D.C. Circuit Upholds Remote ID Rules for Drones

On July 29, 2022, the U.S. Court of Appeals for the D.C. Circuit upheld rules set by the Federal Aviation Administration (FAA) requiring drones to have remote identification (Remote ID) technology.

In *Brennan v. Dickson*, the D.C. Circuit rejected constitutional and procedural challenges to the Remote ID Rule (the Rule), concluding that the Rule did not violate Fourth Amendment privacy protections, and that the Rule was not an arbitrary and capricious use of FAA regulatory authority. No. 21-1087, 2022 WL 3008030 (D.C. Cir. July 29, 2022).

Remote ID "requires drones in flight to emit publicly readable radio signals reflecting certain identifying information, including their serial number, location, and performance information." This comes as drones are becoming ubiquitous to photograph real estate, manage agriculture, and inspect infrastructure, among other commercial tasks. However, operators have also used drones for nefarious reasons like delivering illegal drugs or wielding dangerous weapons. Without Remote ID regulations, it would be nearly impossible to distinguish between lawful recreational drones and those with potentially malicious intentions.

Brennan, a drone operator and drone-related business owner, made a facial challenge of the Remote ID Rule as infringing on a drone operator's reasonable expectation of privacy. The Court noted that the Remote ID Rule had directly harmed neither Brennan nor his business, so an as-applied challenge was not an option.

The Court rejected Brennan's facial challenge for three reasons. First, the Rule only calls for *installation* of Remote ID technology, not the monitoring. However, as the Court points out, "[i]t is the exploitation of technological advances that implicates the Fourth Amendment, not their mere existence."

Second, the Court distinguishes relatively short drone flights from cases like *Carpenter v. United States*, where "the government accessed 127 days' worth of defendants' cell phone location data," which amounted to "near perfect surveillance." The drone data can also only be accessed from a local signal—a range of about one mile. By contrast, law enforcement can remotely access cell site location information from nearly anywhere.

Last, the only unique identifier included in Remote ID data is the drone's serial number. The Rule gives only the FAA the power to match the serial number to personally identifiable registration information and only in cases where airspace safety and security is compromised. Moreover, the Rule does not allow for storage of Remote ID data.

The Court also rejected Brennan's four procedural challenges to the Remote ID rule. These included allegations of: (1) *ex parte* communications affecting the Rule; (2) the Final Rule not being a logical outgrowth of the Proposed Rule; (3) consultation failures; and (4) failing to respond adequately to significant comments. In short, the Court determined that the FAA did not act arbitrarily and capriciously in promulgating the Remote ID Rule.

The *Brennan* ruling means that drone operators will have to make sure they outfit their registered drones with the necessary Remote ID technology devices to comply with the FAA's overall goals of protecting the safety and security of the navigable airspace.

If you have any questions about the new drone Remote ID rules, please do not hesitate to contact the authors or Anderson & Kreiger's Airport Law Group.