The Basics

Drone Law for Defense Lawyers

By Caroline Gentry

Although drone law is in its infancy, governmental entities and businesses operate in industries that use drones. Knowing something about that law may be more pertinent to your practice than you think.

First, congratulations for reading this far. If you are like most defense lawyers, your initial thought on reading the title of this article was: "This isn't written for me, because I don't need to know about drones or drone law." Are you sure? Read a little further, and you might be surprised.

Our clients' problems are our problems, and drones are likely to affect your clients more than you think. If you represent governmental entities or businesses that operate in any of the industries that use drones—including energy, insurance, construction, infrastructure, real estate, agriculture, security, law enforcement, first responders, transportation, or logistics—or if you defend negligence, other tort, or product liability claims, then you may need to know something about drone law.

What is drone law? People often think of federal drone laws and regulations, but they are just a part (albeit an important part) of drone law. Drone law also includes state and local laws and regulations, as well as property, insurance, tort, product liability, criminal, privacy, national security, and constitutional laws. Some laws are drone specific, but many of them are not.

Drone law is still in the early stages of its development. Our legal training teaches us to create new rules based on existing rules, but that only goes so far with unique technologies such as drones. For example, who owns the air? The ancient rule was *cuius est solum, eius est usque ad coelum et ad inferos* ("whoever's is the soil, it is theirs all the way to Heaven and all the way to Hell"). But after the Wright Brothers invented flight, Congress decreed that the United States had exclusive sovereignty of the airspace (*see* 49 U.S.C. §40103(a)(1)), and the Supreme Court declared, "The air is a public highway." *U.S. v. Causby*, 328 U.S. 256, 261 (1946). In a short period of time, private property rights yielded to the public's right to use the airspace.

As a result, we agree that airplanes do not trespass when they fly over our property. But what if a drone (which is legally considered to be an aircraft) flies over your client's property at an altitude of 400 feet? What if it flies at a lower altitude, perhaps fifty or one hundred feet? Does it matter if the drone maintains a safe altitude above the top of the highest structure on the property? Does it matter if the drone can be seen easily? Does it matter if the drone does not fly at a constant speed, but instead, slows down or even hovers? Does the purpose of the flight matter, e.g., is the drone simply in transit, or is it surreptitiously recording

■ Caroline Gentry is a litigation partner in the Dayton, Ohio, office of Porter Wright Morris & Arthur LLP. She practices in the areas of commercial litigation, class action defense, ERISA litigation, telecommunications law, and drone law.

data about the property or its owners? Reasonable people can disagree—and these are just a few of many legal issues to be decided.

There is also vigorous disagreement about the proper roles of federal, state, and local governments in the regulation of drones. We readily accept federal regulation of aviation, but when a drone hovers outside your window, you will probably call the local police and not the Federal Aviation Administration (FAA). One approach would divide each government's jurisdiction by altitude (e.g., federal regulation of higher altitudes versus state and local regulation of lower altitudes). Another approach would divide each government's jurisdiction by issue (e.g., state or local regulation of crimes, torts, etc. versus federal regulation of airspace, pilots, airworthiness, and maintenance, etc.). Numerous state and local governments have not waited for a consensus, but instead have enacted a myriad of drone-specific laws. The result is a disorganized mess that creates uncertainty for businesses and pilots who need to know which laws apply.

This article does not try to answer (or even ask) all of the relevant questions. Instead, its goal is threefold: 1) to provide a brief explanation of drone technology and describe the legal issues that drones may create for your clients and your practice; 2) to provide an overview of the federal regulatory framework for drones; and 3) to describe trends in drone-specific state laws. Drone law will keep evolving, of course, so stay tuned.

Drone Technology and the Resulting Legal Issues

It is helpful to know something about drones when thinking about how they will affect your legal practice. "Drone" is a colloquial term for an unmanned aerial vehicle (UAV), which is a component of an unmanned aerial system (UAS). Every UAS has six components: 1) the human operator or operators; 2) the payload or sensor; 3) the command and control function; 4) the communication links; 5) the UAV; and 6) the launch and recovery mechanisms. Each component comes with its own unique technological and legal issues.

