Volume 3, No. 5 | September–October 2020

RAIL

The Journal of Robotics, Artificial Intelligence & Law

fastcase FULL COURT PRESS

RAIL
The Journal of Robotics, Artificial Intelligence & Law
Volume 3, No. 5 | September–October 2020

THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW (ISSN 2575-5633 (print) /ISSN 2575-5617 (online) at $495.00 annually is published six times per year by Full Court Press, a Fastcase, Inc., imprint. For customer support, please contact Fastcase, Inc., 711 D St. NW, Suite 200, Washington, D.C. 20004, 202.999.4777 (phone), 202.521.3462 (fax), or email customer service at support@fastcase.com.

Publishing Staff
Publisher: Morgan Morrissette Wright
Journal Designer: Sharon D. Ray
Cover Art Design: Juan Bustamante

Cite this publication as:

The Journal of Robotics, Artificial Intelligence & Law (Fastcase)

A Full Court Press, Fastcase, Inc., Publication

Editorial Office

711 D St. NW, Suite 200, Washington, D.C. 20004
https://www.fastcase.com/

POSTMASTER: Send address changes to THE JOURNAL OF ROBOTICS, ARTIFICIAL INTELLIGENCE & LAW, 711 D St. NW, Suite 200, Washington, D.C. 20004.

Articles and Submissions

Direct editorial inquiries and send material for publication to:

Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway, #18R, Floral Park, NY 11005, smeyerowitz@meyerowitzcommunications.com, 646.539.8300.

Material for publication is welcomed—articles, decisions, or other items of interest to attorneys and law firms, in-house counsel, corporate compliance officers, government agencies and their counsel, senior business executives, scientists, engineers, and anyone interested in the law governing artificial intelligence and robotics. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the Editorial Content appearing in these volumes or reprint permission, please contact:

Morgan Morrissette Wright, Publisher, Full Court Press at mwright@fastcase.com or at 202.999.4878

For questions or Sales and Customer Service:

Customer Service
Available 8am–8pm Eastern Time
866.773.2782 (phone)
support@fastcase.com (email)

Sales
202.999.4777 (phone)
sales@fastcase.com (email)
ISSN 2575-5633 (print)
ISSN 2575-5617 (online)

Attorney General Charts Course for DOJ Counter-Drone Protection

James J. Quinlan and Elaine D. Solomon*

The authors discuss how federal law enforcement agencies are permitted to "police" the skies with respect to counter-drone measures.

Continuing increased capabilities and technological advancements of unmanned aircraft systems ("UAS")/drones make them increasingly dangerous in the hands of negligent and reckless operators, and a more serious threat if under the control of criminals and terrorists. Relevant 2018 legislation permitting federal law enforcement to conduct counter-drone activities gained traction recently through detailed guidance provided by Attorney General William Barr.

This article explains how federal law enforcement agencies are permitted to "police" the friendly skies with respect to counter-drone measures. Individuals and companies with operations affected by the unmanned aircraft industry should be aware of these newly promulgated rules regarding counter-drone measures, including processes available for federal law enforcement's procurement of training and technology regarding counter-drone measures.

AG Barr's Drone Memo

In 2018, Congress passed the Preventing Emerging Threat Act (the "Act").[1] The Act provided U.S. Department of Justice ("DOJ") and Department of Homeland Security components with authority to take certain counter-unmanned aircraft systems ("C-UAS") actions or counter-drone actions, irrespective of other federal regulations which could otherwise limit such actions, to protect designated facilities and assets from credible drone threats, including destroying the threatening drone in flight.

However, with respect to the DOJ, empowered "components" or agencies such as the Federal Bureau of Investigation ("FBI"),

Robotics, Artificial Intelligence & Law / September–October 2020, Vol. 3, No. 5, pp. 305–310.

