Robinson+Cole

The Rise of Drones

The Erosion of Privacy, Cyber Threats and How to Mitigate Risk

KATHRYN M. RATTIGAN, ESQ.

APRIL 5, 2022

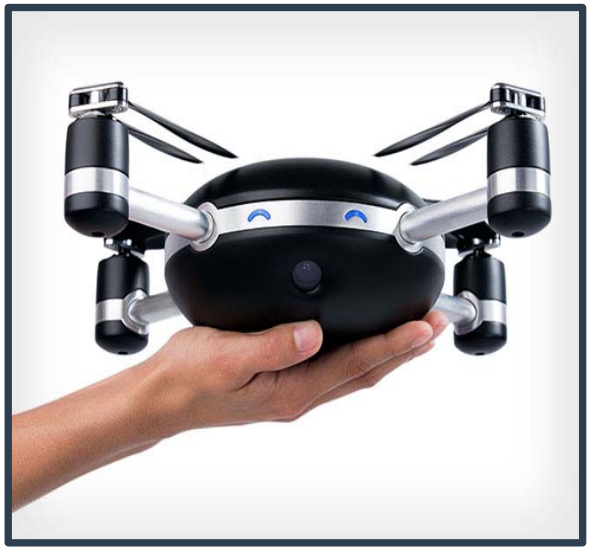
Introduction

Drones are becoming increasingly important for businesses of **all types and sizes**. Many drone applications already exist, but many more will certainly arise as drone technology continues to **evolve and advance**.

Unfortunately, this means that the **cyber threats** will also continue to evolve and advance, so we must protect the transmission and storage of data collected through drones. Drones will continue to fill our airspace and pose risks to our **privacy**, too.

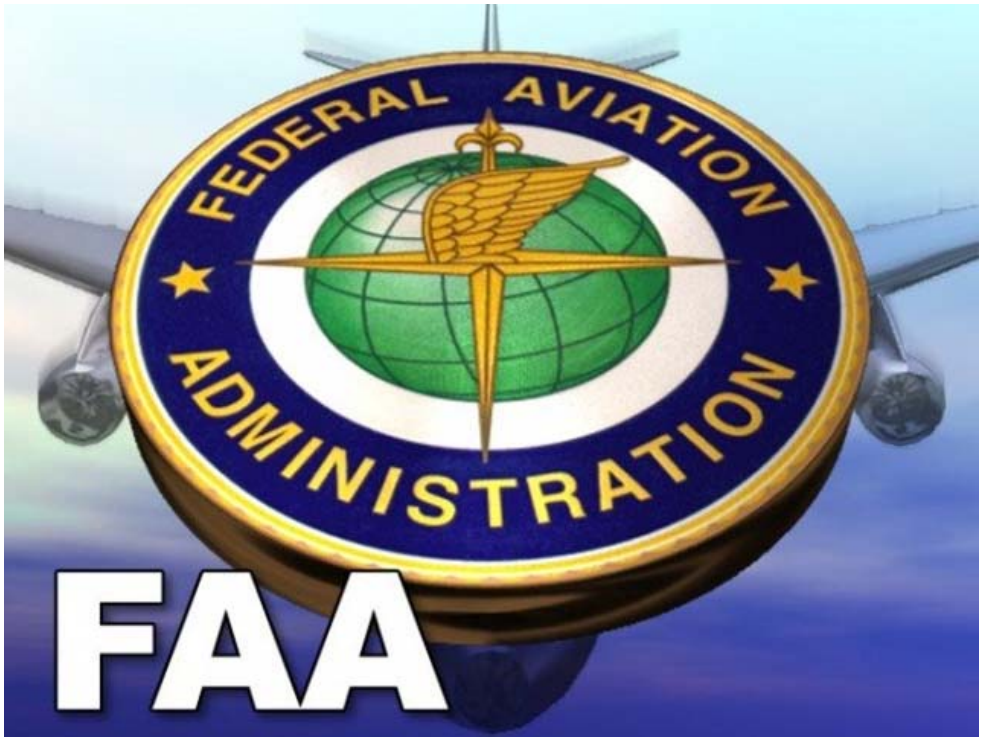
Drone Uses

Drones can collect valuable data and increase productivity, safety and efficiency across all industries.



