestic Surveillance Drones

This year many state legislatures and other governmental entities have begun to propose and enact legislation concerning the deployment of domestic surveillance drones by local law enforcement and other governmental entities. Legislation has been proposed in 41 states with legislation still active in 28 of those and with 5 states already passing some sort of regulatory laws. In terms of general trends, almost all states are passing bills requiring law enforcement agencies to obtain a probable cause warrant before employing a surveillance drone in an investigation. This includes the bills introduced in Arizona, California, Florida, Georgia, Idaho, Illinois, Kentucky, Maryland, Massachusetts, Minnesota, Missouri, Montana, New Hampshire, New Mexico, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee,
Texas, Washington, and Wyoming. Many are also calling for a temporary moratorium to allow for information gathering and well thought out regulation before drones are introduced for use. This seems to be an extremely active area of legislation and no doubt there will be more developments in the very near future.

There are other commonly recurring themes to enacted and proposed laws. Some legislation has sought to ban the “weaponization” of domestic drones. Others have required law enforcement agencies to report their drone usage to the legislature to ensure that elected officials are aware of how drones are actually being used. In a similar vein, certain proposed laws would make law enforcement agencies justify the necessity of purchasing an aerial drone to the local governing body before purchase. In Georgia, the bill only allows drones to investigate felonies, not misdemeanors.

In terms of laws focusing on the protection of privacy rights, Massachusetts and Rhode Island can be considered leaders. Both states have prohibited law enforcement from identifying anyone but the specific target of the drone’s use in the footage and have explicitly disallowed any data incidentally collected from being admissible in court. Furthermore, Rhode Island mandates that any incidentally collected data be deleted within 24 hours. Massachusetts, on the other hand, has explicitly forbidden the surveillance based only an individual’s protected First Amendment right (e.g. demonstration, religious ceremony, etc.).

Some states, like Montana, have prohibited private use of drones. Oregon has a proposed statute that would prohibit anyone from using domestic drones without express permission from

27 See proposed or enacted legislation in Georgia, Illinois, Massachusetts, Montana, New Hampshire, Oklahoma, and North Dakota.
28 See proposed or enacted legislation in Hawaii, Illinois, Maine, Massachusetts, Rhode Island, and Washington.
29 See proposed or enacted legislation in California, Hawaii, Maine, Oregon, Rhode Island, South Carolina, and Washington.
the individual whose property is being surveilled. In the most extreme, privacy protection cases, proposed legislation would ban all use of drones for evidence collection. States exploring this policy include Montana, Nebraska, and Virginia (for a period of two years).

Finally, there are jurisdictions taking more independent approaches. Indiana has passed a resolution that will create a committee to study drone use. California has a bill that would provide tax breaks for drone manufacturers. There are many different considerations that legislatures need to take into account in regulating domestic drone usage. By the time the Washington legislature takes up the issue again, there should be plenty of precedent on which to lean on. It would be wise to monitor the regulatory and incentive landscape closely. The Technology Law and Public Policy Clinic at the University of Washington School of Law would be glad to undertake this task.