ISSN 2575-5633 (print)/ISSN 2575-5617 (online)

the Drug Enforcement Agency ("DEA"), the Bureau of Alcohol, Tobacco and Firearms ("ATF"), and the U.S. Marshal Service could not utilize that Congressional authority without guidance from the Attorney General. That guidance has now been issued.

On April 13, 2020, Attorney General William P. Barr issued a memorandum titled "Guidance to Department of Justice components regarding counter-unmanned aircraft systems (C-UAS) actions authorized under the Preventing Emerging Threats Act of 2018" (the "Guidance"). The memorandum provides guidance as to how federal agencies can monitor and, if necessary, destroy drones threatening U.S. safety and security.

Aim for Guidance: Collaboration, Safety, Privacy

According to Attorney General Barr, the Guidance was the "product of extensive collaboration between the Department of Justice, the Department of Transportation, and the FAA," which he said, "will ensure that we are positioned for the future to address this new threat, and that we approach our counter-drone efforts responsibly, with full respect for the Constitution, privacy, and the safety of the national airspace." That said, the Attorney General made it clear through the Guidance that designations for protection under the Act would not be widespread, stating, "As a general rule, not every facility or asset will qualify for protection. Only those considered 'high risk and a potential target' for drone activity—and relate to one of the authorized DOJ missions enumerated in the Act and the Guidance—will qualify."

Another important consideration in developing the Guidance, according to Attorney General Barr, was the protection of privacy, civil rights, and civil liberties. Specifically, the Guidance requires that all actions under the Act be taken in compliance with the First and Fourth Amendments. Furthermore, although the Guidance provides that certain drone communications can be intercepted, it provides durational limits for the retention of information gained during a C-UAS action and dissemination controls for the sharing of said information. Finally, DOJ components are specifically required to provide privacy and civil liberties training to its relevant personnel in the context of counter-drone actions.

The Details

At a high level, the Guidance enumerates the DOJ agencies that are authorized to use the authority under the Act. It details the processes that authorized DOJ components must use to request designations of facilities or assets for protection under the Act. It also details the processes that authorized DOJ components use to provide protection through C-UAS actions for those designated facilities or assets. And it includes requirements for technical and compliance training of DOJ personnel who will be tasked with conducting C-UAS actions. Finally, among other things, the Guidance sets forth parameters and considerations for the procurement of materials and technology to conduct counter-drone actions.

Another restriction on the new measure is required coordination and cooperation among certain agencies regarding these anti-drone precautionary measures. Importantly, DOJ components are required to coordinate with the Federal Aviation Administration ("FAA") if the C-UAS action "might" affect aviation safety, civilian aviation, aerospace operations, aircraft worthiness, and the use of airspace, and a risk-based assessment must be conducted in coordination with the Secretary of Transportation.

Essentially, it is mandatory that DOJ components coordinate with the FAA in the process of designating and protecting facilities or assets through C-UAS actions. DOJ components are also permitted to seek designation and provide C-UAS protection at the request of state and local actors for non-federal sensitive facilities or assets, or for public events that might, for example, include large gatherings of people. The Guidance delineates processes to provide that type of assistance to state and local actors.

Trust the Process

The full process for the approval of a request for designation for the protection of a facility or asset is multilayered and involves several administrative checks and reviews. For example, a request would be reviewed by the component's Senior Component Official for Privacy, the component's legal counsel, the DOJ's Unmanned Aircraft Systems Working Group, the FAA, and, finally, the component's top official—for example, the director of the FBI for an FBI

request. Then, once transmitted by the component to the Office of the Deputy Attorney General, the Deputy Attorney General must approve the request. However, in emergency circumstances, a component top official can designate a facility or asset for protection and deploy said protection to take counter-drone actions so long as the Guidance is otherwise complied with and there is contemporaneous coordination with the FAA, as well as immediate notification of Office of the Deputy Attorney General, the Office of Legal Policy, and the National Security Division of the DOJ. Within five days of the emergency designation, full compliance with the other processes set forth in the Guidance must be achieved.