Small UAS Rule (Part 107)

- Effective since August 29, 2016



Drones and Privacy Implications

- Technological advancements are testing the strength and reach of some foundations of the law.
- The growth, development and implementation of unmanned aerial systems/vehicles (UAS/UAV or drones) is forcing state legislators and practitioners to examine common doctrines like trespass and the right to privacy.
- The Federal Aviation Administration (FAA) regulates the **safe operation of drones**; however, the FAA leaves it up to states and local law enforcement to regulate privacy.

Drones and Privacy Implications (cont'd)

FAA's Part 107 does not specifically deal with privacy issues, and the FAA does not (and has not agreed to) regulate how UAS gather data on people or property. Simply put, the FAA "strongly encourages all UAS pilots to check local and state laws ***before gathering information*** through remote sensing technology or photography."

Drones and Privacy Implications (cont'd)

1. Inform others of your use of drones (i.e., where reasonable, provide prior notice to individuals of the general timeframe and area where you may anticipate using a drone to collect identifiable data);
2. Show care when operating drones or collecting and storing personally identifiable data (i.e., retain only information that you must retain and de-identify information when possible)
3. Limit the use and sharing of identifiable data;
4. Secure identifiable data; and
5. Monitor and comply with evolving federal, state and local drone laws and regulations.

Trespass and Aerial Trespass

- **What is trespass and how does it relate to navigable airspace?**
- **What is aerial trespass?**
- An important distinction between the trespass doctrine and aerial trespass when it comes to drone operations.

Trespass

- Trespass is defined as an entry onto another's land without permission, irrespective of any damage caused.
- The schoolkids cutting across the elderly man's lawn illustrates a trespass. The kids cross the land without permission of the landowner; thus, their mere entry onto the land constitutes a trespass.

Trespass (cont'd)

- Trespass is an intentional tort, and, from a policy perspective, the kids' intrusion onto the owner's property without permission entitles the owner to damages because of the infringement of the property owner's right to exclude.
- **When a drone replaces the kids in the hypothetical, then the trespass analysis becomes tortured because the drone never physically touches the land but instead encroaches into the airspace immediately above the land.**

Trespass Turns into Aerial Trespass

- In reliance in large part on the Restatement (Second) of Torts, the traditional trespass doctrine does not apply when a drone invades only a property owner's airspace.
- Instead, the trespass doctrine that makes sense when a physical touching occurs gives way to the tort of aerial trespass, which applies to the right of a drone operator to operate through the navigable airspace above the land.

Trespass Turns into Aerial Trespass (cont'd)

Trespass Turns into Aerial Trespass (cont'd)

- **United States v. Causby**, a seminal constitutional law case widely known for its holding on the Takings Clause of the Fifth Amendment to the U.S. Constitution.
- In Causby, the U.S. government leased an airfield adjacent to a chicken farm operation.
- The government used the airfield to train bombers prior to deploying them for combat in the European theater during World War II. As part of the operations, the bombers flew low-level approaches into the airspace directly above the chicken farm.
- The bombers flew so low that they barely cleared the treetops on some occasions.

Trespass Turns into Aerial Trespass (cont'd)

- The noise and vibrations emanating from continuous bomber-training operations had a deleterious effect on the chicken farm's operations.
- The most vivid consequence was that the chickens were frightened out of their minds—literally.
- The chickens got so scared that they ran at top speed into the sides of buildings on the farm, killing themselves—historical poultricide.
- As a result of the loss of revenue, the Causbys sued the federal government, arguing that the intrusion of bombers into the airspace above their real property constituted a taking under the Fifth Amendment requiring compensation.
- The court agreed.

Trespass Turns into Aerial Trespass (cont'd)

- The Court, in dicta, rejected the ad coelum doctrine but recognized that real property owners' rights of ownership extended to the "superadjacent" airspace or "at least as much of the space above the ground as they can occupy or use in connection with the land."
- The Court also acknowledged that aircraft flight was considered to be lawful unless the altitude was so low that the flight path interfered with the existing use of the land or the flight path posed an imminent danger to persons or property on the land.
- Building upon this language, the Court recognized that aircraft skimming along the surface of the land, but not touching the land, intruded upon the landowner's use and enjoyment of the land to the same extent as a physical trespass at ground level.
- From this combination of holdings, the term aerial trespass was born.