Human Operators

Every remote flight crew must have one pilot in command. The crew can consist of just the pilot in command, or it can include additional pilots, sensor operators, and visual observers. As in manned aviation, the remote flight crew must use principles of crew resource management and manage common human-factor risks, such as fatigue and overreliance on automation. The remote flight crew must also handle unique challenges posed by drones, including a lack of situational awareness and a lack of direct control over the UAV. The pilot in command must conduct preflight and post-flight checks, confirm that the weather allows the mission to be flown safely, be thoroughly familiar with the terrain and any obstacles, and ensure that all applicable rules are being followed. Safety is always the paramount concern. As with manned aviation, human error will always be a possible cause of a UAV crash.

Payload/Sensor

Think of the payload as the way that a remote pilot gets "paid." Simply put, the payload is the reason why businesses fly drones. The payload may be a physical object that is delivered, such as a pizza or an Amazon package. Or the payload may be a physical object that provides a service, such as an ultraviolet light used to disinfect health-care facilities, or a radio-frequency identification (RFID) scanner used to conduct inventories.

Most commonly, however, the payload is a remote sensor that collects information that has a tangible value. Remote sensors fall into two categories: passive and active. Passive sensors rely on existing electromagnetic radiation that is emitted from the sun or reflected from an object of interest, including people, plants, rocks, and animals. A basic passive sensor is an electro-optical sensor that takes pictures and records video; many cameras fit this bill. Infrared or thermal sensors detect heat and can identify pipeline leaks or find missing persons at night. Hyperspectral sensors can identify specific objects, such as which minerals exist in a rock.

Active sensors do not rely on existing electromagnetic radiation; instead they actively send some form of energy toward an object and then measure the reflected or backscattered energy. For example, a light detection and ranging sensor (LiDAR) sends a laser pulse toward the target and measures the energy that is returned. LiDAR creates extremely precise, three-dimensional images and has many applications, including accident reconstructions, as-built drawings, high-resolution maps, elevation values, volumetric calculations, infrastructure planning, environmental assessments, mining operations, archeological digs, and automated vehicles.

There is also vigorous disagreement about the proper roles of federal, state, and local governments in the regulation of drones. We readily accept federal regulation of aviation, but when a drone hovers outside your window, you will probably call the local police and not the Federal Aviation Administration (FAA).

The potential commercial applications for remote sensors are exciting, wide-ranging, and constantly changing. They are also beyond the scope of this article, so I encourage you to research how your clients and their industries are using remote sensors. Legal issues that arise from remote sensors include invasion of privacy, theft of trade secrets, violations of the Fourth Amendment, negligence, and securing confidential client data.

Command and Control

A control station enables the remote pilot to program and revise automated flight routes and to control the UAV manually during launch, flight, and recovery. Simple missions can use a small control station, such as an iPhone or a handheld controller that

resembles a video game controller. More complex missions might require a larger control station, such as a laptop computer or a multimonitor ground control station. A sensor operator may need to review real-time data on a separate monitor as the UAV collects it. The sensor operator can detect and correct any problems with the data collection and request a change in the flight path to collect additional data, as necessary. Command and control functions create points of failure that may be relevant to negligence and product liability claims.

Many legal issues will arise from the design, manufacture, and operation of the UAV itself.

Communication Links

Without a pilot onboard the aircraft, it is critical to maintain the communication links between the control station and the UAV at all times. The remote pilot must continually be able to send commands to the UAV. The UAV must continually be able to transmit information to ground control about its status and any problems. The sensor may be required to transmit real-time data to ground control. Finally, the UAV must have a constant communication link with GPS satellites to know its location relative to the Earth's surface. When the GPS signal is interrupted—which can happen for several reasons—the resulting "lost link" may cause the UAV to hover in place, land in a prearranged location (also known as the "return to home" feature), or in a worst-case scenario, to crash. The communication-links component creates points of failure that may be relevant to negligence and product liability claims.

UAV

UAVs come in three sizes: small (under 55 lbs.), medium, and large. The FAA allows small UAVs to be flown pursuant to certain regulations, but requires operators to get special permission before flying medium and large UAVs. Small UAVs are typically battery powered, but some can be powered by different types of engines. UAVs can be fixed wing (as in airplanes), or rotorcraft (as in helicopters). Fixed-wing UAVs are aerodynamically efficient, have longer flight times, and are well-suited for missions flown over large areas, such as farms or power lines. Rotorcraft UAVs are less aerodynamic and have shorter flight times but are able to hover, so they are well suited for missions such as infrastructure inspections and to create as-built drawings.

