Protecting Airport Air Traffic From Errant Drones: What Are the Legal Issues and Risks?

Presented at NBAA 2016 BACE
November 1, 2016 – Orlando, Florida

E. Tazewell “Ted” Ellett, Aviation Partner and Member of Global UAS Practice, Hogan Lovells
tazewell.ELLETT@hoganlovells.com
Protecting Airport Traffic from Errant Drones: What Are the Legal Issues and Risks?

Topics To Be Covered

• Counter-Drone Technology Applications
• Developments in Airport-Related Counter-Drone Activity
• Counter-Drone Methods
• Hypothetical Airport Scenario
• Legal Issues Raised by Interfering With (Countering) Rogue Drone
• What Are the Risks of Deploying Counter-Drone Technology?
• How Should the Legal Issues and Risks Be Addressed?
Possible Counter-Drone Technology Applications

- Airports
- Sensitive Government Facilities
- Sensitive Commercial and Industrial Facilities
- Prisons
- Sporting Events / Large Public Gatherings
- VIP Protection

The US Navy built this laser to shoot down drones in military operations. Credit: Wikimedia
Developments in Airport-Related Counter-Drone Activity

• Fall 2015 – FAA Pathfinder Agreement with CACI International, Inc.
  – Evaluate technology to detect drones

• FAA Extension, Safety, and Security Act of 2016 (Became law on July 15, 2016)
  – Section 2202(a) -- Identification Standards
    – FAA shall convene industry stakeholders “to facilitate the development of consensus standards for remotely identifying operators and owners of unmanned aircraft systems and associated unmanned aircraft.”
Developments in Airport-Related Counter-Drone Activity

- FAA Extension, Safety, and Security Act of 2016 (Cont.)
  - Section 2206 -- Pilot Project for Airport Safety and Airspace Hazard Mitigation
    - FAA shall “establish a pilot program for airspace hazard mitigation at airports and other critical infrastructure using unmanned aircraft detection systems.”
    - FAA Administrator shall work with Secretary of Defense, Secretary of Homeland Security, and other Federal departments and agencies to ensure that the threat mitigation technologies that those departments and agencies develop or deploy “do not adversely impact or interfere with safe airport operations, navigation, air traffic services, or the safe and efficient operation of the national airspace system.”
    - After the pilot program is over, “the Administrator may use unmanned aircraft detection systems to detect and mitigate the unauthorized operation of a unmanned aircraft that poses a risk to aviation safety.” (Emphasis added.)
FAA Extension, Safety, and Security Act of 2016 (Cont.)

- **Section 2209 -- Application for Designation**
  - Secretary of Transportation shall establish a process to allow applicants to petition the FAA “to prohibit or restrict the operation of an unmanned aircraft in close proximity to a fixed site facility.”
  - Operators of fixed site facilities shall be allowed to apply for designation individually or collectively.
  - In a designation, the FAA shall outline:
    1. Boundaries for unmanned aircraft operations near the fixed site facility; and
    2. Other limitations that the Administrator determines may be appropriate.
  - In making a determination on a designation, the Administrator may consider:
    1. Aviation safety;
    2. Protection of persons and property on the ground;
    3. National security; or
    4. Homeland security.
Counter-Drone Methods Include:

- Detection, Tracking, and Identification

- Mitigation
  - Targeting operator and neutralizing operator’s ability to operate the drone
  - Targeting the drone and destroying it or preventing it from operating in inappropriate areas
  - Targeting the drone’s command and control links or its navigation system and flying the drone away from an inappropriate area
Real Life Example of Errant Drone Mitigation: Boggs v. Meredith

- Pending case in Federal court in the Western District of Kentucky
- Meredith shot down a drone flown by Boggs over Meredith’s land
- Meredith was initially charged with “wanton endangerment” and “criminal mischief”
  - State court judge dismissed the charges, holding that Meredith had a right to shoot at the drone
- Boggs seeks a monetary recovery for damages to his drone, and a declaratory judgment that a landowner is not permitted to shoot down a drone operating in the navigable airspace in the U.S.
- Boggs’ position is that the U.S. navigable airspace immediately above a landowner’s property is not owned by the landowner
  - Thus a drone flight over the land cannot constitute a trespass
- U.S. Supreme Court has never addressed this issue, although it did address a related issue in U.S. v. Causby in 1946
Real Life Example of Errant Drone Mitigation: Boggs v. Meredith (Cont.)

- The Boggs case could create important new law regarding:
  - Landowner’s property rights in the airspace immediately above the land
  - Drone operator’s right to operate in the navigable airspace immediately above another’s land
  - FAA’s exclusive sovereignty over the navigable airspace in the U.S.
Hypothetical San Francisco International Airport (SFO) Scenario

• SFO is located in San Mateo, California, operated by the San Francisco Airport Commission, and subject to the laws of the City of San Francisco

• Recreational drone operator thinks it would be fun to fly near or over the airport with a camera-equipped drone and take photos or videos

• To ensure safety and security of airport, and to prevent drones from interfering with manned aircraft operations or becoming a hazard to people or property on the ground, SFO seeks to prevent anyone from operating a drone near or over the airport

• SFO decides to deploy Counter-Drone technology for this purpose
Hypothetical SFO Scenario (Cont.)