Trespass Turns into Aerial Trespass (cont'd)

- The result was an **implied but recognized buffer zone** between the airspace next to a landowner's property interests and the navigable airspace utilized by the federal government.
- The boundaries of the buffer zone became defined by the Federal Aviation Regulations (FARs), which set the floor for navigable airspace at 500 feet above the ground. Aircraft are not permitted to operate below this altitude unless maneuvering for takeoff and landing.

Aerial Trespass

- In 2016, the Federal Aviation Administration (FAA) released its final rule on drone operations, which established a hard ceiling of 400 feet for the operation of drones as long as those operations are far enough away from landing and departing aircraft.
- The 400-foot altitude was selected to provide a vertical safety buffer zone between unmanned flight operations and manned flight operations, which may be permitted to descend to 500 feet.

Aerial Trespass and FAA Part 107

- Drones in compliance with Part 107 regulations now legally transit through airspace that sits within the ambit of the landowner's envelope of protection.
  - From a strict tort law perspective, drones that operate through this superadjacent airspace commit a trespass, violating landowners' rights.
- The FAA relegation of drones to airspace not previously designated for aircraft flight by the federal government thus increases the pressure to reevaluate and demark the boundary between what is now usable navigable airspace and a landowner's superadjacent airspace envelope.

Aerial Trespass and FAA Part 107 (cont'd)

- Consider the following in order to assess whether or not an aerial trespass has occurred:
  - the amount of time the drone was over the landowner's property;
  - the altitude of operation;
  - the number and frequency of times that the drone has been operated over the property;
  - the time of day of the operation;
  - the operator's purpose in operating the drone over the property;

Aerial Trespass and FAA Part 107 (cont'd)

- physical damage caused by the drone operation;
- economic damage caused by the drone operation;
- whether or not the drone was seen or heard over the property;
- **whether or not the drone captured audio, video, or photographs**; and
- whether or not the landowner has regularly allowed the operation of drones over the property

Right to Privacy

What is the right to privacy? Is there a lower standard when it comes to drones?

- The drone's capture of images or video footage without permission may infringe on the privacy right of the subject
- Individuals' actions to protect their privacy rights and property interests could have implications on public policy

Right to Privacy (cont'd)

- Based on the Restatement, privacy consists of a mixture of different rights.
- The privacy interests protected in tort law include the right to be free from
  - (i) an unreasonable intrusion of a person's seclusion
  - (ii) the appropriation of a person's name or likeness
  - (iii) unreasonable publicity given to one's private life, and
  - (iv) publicity that places one in a false light before the public

Right to Privacy (cont'd)

- The infringement of the first privacy right occurs when drones pass through a landowner's airspace.
- The pass-through represents an unreasonable intrusion on a person's seclusion.
- If the drone is equipped with a video camera, then the drone's capture of images or video footage without permission infringes on the privacy right of the subject of the images by giving unwanted and unauthorized publicity to a person's private life.
- **In crafting public policy on a drone's privacy intrusion, concerns about the protection of privacy rights of the populace at large come to the forefront of the discussion.**

Consider this:

- A drone operator conducts a flight with the purpose of capturing the identity of people submitting themselves for treatment at a plastic surgery facility, a family planning facility, or a cancer treatment facility.
- The mere presence of the patients at those facilities may not be information that the patients want in the public domain through the internet or social media platforms.
- **Only the implementation of strong privacy laws that disincentivize this type of behavior will serve to protect the population's privacy rights from rogue drone operators.**

Finding the Balance

- When citizens feel that their privacy rights and property interests are threatened, they may take matters into their own hands, and their actions may have real world implications.
- Policy makers must step in and create sensible laws that achieve the dual purpose of **(1) protecting landowners' rights against trespass and citizens' rights against privacy invasions by drone operators and (2) protecting drone operators' rights to fly their craft in the airspace as designated by the FAA.**

Drone Litigation

- There has been a wide range of drone-related cases in the last couple of years ranging from flamethrowers mounted on drones to a drone crashing into a wedding guest.
- Most of the criminal cases tend to be prosecuted under the state law equivalent of careless and reckless endangerment or something along those lines. The other batch of prosecutions has to do with violations of exporting technology associated with military drones.
- DJI's lawsuits involve them being on the receiving end of a class action or DJI being the plaintiff in a patent infringement lawsuit.
- **Then there is everything else**. The civil drone lawsuits are all over the place (an Equal Protection Clause challenge against a state drone law, injured people suing drone flyers, products liability, breach of contract, invasion of privacy, etc.).

