





CHINESE DRONES ARE IN THE PENALTY -BOX-

WHO'S NEXT?

By Mary-Caitlin Ray

Though dubbed “the year that wasn’t,” 2020 has marked a turning point in the U.S. relationship with the People’s Republic of China (China). Along with numerous other trade restrictions, 2020 has seen a series of actions by executive agencies, Congress, and the White House to restrict government use and procurement of Chinese-made unmanned aircraft systems (UAS or drones). Largely in response to national security concerns that the Chinese Communist Party (CCP) could access data collected by drones manufactured in China or by Chinese companies, these actions have bipartisan support, and other countries are beginning to follow suit.

The concern, so far, has been limited to drones, but drones are not the only vehicles that collect and disseminate data. Other autonomy-driven industries, such as the automated vehicle (AV) industry, should be mindful of the evolving legislative and regulatory regime. Their operating environments differ, but drones and AVs are both data-collection vehicles with the capability to operate with high levels of independence

and self-determination. Given their similarities, AV manufacturers should take note of these government actions, as they could prove a roadmap for future action against Chinese-made AVs. At the same time, similar attention to AVs is not a forgone conclusion, given the different current uses and existing market conditions between AVs and drones. However, if other types of autonomous systems are the next phase of the tech war with China, what does that mean for attorneys who advise in these ecosystems and for their clients?

LAWMAKERS TAKE AIM AT CHINESE DRONES

A bit of context is necessary. Today's existing and proposed restrictive policies and legislation have their roots in China's National Intelligence Law. Under this law, companies domiciled in China must cooperate with Chinese state intelligence operations, including by potentially routing sensitive data back to servers located in China where they could be accessed by the CCP.

A flurry of U.S. legislation and policies began in August 2017, when the U.S. Army issued a blanket ban on all drones made by Chinese drone maker Da-Jiang Innovations (DJI). Nearly two years later, the Department of Homeland Security (DHS) and the Department of Defense (DOD) followed suit, the former issuing an advisory warning U.S. companies against using Chinese drones, and the latter banning all military agencies from procuring Chinese-made drones with limited exceptions. In early 2020, the Department of Interior grounded its entire fleet of more than 800 drones, citing potential cybersecurity risks and the need to support U.S. drone production. In March 2020, the White House joined the fray with a draft Executive Order that would ban all federal agencies from purchasing or using Chinese drones on federal lands. Finally, in October 2020, the Department of Justice (DOJ) implemented its ban on the use of funds for procurement or operation of drones manufactured by Chinese entities.

The legal framework is currently a patchwork of agency-specific legislation and individual agency policies. That

patchwork was expected to be somewhat standardized with the passage of the National Defense Authorization Act for Fiscal Year 2021 (NDAA 2021), which would have prohibited all executive agencies from procuring or operating drones or components that are manufactured or assembled by a Chinese company with narrow exceptions. The procurement prohibition of the relevant provision, section 830B, was broad, extending to "the use of Federal funds award through a contract, grant, or cooperative agreement, or made available to a State or local government, or any division thereof," and would have had far-reaching effects for government contractors and other recipients of federal funds.

Although section 830B was ultimately struck from the NDAA 2021 in the early December conference report, the government's overall concerns about Chinese drones remain unchanged.¹ The consequences of section 830B would have extended far beyond executive agencies, and the proposed blanket procurement ban is a sharp distinction from existing domestic preference regimes, such as the Buy America framework, to which government contractors and recipients of federal funds are accustomed. Due to the broad scope of the procurement prohibition, there would have been significant downstream effects on organizations that provide drones and drone-related services to the government or that rely on them internally, including government contractors and their subcontractors, state and local law enforcement agencies, and educational institutes. Prime contractors, for example, will be responsible for certifying that drone products provided under a government contract comply with section 830B. Making such a certification will require significant supply chain analysis for the prime and for its subcontractors, as described in greater detail below. Because many of the agency-specific policies contain similar provisions, recipients of federal funds will still need to consider the effects of procurement and operational bans, as well as the downstream effects on their supply chains.

Unlike existing domestic preference regimes, which generally establish

acceptable thresholds of foreign manufacturing and assembly and further distinguish between components and end products, existing and proposed drone measures establish blanket bans with limited exceptions. Attorneys that advise contractors providing drones, drone components, or related operational services to government agencies should prepare for a regulatory framework that is more stringent and less nuanced than traditional domestic preference regimes.

