Articles + Publications | January 24, 2022

Drones 2022 – To Infinity and Beyond, or Back to the Drawing Board?

Privacy & Cybersecurity Newsletter

WRITTEN BY

Matthew J. Kalas | T. Patrick Byrnes

For the better part of a decade, the buzz within the Unmanned Aircraft Systems ("UAS") industry has centered on when the Federal Aviation Administration ("FAA") would put in place a regulatory environment that would allow for widespread complex operations, inclusive of flights over people and beyond visual line of sight ("BVLOS") operations. In 2021, we saw a major step forward, when on January 15th, the FAA published its long awaited Remote Identification of Unmanned Aircraft Final Rule ("Remote ID Rule"). There are significant public safety and security concerns associated with more complex UAS operations, and in particular operations over individuals and BVLOS operations. The Remote ID Rule is intended to address those concerns by establishing what the FAA describes as a "digital license plate" for drones.

In short, the Remote ID Rule requires drones operating in the National Airspace System to have the capability to transmit identification and location information. There are three ways that UAS pilots will be able to meet the identification requirements of the Remote ID Rule:

1. Operate a Standard Remote ID Drone that broadcasts identification and location information about the drone and its control station. A Standard Remote ID Drone is one that is produced with built in remote ID broadcast capability in accordance with the Remote ID Rule's requirements.
2. Operate a standard UAS that has been retrofitted with a remote ID broadcast module attached.
3. Operate without remote ID equipment at a FAA-recognized identification area sponsored by a community-based organization or educational institution.

The Remote ID Rule requires both a Standard Remote ID Drone and a retrofitted model to broadcast the drone ID, location, altitude, and velocity along with time mark via radio frequency broadcast (likely Wi-Fi or Bluetooth technology). Of note, however, while a retrofitted model is required to broadcast the drone's takeoff location and elevation, a Standard Remote ID Drone must broadcast the actual location and elevation of the control station. This means real time broadcasting of the location of the individual operating the drone, as well as the location of the drone itself. Remote ID broadcast information will be publicly available to anyone who is capable of receiving the broadcast signal, likely via their phones.

ID data that is broadcast publicly will not contain personally identifiable information. However, the Remote ID Rule does contemplate that the FAA may match an unmanned aircraft's Remote ID information with the unmanned aircraft owner's personal information, and that the FAA may share that information with law enforcement agencies "to identify, locate, or contact the person manipulating the flight controls of the UAS during an incident response."

While operator compliance with the Remote ID Rule is not required until September 16, 2023, the next major milestone on the march towards more complex operations takes place on September 16, 2022. That is the deadline by which manufacturers must commence producing Standard Remote ID Drones with the broadcasting capability called for by the Remote ID Rule. Of interest, the Remote ID Rule does not say how manufacturers must comply; instead, it lays out minimum performance requirements describing the desired outcomes, goals and results for Remote ID. Manufacturers will be required to submit their proposed means of compliance ("MOC") to the FAA for approval prior to using the MOC in the design or production of a Standard Remote ID Drone. Thus, until September 2022, we can look forward to seeing how manufacturers intend to go about meeting the Remote ID Rule, and what the FAA will allow. It will also be interesting to see what new hardware options come to market once the FAA begins approving various MOC.

While it seems there are only blue skies ahead, there are some clouds forming. On October 12, 2021, Tyler Brennan and RaceDayQuads LLC filed a challenge to the Remote ID Rule in the U.S. District Court of Appeals for the District of Columbia Circuit.[1] The Brennan plaintiffs raise two sets of challenges. The first involves arguments around the FAA's alleged failure to comply with certain rulemaking requirements. The second concerns arguments that the Remote ID Rule violates the privacy rights and rights against warrantless searches guaranteed by the 4th Amendment of the U.S. Constitution.

Among the more interesting arguments raised is that the Remote ID Rule allows for what is in essence a warrantless search of curtilage. The plaintiffs note that the Rule requires an individual operating a Standard Remote ID Drone to broadcast the location of themselves and their UAS to the FAA even if the user and UAS remain on the individual's own property at all times and the UAS is flown below the property's tree line. Thus, argue the Brennan plaintiffs, the FAA will be tracking an individual's movements and activities on their own property any time they operate a drone, and the FAA will be able to share that information with law enforcement, all without a warrant. The Brennan plaintiffs raise other 4th Amendment challenges as well, which appear to have varying levels of potential merit.

The Brennan plaintiffs do not have a friend in the UAS industry, as their challenge represents a potential serious setback to efforts to move forward with more complex UAS operations on a wide-spread basis. The Association for Unmanned Vehicles Systems Inc., which is the largest UAS industry trade association, filed an amicus brief in support of the Remote ID Rule. The D.C. Circuit held oral argument on December 15, 2021, and a decision is expected sometime in the first half of 2022.

While some may see the Brennan plaintiffs' challenge as a long-shot, it is worth noting that the FAA has faced rough sledding in the D.C. Circuit. Back in 2017, the D.C. Circuit in *Taylor v. Huerta*, No. 15-1495 (D.C. Cir. 2017) invalidated the FAA's UAS registration requirement. There, the D.C. Circuit found that the FAA's requirement that all UAS users, including recreational users, register with the FAA exceeded the FAA's statutory authority. That defeat was readily addressed via a legislative fix.

A defeat in the Brennan case may not be so easily resolved. Even if the Brennan plaintiffs are unsuccessful, their case is a reminder that the wide-spread integration of UAS into the National Airspace System raises a number of complex privacy and property right issues that will need to be addressed going forward.

---

[1] *Brennan v. Dickson*, Case No. 21-1087 (D.C. Cir. filed Mar. 12, 2021).

RELATED INDUSTRIES + PRACTICES

- Privacy + Cyber