Many legal issues will arise from the design, manufacture, and operation of the UAV itself. UAVs have several unique attributes that will likely contribute to these issues.

- Heavy UAVs burn through power faster, thereby shortening their flight times; small UAVs are designed to weigh as little as possible so they can stay in the air longer. The need to have a lightweight aircraft means that small UAVs, unlike manned aircraft, lack redundant systems that ensure safety. The lack of redundant critical systems means that a single point of failure could lead to the loss of the aircraft and damage on the ground. The FAA is considering whether to require redundancy of critical UAS systems, but there is currently no such requirement.
- Unlike manned aircraft, UAVs are heavily dependent on the proper functioning of automated flight programming and the GPS communication link. Any error or mishap, such as a faulty line of code or a lost-link signal in a congested urban area, could result in the loss of the aircraft and damage on the ground.
- Current rules require UAVs to be flown within the pilot's line of sight. However, many commercial UAV flights will need to take place beyond visual line of sight (BVLOS) to be useful and cost-efficient. Such BVLOS flights will need to rely on sense-and-avoid technology to avoid collisions with structures and other aircraft. This technology will create yet another point of failure.
- Unless appropriate security measures are put in place, it can be possible to hijack and assume control of another pilot's UAV, or to steal confidential client data that the UAV has collected. A bad actor who hijacks a UAV can deliberately crash it and cause damage on the ground.

In sum, many technological failures can cause UAVs to crash and cause damage on the ground. These technological failures exist alongside a number of other potential causes, including human error, bad weather, faulty design or manufacturing, and bird strikes (yes, these have happened). Identifying the causes of a UAV crash, determining liability, and awarding damages will become increasingly common parts of negligence and product liability lawsuits.

Launch and Recovery

The final component of a UAS describes the mechanisms that allow a particular UAV to take off and land. Unlike manned aircraft and larger UAVs, most small UAVs do not require long permanent runways. Small, fixed-wing UAVs can be launched by hand (literally, thrown into the air); by slingshot; off a car rooftop; or off a short, makeshift runway. They can be recovered by belly-landing onto a makeshift runway, or by being caught by a net or other device. Rotorcraft UAVs are able to land and take off vertically. Legal issues relating to launch and recovery operations include trespass, negligence, and product liability.

Overview of the Federal Regulatory Framework

The federal regulatory framework for drones has developed over a relatively short period of time, primarily during the last eight years. Although substantial progress has been made, a significant number of technological and legal issues remain to be addressed.

The FAA established its Unmanned Aircraft Program Office in February 2006. Before that date, and for several years after, the FAA granted applicants permission to fly UAS under specific conditions. Although the FAA issued many such certificates of authorization and certificates of waiver, the application process was laborious and time-consuming. Progress toward establishing a comprehensive regulatory framework was incremental at best.

In the 2012 FAA Modernization Act, Congress ordered the U.S. Department of Transportation (DOT) and the FAA

to speed things up. The department was required to develop, within 270 days, a comprehensive plan to accelerate the integration of civil UAS safely into the National Airspace (NAS). Congress ordered the DOT to define acceptable standards for operation and certification of UAS, including requirements for remote pilots and sense-and-avoid capabilities. The FAA was required to carry out all necessary safety studies to support integration of UAS. In a nod to model airplane owners, Congress forbade the FAA from issuing regulations regarding small model aircraft flown strictly for hobby or recreational use. The FAA was still permitted, however, to regulate hobbyist use of UAS to the extent that it endangered the safety of the NAS.

In 2015, the FAA proposed new rules that would authorize flights of commercial small UAS under specific conditions. Operators were permitted to request an FAA waiver of certain conditions if they showed that they could operate safely. After reviewing more than 4,000 public comments on the proposed rules, the FAA published the final rules in 14 C.F.R. 107 (referred to as "Part 107"), with an effective date of August 29, 2016. Part 107 has generally been well received and marked a significant step forward for the commercial use of small UAS.