Section 830B would likely have come to life in the form of a new provision under the Federal Acquisition Regulation (FAR), which governs most executive agency procurement activities, and under agency-specific procurement rules for agencies that do not follow the FAR (the FAA, for example). Government agencies would then have been required to include the corresponding contract clause in their contracts based on the provision's applicability (dollar value thresholds, types of contracts, etc.). In practice, and because of similar procurement regimes being implemented in specific agencies, prime contractors need to carefully examine their supply chains, "flowing down" the applicable FAR provision (or its agency-specific equivalent) to their subcontractors to ensure that the prime is able to make the necessary certification. Because the procurement prohibitions generally apply to drones as well as their components, prime contractors will need to cast a wide net in their supply chain analysis, including ground stations, gimbals, radios, and cameras, paying special attention to percentage requirements for Chinese-made printed circuit board components. Grant recipients will likely find themselves subject to the same requirements, and they should carefully review all required "flow down" provisions contained in their grant documents and ensure that their subcontractors and suppliers are able to make the requisite certifications and representations regarding their drone products. A misstep in the supply chain analysis could result in an offeror being rendered ineligible for award or, if award has already been made, in a termination of the contract and potential enforcement action.

AV manufacturers
should continue
to track
developments
in this area.

DATA MINING: IN THE SKY AND ON THE ROAD

Despite their similarities, AVs have not been the target of the same government procurement restrictions that have rocked the drone industry. The absence of such restrictions at this stage can be attributed to several factors: the relatively nascent state of the AV industry in comparison to the drone industry; the fact that AVs are currently largely for personal use, as opposed to government use; and the United States' relatively dominant position in the AV market.

Drones and AVs operate in different environments, but they both collect, store, and transmit vast amounts of data, either actively as part of their primary operational purpose, in the case of many drones used specifically for data collection operations, or passively as part of a suite of anticollision hardware and software. Drones use these systems to detect and avoid airborne obstacles, such as other aircraft, and to ensure that the aircraft follows its intended flight path. Like their airborne counterparts, AVs are equipped with hardware and software, including sensors, cameras, and radars, to help the vehicle independently identify and deconflict safety risks, such as drifting into adjacent lanes or making unsafe lane changes.

AVs trail drones in regulatory development, number, and technological sophistication of vehicles on the market. On the drone side, industry continues to push the Federal Aviation Administration (FAA) and other key agencies for broader enabling regulations, but

the regulatory framework has allowed for a large-scale deployment of military, commercial, and recreational drones. As of November 10, 2020, 1,733,549 drones were registered in the United States, 505,394 of which are commercial drones. And while some of those drones are simple in configuration, there are many drones on the market that offer varying levels of autonomous flight.

Meanwhile, federal regulation of AVs continues to lag behind, and meaningful legislative movement is unlikely for the remainder of 2020 or even early 2021. Similar to the FAA's "crawl, walk, run" approach for integrating drones into the National Airspace System, AVs are being introduced on our roads based on a graduated system classifying the vehicle's level of automation. Today, even the most advanced AVs on the road are a Level 2 classification, where the vehicle has combined automated functions, but the driver must remain engaged and monitor the environment at all times. Tesla, for example, sold an estimated 192,259 vehicles with similar capabilities in the United States in 2019. Given the difference in the number of AVs and drones in operation and the more advanced remote and autonomous capabilities of drones, comparing the state of the drone industry and the AV industry in the United States is not necessarily an apples-to-apples comparison but provides some context for the government's recent actions concerning Chinese drones.

The difference in use profiles between drones and AVs partially explains the government's concern over Chinese drones versus its lack of action in the AV space. The military and other government agencies have come to rely heavily on drones for certain tasks, using them for sensitive and classified missions and to collect unclassified data that could be used against U.S. interests. AVs, on the other hand, are currently marketed mainly for individual consumer use. The use profile for AVs, however, could shift as the technology continues to advance.

One of the most vexing consequences of the recent drone restrictions is that there are currently few compliant

alternatives available that offer capabilities similar to those of Chinese drones. The drone market is currently highly consolidated, with the Chinese drone-maker DJI holding an estimated 77% share of U.S. consumer drone sales. This is in sharp contrast with the AV industry, in which the United States continues to be one of the dominant influences.

DRONE REGULATIONS: A CAUTIONARY TALE FOR THE AV INDUSTRY

There has been little public discourse thus far on whether a blanket ban on government procurement and operation is likely forthcoming for Chinese AVs, and the government's focus to date has been limited to the drone industry. The existing drone framework is largely reactionary, set in motion after Chinese drones had already become deeply entrenched in certain military and government agencies. AV manufacturers should continue to track developments in this area so that if the government does become concerned about Chinese AVs, manufacturers are prepared to engage with the relevant agencies and have conversations about their products as necessary. Although there is no indication that the government is imminently considering similar moves related to AV products, the AV industry should hope for the best but be prepared for the worst by evaluating their supply chains and determining their reliance on Chinese products and components. By considering the implications of prescriptive legislation and policies related to AV products now, the AV industry can scout ahead to avoid trouble, if trouble indeed comes.

Mary-Caitlin Ray is a counsel in the Washington, DC, office of Crowell & Moring LLP, where she specializes in drone regulatory and business aviation matters and aircraft transactions.

ENDNOTE

1. Ultimately, the NDAA was passed via legislative override. A.P., "In a First, Congress Overrides Trump Veto of NDAA," Jan. 1, 2021, <https://federalnewsnetwork.com/defense-main/2021/01/in-a-first-congress-overrides-trump-veto-of-ndaa>.