Hogan Lovells

Federal agencies issue joint advisory on Unmanned Aircraft System detection and mitigation technology

21 August 2020

Unmanned Aircraft Systems (UAS or drones) have become increasingly popular in the United States and around the world. While the vast majority of UAS operators operate safely and in compliance with relevant laws, growing security and privacy concerns over illegal or rogue UAS operations have prompted the development of a variety of counter-UAS systems designed to detect, identify, and track rogue UAS. Many of these systems also provide the ability to mitigate the threat by interfering with, hacking, capturing, or destroying unauthorized UAS that present a threat.

The legal and regulatory framework surrounding the deployment of UAS detection and mitigation technology has lagged behind advancements in the technology. To assist nonfederal public and private entities interested in using different types of counter-UAS technology, the Federal Aviation Administration (FAA), U.S. Department of Justice (DOJ), Federal Communications Commission (FCC), and the U.S. Department of Homeland Security (DHS) issued on 17 August a joint advisory guidance on the application of federal laws to the acquisition and use of technology to detect and mitigate UAS.

While the information contained in the joint advisory guidance is not new, the joint advisory from the FAA, DOJ, FCC, and DHS remains significant. There is a great deal of confusion surrounding how federal laws will apply to this new and growing industry and the advisory confirms the federal government's view on the applicability of federal laws and regulations to UAS detection and mitigation technology. The advisory highlights the importance of understanding the legal and regulatory framework for UAS detection and mitigation systems.

The advisory addresses two categories of federal laws that may apply to UAS detection and mitigation capabilities: (1) various provisions of the U.S. criminal code enforced by DOJ that prohibit computer hacking, the interception of communications, and the use of a device to capture certain signaling information associated with communications; and (2) federal laws and regulations administered by the FAA, DHS, and FCC. The guidance notes that potential legal prohibitions are not based on broad classifications of systems, such as active versus passive or detection versus mitigation, but are instead based on the functionality of a particular system and the specific ways in which it operates and is used. Notably, various of the provisions of the U.S. criminal code the advisory addresses also contain private rights of action.

Detection capabilities

With respect to capabilities designed to detect the physical presence of a UAS or signals sent to or from the UAS, the advisory draws a distinction between technologies that capture, record, decode, or intercept electronic communications, and those that do not. While detection systems that rely on emissions which are reflected off an object and back to the detection system (such as radar, electro-optical (EO) and infrared (IR), and acoustic systems) are less likely to pose concerns under federal criminal surveillance statutes, detection systems that rely upon radio frequency (RF) capabilities to detect and track UAS by monitoring the communications passed between a UAS and its ground control station may implicate the federal Pen Register and Trap and Trace Statute, 18 U.S.C. § 3121 et. seq., and/or the Wiretap Act, 18 U.S.C. § 2510 et. seq.

Mitigation capabilities

The advisory separates mitigation capabilities into two categories: (1) kinetic technologies that physically disrupt or disable a UAS, using tools like nets, projectiles, and lasers, and; (2) nonkinetic solutions to disrupt or disable UAS, including RF, WiFi, or Global Positioning System (GPS) jamming, spoofing, or hacking techniques. The advisory clarifies that the use of nonkinetic or kinetic solutions may implicate federal criminal prohibitions against intercepting and interfering with communications, damaging a "protected computer," or damaging an "aircraft."

With respect to jamming, spoofing, and hacking technologies, the advisory identifies the Computer Fraud and Abuse Act, 18 U.S.C. § 1030; Interference with the Operation of a Satellite, 18 U.S.C. § 1367; and Communication Lines, Stations, or Systems, 18 U.S.C. § 1362, as laws that may apply.

In addition to federal criminal laws, the advisory addresses laws and regulations administered by the FAA and FCC relating to aviation and RF spectrum that may be implicated by the use of UAS detection and mitigation technology.

Finally, the advisory clarifies that detection and mitigation systems that involve emission of radio waves, including radar, must be evaluated for compliance with laws and regulations administered by the FCC.

Before deploying UAS detection or mitigation technologies, facility owners and operators must understand the legal and regulatory risks associated with their use to avoid civil and potentially criminal liability. The legal framework and policies surrounding the deployment of these technologies are evolving quickly, and companies should work with experienced legal counsel to stay abreast of new developments.

Contacts

Lisa Ellman
Partner, Washington, D.C.
T +1 202 637 6934
lisa.ellman@hoganlovells.com

Michele C. Farquhar
Office Managing Partner, Washington, D.C.
T +1 202 637 5663
michele.farquhar@hoganlovells.com

Trey Hanbury
Partner, Washington, D.C.
T +1 202 637 5534
trey.hanbury@hoganlovells.com

Ari Q. Fitzgerald
Partner, Washington, D.C.
T +1 202 637 5423
ari.fitzgerald@hoganlovells.com

Mark W. Brennan
Partner, Washington, D.C.
T +1 202 637 6409
mark.brennan@hoganlovells.com

Tim P. Tobin
Partner, Washington, D.C.
T +1 202 637 6833
tim.tobin@hoganlovells.com

Matthew J. Clark
Senior Associate, Washington, D.C.
T +1 202 637 5430
matt.clark@hoganlovells.com

www.hoganlovells.com