Once a request reaches the Deputy Attorney General (designated by the Guidance as the "Approving Official"), the Deputy Attorney General must consider whether the request is consistent with the requirements of the Act, other applicable law, and the Guidance, and whether it furthers the DOJ's priorities and objectives, including consideration of resource constraints and priorities. Assuming those criteria are met, the Deputy Attorney General has three varying options including:

- Designating the facility or asset as a "covered facility or asset" based on a finding that (a) the activities of unmanned aircraft or UAS pose a credible threat to the facility or asset, and (b) the facility or asset is high risk as a potential target of the unlawful activities of drones;
- Approving the deployment and use of some or all of the requested protective measures at the covered facility or asset; and
- Specifying any conditions for the deployment or use of protective measures, such as requirements for approval of operational plans and technical measures necessary to sufficiently mitigate impacts on aviation safety and the national airspace system.

With respect to the deployment of C-UAS or counter-drone actions at a designated facility for protection, the acting component has a range of options. It can detect, track, identify, and monitor a UAS by intercepting and/or accessing wire, oral, or electronic communications used to control the UAS. It can issue warnings to the UAS operator by various direct, indirect, physical, verbal, or

electronic means. It can take physical and/or electronic measures to disrupt the UAS' operation. It can also confiscate and/or seize the drone. Finally, the authorized component can use reasonable force to damage, disable, or destroy the UAS in flight or otherwise.

Conclusion

Congress took an important first step in 2018 to authorize federal law enforcement and national security agencies to protect valuable but prone facilities and assets from the threat that drones could pose. As the Attorney General stated, "As drones become more powerful and capable, however, they also become a more attractive tool for criminals, terrorists, and other bad actors to cause disruption and destruction. Unfortunately, the threat is not theoretical." However, without guidance from the Attorney General, DOJ components like the FBI, DEA, and ATF, among others, were limited in their use of this powerful Congressional authority.[2]

The Guidance provided in Attorney General Barr's memorandum addresses that limitation. The Guidance provides multiple processes and rules for how DOJ components can apply to protect a facility or asset from a drone, and how those components can actually provide C-UAS protection against a drone. It also provides processes and rules for the training of relevant DOJ personnel and the procurement of materials and technology to conduct C-UAS actions. The Guidance provides a process for federal law enforcement to assist and support state and local actors with C-UAS protection upon request. Most importantly, the Guidance requires collaboration with the Department of Transportation and the FAA to ensure that U.S. airspace remains safe for those operating in the skies and those on the ground below while federal law enforcement protects designated facilities and assets from rogue drones.

The new Guidance does state that implemented policies need to take into consideration the legitimate use of drones. Thus, it remains to be seen what effect these measures will have on the recent increased use of drones due to the coronavirus COVID-19 pandemic, where there has been increased use of drones for things such as medical supplies delivery, and local law enforcement uses including crowd control and monitoring/enforcing lockdown policies.

Notes

* James J. Quinlan, a partner in Blank Rome LLP, concentrates his practice on complex tort litigation, with particular emphasis on matters arising from product liability, aviation, maritime, and other transportation accidents. Elaine D. Solomon, a partner at the firm and co-chair of its aviation practice, is a member of the Board of Editors of *The Journal of Robotics, Artificial Intelligence & Law*. She concentrates her practice in the areas of aviation law and litigation, product liability and tort litigation. Resident in the firm's office in Philadelphia, the authors may be contacted at quinlan@blankrome.com and solomon@blankrome.com, respectively.

1. 6 U.S.C. § 124.

2. *See* 49 U.S.C. § 46502 (aircraft piracy), 18 U.S.C. § 32 (destruction of aircraft), 18 U.S.C. § 1030 (computer fraud), 18 U.S.C. § 1367 (interference with the operation of a satellite), and Chapters 119 (interception of communications) and 206 (pen registers and trap and trace devices) of Title 18.