The FAA continued to lag behind in other areas. In the 2016 FAA Extension Act, Congress again pressed the FAA to make progress on a number of UAS-related issues. The FAA was required to work with industry stakeholders to develop consensus standards for the remote identification of UAS and their owners or operators. Within 180 days, the FAA had to establish a process by which applicants could petition it to prohibit the operation of UAS in close proximity to critical infrastructure or similar locations. The FAA had to create a pilot program to assess the use of UAS detection systems to mitigate threats posed by errant or hostile UAS operations near airports and critical infrastructure. The FAA had to coordinate with the National Aeronautics and Space Administration (NASA) to develop and deploy a UAS Traffic Management (UTM) pilot program. The FAA also had to encourage and streamline the use of UAS for emergency response operations (e.g., firefighting, search and rescue, and utility and infrastructure restoration efforts).

The FAA took some steps to accomplish these directives, but it did not comply with all of the required deadlines. Two years later, Congress revisited some of the same issues and imposed additional requirements in the FAA Reauthorization Act of 2018. The numerous UAS-related provisions of the 2018 act cannot all be summarized here, but these are worth noting:

- 49 U.S.C. §44802 pointedly codifies a previously uncodified law that required the FAA to integrate UAS into the NAS safely by September 30, 2015—a deadline that it had plainly missed.
- The FAA is required to develop, test, and deploy counter-UAS technologies capable of detecting and mitigating potential risks posed by errant or hostile UAS operations, including the testing of such technologies at five airports.
- The FAA is required to establish risk-based, consensus safety standards for the design, production, and modification of small UAS. Congress helpfully listed specific issues that the FAA should consider when creating those safety standards.
- The DOT must determine whether certain UAS can operate safely without further rulemaking or special grants of permission, based on the UAV's size, speed, weight, and operational capability, as well as where, when, and how the UAV is flown.
- The FAA is required to promulgate regulations for drone delivery (i.e., the carriage of property by small UAS for compensation), which is expressly not allowed by Part 107. Pending issuance of those rules, small UAS operators must be allowed to apply for permission to conduct drone delivery operations.
- The FAA is required to issue an updated plan (i.e., a roadmap) that discusses its efforts toward safely integrating civil UAS into the NAS.
- Congress rescinded the previous law that prohibited the FAA from regulating hobbyist or recreational UAS operators. These pilots must now pass an aeronautical knowledge and safety test and follow rules similar to those in Part 107.
- Congress created new, federal crimes for UAS operators who interfere with manned aircraft or wildfire suppression efforts.

Since the passage of the 2018 act, the FAA has continued to work toward accomplishing the many UAS-related goals assigned to it by Congress.

In February 2019, the FAA issued a notice of proposed rulemaking titled, "Operations of UAS Over People," which would allow small UAS flights over people, depending on the risk of injury resulting from a crash. Small UAS that weigh less than 0.55 lbs. pose a low risk and could be flown over people without restrictions. Small UAS that are expected to cause injuries below a certain threshold pose a medium risk, and they could be flown over people unless they have exposed rotating parts or a safety defect. Small UAS that are expected to cause higher levels of injuries could only be operated over people under certain conditions. The proposed rule would also allow small UAS operations to be conducted at night if the UAV has anti-collision lighting and the pilot completes night-related testing or training. Comments were due by April 15, 2019, and the FAA expected to finish reviewing those comments by December 2019.

In February 2019, the FAA issued an advanced notice of proposed rulemaking that sought comment on whether and how to enact various UAS safety-related rules, including the following: 1) stand-off distances (i.e., the amount of space between a small UAS and a person or object); 2) UAS traffic-management operations; and 3) mandatory redundancy for critical UAS systems. Comments were due by April 15, 2019, and the FAA expected to finish reviewing them by May 2020.

In May 2019, the FAA issued a notice stating that it needed time to implement new rules for hobbyist and model UAS operations. It therefore released interim guidance for such operators.

