Summer 2016

Preferred News

Inside This Issue:

Drones and Public Sector Liability

By Tim Lyons, Vice President - Munich Re Specialty Markets

By 2020, an estimated 30,000 commercial and civil drones could be navigating the US skies. Called either unmanned aerial vehicles (UAVs) or unmanned aerial systems (UASs), drones are classified by navigational methods, the type of drone operation and the drone's physical characteristics.

Drones are unmanned aircraft that are operated remotely from the ground through a data-transmission link. The wave of new UAS owners is a major concern to the Federal Aviation Administration (FAA) as consumers rush to buy and fly drones. The FAA has complete authority over any craft that flies in the US.

The FAA unveiled an interim final rule (IFR) for owners of small unmanned aircraft effective October 19, 2015. Those who own a small unmanned aircraft that weighs more than 0.55 lbs. (250g) and less than 55 lbs. (25kg) must register their drone before its first flight with the FAA or face civil and criminal penalties. Operators receive a registration number that must be marked on the drone. Requests to operate a drone can be made online to the FAA stating the specifics (operator qualifications, type of equipment, when, where and how it will be used, etc.).

In the public sector, municipalities, school districts, universities, law enforcement, fire fighting, disaster relief and search-and-rescue efforts now use or plan to use UASs soon. Public sector drones operate under a Certificate of Airworthiness (COA) from the FAA (Civil use of drones operate under a similar authority called Special Airworthiness Certificate). Drones owned by US Armed Forces are not required to be registered.

States, such as Florida, and local governments are passing legislation regulating and, in some cases, strongly restricting the use of drones, particularly for law enforcement.

Where Florida stands on drone use

Under the Freedom from Unwarranted Surveillance Act, which went into effect in Florida on July 1, 2015, it is unlawful to use a drone to "capture an image of privately owned real property or of the owner, tenant, occupant, invitee or licensee of such property with the intent to conduct surveillance without his or her written consent."

This law protects Floridians' right to privacy, and is designed to prevent drone operators from flying over someone's personal or business property to watch their activities, see what they have in their backyard, or to look in their windows.

CONTINUED ON PAGE 2

Law enforcement agencies cannot use drones to gather evidence or other information unless:

- the United States Secretary of Homeland Security determines there is a high risk of a terrorist attack by a specific individual or organization;
- a judge signs a search warrant that permits the use of a drone;
- a law enforcement agency realistically suspects that lives or property are about to be seriously endangered, that a suspect is about to escape, or that evidence is about to be destroyed;
- using a drone to search for a missing person can reasonably be expected to help find that person; and/or
- the drone is used only to assess for taxes based on the assessed value of real estate or personal property.

Persons and entities can use drones under a state license only if the use is limited to what the license permits, but this does not apply to licenses that allow obtaining personal information, such as "the identity, habits, conduct, movements, whereabouts, affiliations, associations, transactions, reputation, or character of any society, person, or group of persons."

Electric, water, natural gas utilities and 18,000 US or city or state agencies may use drones to carry out their lawful activities, such as reading meters; inspecting facilities, including pipelines; and "environmental monitoring, as provided by federal, state, or local law, rule, or permit." Other persons or entities that may use drones include those who comply with FAA regulations, such as for aerial mapping and to deliver cargo.

Protecting public safety officials is one advantage

Today, approximately 18,000 US police agencies and 30,000 fire departments could use drones for a variety of public safety missions. One study completed by the Department of Transportation's Volpe Center in 2013 predicted that public agencies will employ about 58,000 UAS by 2035, with federal agencies operating 10,000 and the rest operated by state and local governments. These could include wildfire and wildlife management, crop surveys, border protection, surveillance and search-and-rescue operations. Experts predict agriculture and public safety will account for 90% of future drone use.

Privacy rights a driving issue for drone use

Public agencies must walk a fine line in many instances – balancing where the rights of individuals and government agencies to use new technology intersect with the public's right to privacy.