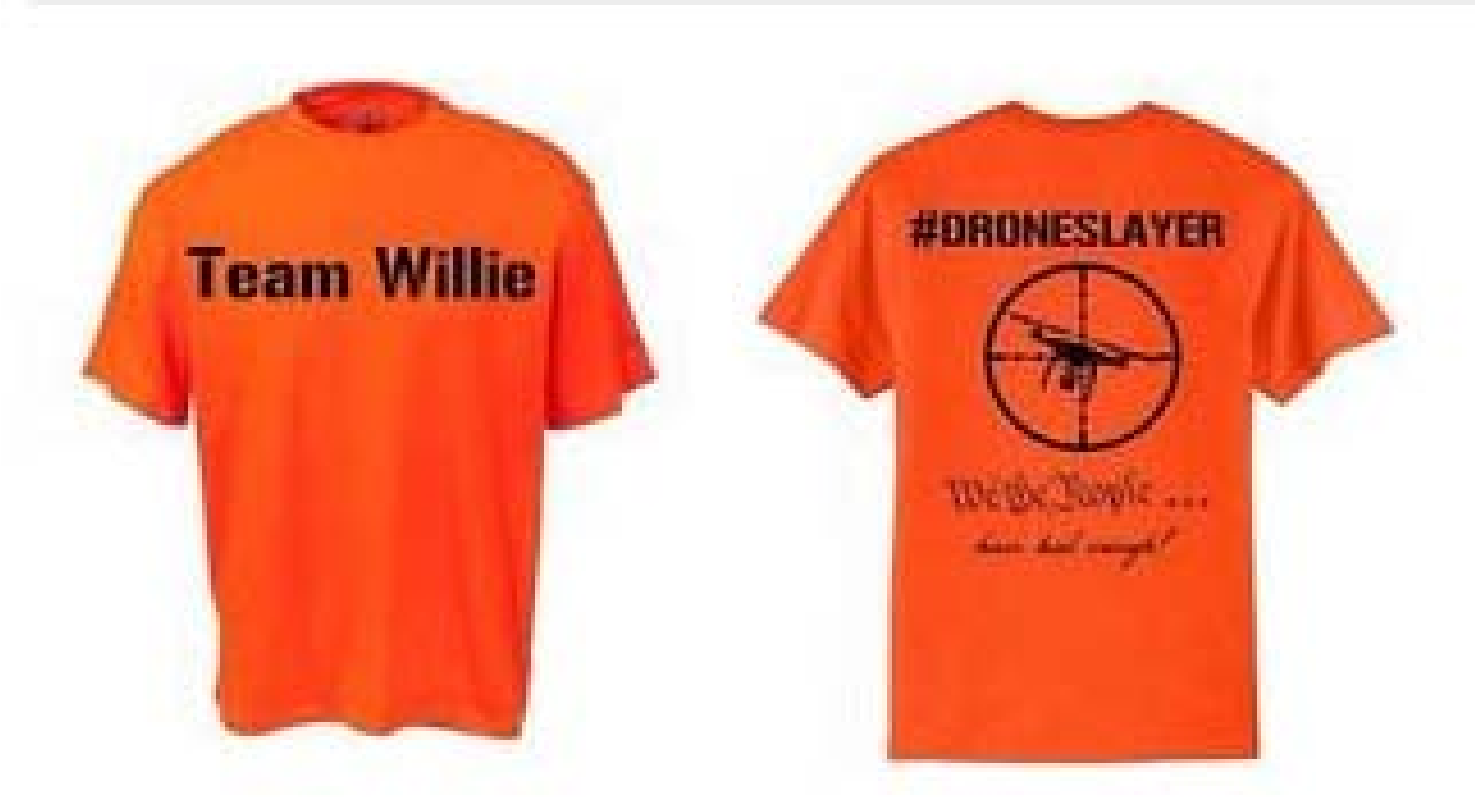
Drone Litigation (cont'd)

- **Federal Circuit Court**
  - **RaceDayQuads LLC and Tyler Brennan v. FAA** (Lawsuit Challenging Drone Remote Identification Regulations). Filed March 12, 2021.
  - **EPIC v. DRONE ADVISORY COMMITTEE**– EPIC is suing claiming the Drone Advisory Committee's use of sub groups that are meeting privately is a violation of the Federal Advisory Committee Act. There are other claims but that is the big one. The D.C. District Court ruled against them and EPIC is appealing it to the D.C. Circuit Court of Appeals. The D.C. Circuit ruled against EPIC.