On December 31, 2019, the FAA issued a long-awaited notice of proposed rulemaking that proposed to add Part 89 to Title 14 of the Code of Federal Regulations. The FAA explained that a remote ID rule is necessary "to address safety, security, and law enforcement concerns … while enabling greater operational capabilities," including detect-and-avoid technologies, flights beyond visual line of sight, and UAS

traffic management. Remote IDs will also allow law enforcement and national security agencies to "distinguish compliant airspace users from those potentially posing a safety or security risk." The proposed rule would establish technical requirements for minimum, remote ID message elements and create three categories of UAS:

- Standard remote ID UAS would be capable of broadcasting the minimum remote ID message elements at all times, either via the internet, or directly from the unmanned aerial vehicle (UAV) if the internet is unavailable.
- Limited remote ID UAS would only be able to broadcast the minimum remote ID message elements via the internet. They would only be permitted to be operated within visual line of sight and within 400 feet of the ground control station.
- UAS that lack remote ID equipment would only be permitted to be flown either for aeronautical research, or within visual line of sight at FAA-recognized identification areas (FRIA) that are established at the request of community-based organizations. ("The FRIA category is for the recreational drone pilots who do not want to deal with Remote ID and just want to fly. The catch is that they can only operate in specific areas and must stay within 400 feet of the control station." **https://www.dronepilotgroundschool.com**).

The proposed rule would require almost all UAS (except those that weigh less than 0.55 lbs., are amateur built, or are owned by the U.S. government) to comply with these requirements within three years of the rule's effective date. It also would require UAS manufacturers to meet the minimum performance requirements for standard or limited remote ID within two years of the rule's effective date. Comments were due by March 2, 2020.

In sum, the federal regulatory framework for UAS is continuing to develop, but several technical and regulatory issues must be addressed before the promise of routine commercial UAS flights can be realized. For example, no federal agency is currently authorized or required to regulate the privacy implications of drones. Observers will continue to monitor the FAA's progress and other federal developments with close attention and great interest.

State Drone Law Trends

In part, because of the absence of comprehensive federal regulations, many state and local governments have enacted drone-specific laws on a wide range of issues. There are too many state laws to summarize here, but several notable trends have emerged. (Local laws are beyond the scope of this article.)

Restrictions on Law Enforcement

A substantial number of states (including Arkansas, Florida, Iowa, Idaho, Indiana, Illinois, Kentucky, Maine, Montana, Nevada, North Carolina, North Dakota, Oregon, Tennessee, Texas, Utah, Vermont, Virginia, and Wisconsin) restrict the use of UAS by law enforcement; some states also regulate the storage and use of UAS-acquired data. For example, Alaska requires all UAS law enforcement flights to be flown for a public purpose, preapproved, and recorded; law enforcement also must notify the public of each UAS flight if possible. Montana prohibits law enforcement from acquiring weaponized or armored drones.

Criminal Offenses

Many states have created UAS-specific crimes. Common crimes include reckless or careless flying (Arizona, Kentucky, Nevada, and West Virginia); interference with law enforcement or first responders (Arizona, California, Colorado, Delaware, Indiana, Michigan, Montana, New Jersey, and West Virginia); prohibited acts near or over critical infrastructure (Arizona, Arkansas, Delaware, Florida, Kentucky, Louisiana, Michigan, Nevada, New Jersey, Oregon, Tennessee, and Texas); voyeurism (Arizona, Delaware, and Louisiana); operating over a correctional facility (California, Iowa, Louisiana, New Jersey, North Carolina, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, and Wisconsin); invasion of privacy (Delaware, Indiana, Michigan, Pennsylvania, South Dakota, Tennessee, Texas, Utah, West Virginia, and Wisconsin); weaponized drones (Florida, Kentucky, Nevada, North Carolina, Oregon, Utah,

Vermont, West Virginia, and Wisconsin); harassment or stalking (Indiana, Kansas, Missouri, Oregon, and West Virginia); and criminal trespass (Louisiana, South Dakota, Tennessee, Utah, and Virginia). Less common crimes include flying over large public events (Delaware); resisting an officer by crossing police cordons (Louisiana); abuse of persons with infirmities by electronic means (Louisiana); flying under the influence of drugs or alcohol (Nevada and New Jersey); violating a restraining order (New Jersey and West Virginia); delivering medical marijuana (New Jersey); publishing images taken with thermal imaging that reveal individuals, materials, or activities inside a structure without the property owner's consent (North Carolina); placing another in reasonable fear of bodily injury (Pennsylvania); delivering contraband (Pennsylvania and South Dakota); dropping items into an open-air, ticketed event attended by more than 100 individuals (Tennessee); flying over a designated fireworks discharge site (Tennessee); operating over a sports venue that seats 30,000 or more people (Texas); operating over a wildland fire scene (Utah); and harassment of livestock (Utah).