In February 2015, the White House issued a Presidential Memorandum that outlines key requirements for drone use. These included:

- Federal agencies must ensure their practices are consistent with limitations regarding the use, retention and dissemination of information collected by UASs.
- Information collected that contains personally identifiable information cannot be retained longer than 180 days from collection unless certain circumstances apply.
- Policies must ensure the protection of the First Amendment and not discriminate against persons based on ethnicity, race, gender, national origin, religion, sexual orientation, or gender identity.
- Agencies have one year to establish provisions describing how to access their publicly available policies and procedures implementing the Presidential Memorandum.
- Due to rapidly emerging technology, agencies must examine their policies before deploying new UAS technology and at least every three years to ensure "protections and policies" keep up with technology.

If states or local governments share drones, purchase drones with federal funds, or share the information gathered by the drones with others, the agencies must follow this executive memorandum and applicable laws and regulations. Of course, it is in the best interest of the public entity, school or other nonprofit agency to have its own policy to govern the appropriate use of drones on its behalf. The US Department of Commerce continues to solicit input in developing voluntary best practices for privacy, transparency and accountability for both private and commercial drone use.

CONTINUED ON PAGE 3

Civil liberties violations could become fertile ground for litigation

According to civil liberties advocates, the 2015 Presidential Memorandum regarding drones does not go far enough. As far back as 2011, the American Civil Liberties Union issued a report, "Protecting Privacy from Aerial Surveillance," warning US citizens that drones would "...allow for pervasive surveillance, police fishing expeditions, and abusive use of these tools in a way that could eventually eliminate the privacy Americans have traditionally enjoyed in their movements and activities." UASs carry increasingly sophisticated camera equipment with high-powered zoom lenses. This technology can clearly photograph people on the ground from 15,000 feet, posing significant civil liberties issues that will only increase as drone technology continues its rapid advance.

While the President's new public reporting requirements strive for transparency, the collection and dissemination of public information could provide challenges to any state or local government and raise Fourth Amendment arguments due to privacy concerns. Potential issues such as harassment, trespass and civil liberty breaches will be some of the areas public agencies must understand and manage. Decisions about low-altitude airspace rights—those of the land owner versus those of the drone owner—are among those facing public agencies. Personal injury and privacy will be two areas of developing law, leading to potential litigation that public agencies will need to grapple with. While liability coverage for drone use may insure against personal injury, what about the drone that collects information outside the scope of its official duties? Will coverage still apply?

The insurance industry responds to societal changes with new products, and the commercial aviation sector of the industry is no exception despite limited availability of credible loss and claims data related to drones. They are rapidly offering ways to provide coverage for this emerging risk or endorsements to limit drone risk. New technology creates new case law and increasingly specific solutions to complex problems. Examples of what types of claims will arise and how civil liberties claims will impact losses are largely hypothetical at this point.

Private use of drones in public spaces

Public entities increasingly face drone use in public parks, and colleges face use from hobbyists and others. College risk managers voice concern regarding the potential use of media-owned drones after campus emergencies. At this time, it is unclear if campus risk managers can limit the use of media-owned drones over campus locations.

For colleges with agricultural programs, drone use is a promising arena for both monitoring crops and training students in drone technology. It is clear public agencies, including colleges, must remain aware of local and state regulations while awaiting final FAA rules.

Additional coverage considerations

Public entities, schools and other nonprofits should fully understand and document the intended use of the UAS and its exposure to loss, including pilot certification and whether or not the insured has received a COA from the FAA. In addition, risk managers should know physical attributes such as speed, flying height and weight of each of its drones. This information gives underwriters a more complete understanding of the exposures to be insured.

The next question involves data breaches. When agencies gather photos or other logistical data, data breaches can occur. Cyber liability insurance can help public agencies address the aftermath of a data breach. Cyber insurers may also offer helpful risk management techniques that comply with federal data warehousing requirements – for example, how to safeguard records and ensure an appropriate record destruction policy.

How can a public agency best protect itself?

The battle between private property rights and drone technology can place public agencies in the crosshairs of litigation. Working closely with an experienced trust administrator/carrier can be the best risk management tool public agencies have in their toolbox.

Timothy Lyons is a Vice President at Munich Reinsurance America, Inc. who holds both the CPCU and ARe designations. He currently specializes in public entity risks and has thirty years insurance industry experience.