Drone Litigation (cont'd)

- **Federal District Court**
  - **United States v. Jason Muzzicato.** Jason is alleged to have used a DJI Phantom 3 with explosives to terrorize his ex-girlfriends house. Failing to register the drone is one of the count.
  - **United States v. Eric Lee Brown.** Prosecuted for a drone drug drop but what is really interesting is one of the criminal charges was for failing to register the drone. There was a plea agreement.

Drone Litigation (cont'd)



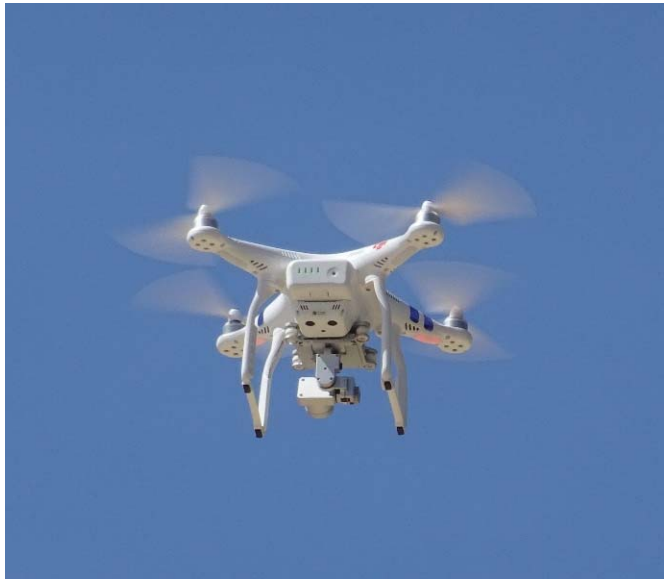
Drone Litigation (cont'd)

- **Federal District Court (cont'd)**
  - **Boggs v. Meredith** case in the federal Western District Court of Kentucky which was dismissed. Boggs' drone was shot down by Meredith. Boggs sued in federal court claiming the drone was in navigable airspace (which means he was not trespassing in Meredith's airspace) and was entitled to compensation. The court dismissed the case because the court did not have the subject matter jurisdiction to decide the case and the case should be resolved in Kentucky state court.
  - **Philadelphia Indemnity Insurance Company v. Hollycal Production, Inc. et al.** Filed April 16, 2018 in California Central District Court. Holly Cal Productions was hired to film a wedding which resulted in a patron being hit in the eye and going blind. The lawsuit is surrounding the insurance policy's aircraft exclusion.

Drone Litigation (cont'd)

- **State Courts**
  - **Long Lake Township v. Maxon (4th Amendment & Drones)**– March 2021, Michigan Court of Appeals held, " persons have a reasonable expectation of privacy in their property against drone surveillance, and therefore a governmental entity seeking to conduct drone surveillance must obtain a warrant or satisfy a traditional exception to the warrant requirement."
  - **State v. Beesmer** – (New York) Adjudicated not guilty. Flew his drone outside a hospital and was charged with unlawful surveillance. Held not guilty by jury.
  - **State v. Haddox** – Haddox was flying his drone during "CMA Fest activities and the Predators watch party on Broadway." He was arrested and charged with reckless endangerment and trespass. The "reckless endangerment charge stems from Haddox being unable to maintain line of sight of the drone and flying it over a ticketed event with thousands of persons present."

Drones and Cybersecurity



Drones are now being looked upon as an emerging security issue – both as targets for cyber-attack, and as potential attack vectors for malicious actors, themselves.