Trespass

Nevada imposes liability for civil trespass if a UAS flies over private property at an altitude of less than 250 feet. North Carolina prohibits take-offs and landings of any UAS from public or private property without consent. Oregon imposes civil liability for repeated trespass after the offender has been warned. In contrast, Wyoming expressly authorizes flights of UAS over private property, except for flights that interfere with existing use or are imminently dangerous; however, UAS will trespass if they land on private property (unless forced to do so).

Hunting and Fishing

A substantial number of states prohibit the use of UAS to assist or interfere with hunting and fishing; such states include Arkansas, Colorado, Indiana, Michigan, Nevada, New Hampshire, New Jersey, North Carolina, Oregon, Vermont, West Virginia, and Wisconsin. While many of these laws are similar, some are unique. Alaska makes it a crime to use UAS to aid in commercial salmon fishing. Idaho makes it a crime to use UAS to locate any big-game animal for the purpose of hunting those animals on the same calendar day that those animals were located from the air. South Dakota prohibits the use of UAS for hunting unless for the purpose of locating a predator or varmint on private land between December and August.

Preemption of Local Laws

Some states prohibit local governments from enacting certain UAS-related laws; those states include Arizona, Connecticut, Florida, Georgia, Iowa, Illinois, Louisiana, Maryland, Michigan, Montana, New Jersey, Oregon, Pennsylvania, Rhode Island, Texas, Utah, Virginia, and Wisconsin. Arizona preempts all local laws except those that apply to publicly owned UAS. Connecticut preempts local regulation of commercial but not recreational UAS. Florida preempts local laws except for those that are generally applicable, meaning those that are not UAS specific, and relate to nuisance, voyeurism, harassment, reckless endangerment, property damage, or other illegal acts. Georgia preempts local laws adopted after March 31, 2017, except for those that enforce FAA regulations or prohibit recreational UAS from taking off or landing on public property. Iowa prohibits its local governments from using UAS to enforce traffic laws. Illinois preempts local laws except for those enacted by cities with more than 1 million inhabitants (i.e., Chicago). Montana preempts local laws governing the private use of UAS in relation to a wildfire. New Jersey preempts local laws that conflict with state UAS laws. Texas preempts all local laws except for those that regulate UAS flown during public events.

FAA-Regulated Issues

Although federal law arguably preempts state laws that purport to regulate UAS issues already regulated by the FAA (e.g., airspace, safety, registration, pilot certification), some states have nevertheless enacted such laws. Illinois authorizes the promulgation of UAS safety regulations. Massachusetts requires UAS owners to register their aircraft. North Carolina requires commercial UAS operators to pay for a state permit and pass a state-administered knowledge test. North Carolina, Oregon, and West Virginia make it a crime to interfere with manned aircraft. Oregon makes it a crime to interfere with or take unauthorized control of a UAS. Utah and Vermont have issued rules for recreational UAS operations.

Confidentiality

In addition to laws that require law enforcement agencies to protect the confidentiality of UAS-acquired data, a handful of states impose similar requirements in other contexts. Louisiana imposes stringent procedures for the use of UAS in agricultural commercial operations, primarily to protect confidential data. Oregon requires all public entities to protect UAS-gathered data from disclosure.

Although federal law arguably preempts state laws that purport to regulate UAS issues already regulated by the FAA (e.g., airspace, safety, registration, pilot certification), some states have nevertheless enacted such laws.

Conclusion

This article is only intended to provide a basic overview of drone law as it exists today. Drone law is still in its early stages of development but has the ability to affect your clients and your legal practice. Consider all potential sources of drone law—federal, state, and local—when advising your clients. And if you can do so, take the time to learn how your clients are using (or are affected by) drones. The attendant technological and legal issues are fascinating, and they will only become more so as we all integrate commercial drones into our everyday lives.