• Counter-Drone methods SFO might use:
  – Detection, Tracking and Identification
  – Mitigation
    – Destroy or disable the drone;
    – Create an electronic “shield” preventing the drone from operating within a protective “bubble” over the airport;
    – Take over control of the drone by electronically hacking into the drone’s command and control link or its navigation system and forcing the drone to fly away from the protected area
Legal Issues Raised by **Destroying or Disabling Errant Drone**

• Potential criminal liability under Federal Law
  
  ─ A drone is considered an “aircraft” under the FAA Modernization and Reform Act of 2012 and the Federal Aviation Regulations
  
  ─ Under 18 U.S.C § 32 (“Destruction of aircraft or aircraft facilities”), destroying or disabling an aircraft is a Federal crime punishable by a fine of up to $250,000, a prison sentence of up to 20 years, or both
Legal Issues Raised by Destroying or Disabling Errant Drone

• Potential criminal liability under State statutes
  – For example, under § 625(b) of the California Penal Code, intentionally injuring or tampering with any aircraft without the consent of the owner is a misdemeanor punishable by imprisonment for not more than 6 months or a fine of not more than $1,000, or both
  – And under California Penal Code § 594(a), a person who maliciously damages or destroys the personal property of another is guilty of vandalism

• Potential criminal liability under local ordinances
Legal Issues Raised by Destroying or Disabling Errant Drone (Cont.)

• Potential civil liability for damages under California common law
  – For example, potential civil liability for the tort of conversion of personal property by depriving the drone owner of his possession or use of his personal property
  – Potential civil liability for personal injury or property damage in the event that a third party is injured or their property is damaged as a result of the counter-drone activity
Legal Issues Raised by Hacking into, or Interfering with, the Errant Drone’s Command and Control Link or Its Navigation System

• Under the Federal Wiretap Act (18 U.S.C § 2510 et seq.) it is illegal to wiretap "electronic communications" without the consent of at least one party to the communication

• “Electronic communications” is broadly defined by the Act to include many types of signals, including potentially the signals sent or received by drones
  – Encrypted electronic communications sent to or from a drone likely would be covered.
  – Non-encrypted communications sent to or from a drone may fall within the Act’s exception for communications "readily accessible to the general public", but the scope of this exception is not well defined
  – The Wiretap Act covers data that is in-transit, not data at rest or stored

• So the interception of electronic communications to or from a drone might well violate the Federal Wiretap Act, even if the interception is merely for the purpose of tracking the drone.

• The Wiretap Act provides for a private right of action and statutory damages

• Many states have similar wiretap statutes. The California Invasion of Privacy Act (Cal. Penal Code §630 et. seq.) prohibits wiretapping and interception of certain communications without the consent of the parties.
In addition, the Federal Communications Act of 1934 makes it illegal to interfere with wireless communications (See 47 U.S.C. §§ 301, 302a(b), 333).

Most Counter-Drone technology that involves the use of a radio transmitting device to interfere with the drone’s wireless communications would be illegal under the Communications Act, and could give rise to both civil and criminal liability.

For example, it would be illegal to use a transmitting device to interfere with a drone’s:

- Radio communications
- GPS link
- Wi-Fi
- Bluetooth connection

Violations are punishable by a monetary penalty of up to $16,000 per incident, or up to $16,000 per day for continuing violations.
In addition to potential violations of Federal law, State laws might be violated.

For example, the use of a transmitter jammer might be considered a felony under § 502 of the California Penal Code, which is entitled, “Unauthorized Access to Computers, Computer Systems and Computer Data.”

Under § 502, it is a felony to:

- Knowingly access and without permission add, alter, damage, delete, or destroy any data, computer software, or computer programs which reside or exist internal or external to a computer, computer system, or computer network; or
- Knowingly and without permission disrupt or cause the disruption of computer services or deny or cause the denial of computer services to an authorized user of a computer, computer system, or computer network.

This might also constitute maliciously injuring or tampering with an aircraft without the consent of the owner, which constitutes a misdemeanor under § 625(b) of the California Penal Code.
What Are the Legal Risks of Deploying Counter-Drone Technology?

- Possible violation of Federal, state, and local laws, and exposure to government prosecution
- Possible exposure to a civil tort action for damages incurred by the drone operator
- What if the technology does not work?
  - Possible breach of contract by the designer, manufacturer, or maintainer of the technology
- What if the technology works, but its use causes an accident injuring persons or property?
  - Product liability exposure
  - Operator negligence liability exposure
  - Possible harm to the airport facility that was supposed to be protected, or to persons working at the facility
How Should the Legal Issues and Risks Be Addressed?

• Operators of airports and other sensitive facilities should work together to have laws passed, at both the Federal and State level, to authorize the appropriate and safe use of Counter-Drone technology in appropriate and narrowly defined circumstances
  – What those circumstances are should be the focus of a healthy public policy debate
• Industry “best practices” for use of Counter-Drone technology need to be developed
• Appropriate insurance products for Counter-Drone technology risks need to be developed by the insurance industry, and appropriate insurance coverage should be obtained by all users of the technology
  – Users of Counter-drone technology should definitely consult their insurance broker
• Any deployment of Counter-Drone technology should be preceded by a thorough safety and legal review
Questions?

E. Tazewell “Ted” Ellett
Aviation Partner and Member of Global UAS Practice,
Hogan Lovells
Washington, D.C.
tazewell.ellett@hoganlovells.com
202-637-8644