Drones + Cybersecurity

- Questions related to UAS operations and use in government surveillance have been discussed at length
- But the legal ramifications of cybersecurity negligence and data breaches for UAS operators has yet to be addressed
- UAS operators can gather imagery data and sell it largely without regulation –back to the issue of privacy

Vulnerability to Cyber Attacks

- Thriving community of ‘drone hackers’ already exists
- Susceptibility to Compromise
  - Vulnerable links streaming data to and from a drone via serial port connections and the ground station interface (whose data could be spoofed, enabling hackers to assume complete control of the vehicle)
  - Protocols implemented on the ground station applications enabling communications with the drones are unsecure, allowing hackers to install malware on the systems running the ground stations

Vulnerability to Cyber Attacks (cont'd)

- Feeds used to monitor drones and facilitate information transfer through wireless transmission are vulnerable to interception, malicious data injection and alteration of pre-set flight paths
- Used to stage man-in-the-middle cyber attacks over guest and short-range Wi-Fi, Bluetooth and other wireless connections
- Threat to sensitive data collected by drones –e.g. critical infrastructure like electric gird, transmission lines, solar and wind power, oil and gas transmissions

Vulnerability to Cyber-Attacks (cont'd)

- Particularly vulnerable to jamming, interception and manipulation (and equipment for this is relatively low cost)
- GPS vulnerability/spoofing
  - Drones rely on GPS as part of their navigation or flight control systems
  - If a spoof is successful
- Software changes during maintenance –could corrupt programming or introduce malware

Vulnerability to Cyber-Attacks (cont'd)

- Threats are evolving rapidly
  - After market models pose threat to security
  - Current UAS designs have different threats than future designs
- No set FAA standards for security
  - FAA recommends using the NIST (National Institute of Standards and Technology) framework as a primary standard
  - Also look to RTCA (Radio Technical Commission for Aeronautics) for security standards

Federal and State Laws: Do they protect this data?

- The robust existing system of aviation regulations is silent on regulating the data chain –the collection, use, retention and dissemination of any imagery, data or information gathered by UAS flight operations
- Federal and state laws regulating certain aspects of cybersecurity and data privacy do, of course, exist
  - e.g. Electronic Communications Act (includes the Wiretap Act, Stored Communications Act, Pen Register Act), the Privacy Act (federal agencies collection of data), 4th Amendment
    - Not protective of non-content or metadata
      - Metadata can include routing information as well
  - e.g. data breach laws –biometric information

Threats to National Security

Another Attempt at Blocking Chinese-Made Drones in the U.S.

By Kathryn Rattigan on February 17, 2022

POSTED IN DRONES

This week, U.S. Senators Marco Rubio, Rick Scott, and Tom Cotton (as well as U.S. House of Representatives member Elise Stefanik, who introduced parallel legislation) introduced the Countering CCP Drones Act in an effort to add DJI, a Chinese technology company, to the Federal Communications Commission's (FCC) "Covered List." The "Covered List" identifies telecommunication equipment that poses a threat to America's national security and bans their use in U.S. communications infrastructure. DJI is the world's largest drone manufacturer, with operations in California as well China and elsewhere.

The U.S. government has long been concerned about the use of DJI drones by government entities, especially in the armed services. The worry is that the Chinese government is collecting a large amount of Americans' data through these drones and their drone software and technology.

This comes after several congressional representatives petitioned U.S. Commerce Secretary Gina Raimondo to add DJI to the Department of Commerce "Entity List." DJI's inclusion on the "Entity List" would make it more difficult for U.S.-based companies to provide DJI with parts or services.

Mitigation Tips

- Good software policy
- Keep anti-virus protections up-to-date
- Train operators, employees with access to data
- Split network to limit and isolate sensitive data
- Communications should be encrypted
- Protect the drone against theft
- Protect against physical changes to the system

Conclusion

- Cyber threats will also continue to evolve and advance, so we must protect the transmission and storage of data collected through drones.
- Unfortunately, security usually comes as an afterthought.
- The drone industry is part of the aviation industry, which, based on its knowledge, keeps safety as a number one concern.
- However, part of that safety should be having proper protection for your systems, including privacy and security as fundamental design principles.

Thank you! Questions?

Kathryn M. Rattigan
krattigan@rc.com

Robinson + Cole
One Financial Plaza
Suite 1430
Providence, RI 02903
401-709-3357

Subscribe to Robinson + Cole's privacy and security blog at
www.dataprivacyandsecurityinsider.com