Bloomberg BNA

Privacy and Security Law Report®

Drones

Over the last several years, drone technology has rapidly transformed the unmanned aerial devices from recreational toys into important tools with tremendous commercial potential. But concerns over privacy and personal data collection continue to swell. Drone laws are constantly evolving, and there are hundreds of proposed laws across the U.S., so drone users should closely follow legal developments and best practices, the authors write.

Drone Privacy: Voluntary Best Practices Released by Multi-Stakeholder Group

BY ERIC D. VANDEVELDE AND JARED GREENBERG

On May 18, the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce released voluntary best privacy practices for Unmanned Aircraft Systems (UAS), more commonly referred to as ''drones'' (15 PVLR 1059, 5/23/16). Over the last several years, drone technology has rapidly transformed from recreational toys into important commercial tools with tremendous potential. The technology is currently used for dozens of applications, including film production, journalism, photography, sensory data collection, agriculture monitoring and treatment, building inspections, search and rescue missions, disaster response support, railway inspections, pipeline inspections and measuring quarry stockpiles. As the popularity of drones increases, concerns over privacy and personal data collection continue to swell.

Eric D. Vandevelde is of counsel at Gibson, Dunn & Crutcher LLP in Los Angeles and serves on the Cyber Crime Committee of the American Bar Association.

Jared Greenberg is an associate at Gibson, Dunn & Crutcher LLP in Orange County, Calif., and is a member of the Litigation Department.

This article is not legal advice, and corporations should consult counsel as they develop unmanned aircraft programs.

In February 2015, President Obama issued a Presidential Memorandum directing that privacy, civil rights and civil liberties concerns be taken into account as drones are integrated into the National Airspace (14 PVLR 322, 2/23/15). The President ordered the NTIA to create a private-sector engagement process to help develop voluntary best practices for privacy, accountability and transparency issues regarding commercial and private drone use. That process took place over the past year, with multiple private-sector groups participating in a series of meetings to develop such practices. The voluntary best practices received agreement from technology companies, insurance companies, media organizations, drone industry associations and privacy groups. Although these best practices do not create any legal standards, they set useful guidelines for any organization conducting drone operations.

Many of the recommended best practices take into account the size and complexity of the operator (*e.g.*, a large public company is expected to have a more comprehensive privacy policy with respect to its use of drones than an individual real estate photographer). Moreover, newsgathering organizations are expressly excluded from the best practices due to their strong

 ISSN 1538-3423

First Amendment protections. The following summarizes the best practices:

Covered Data: The best practices heavily focus on the collection and storage of ''covered data.'' Covered data is information collected by drones that identifies a particular person. If the data are unlikely to be linked to a particular person, or if they are altered so that a particular person is not recognizable, they aren't considered covered data.

Privacy Policy: Organizations collecting covered data should make reasonable efforts to inform individuals directly impacted by those organizations' use of drones, and they should maintain a publicly available privacy policy appropriate to their size. The policy should identify:

- the kind of covered data the drone operations will collect;
- the purpose for which the data are collected;
- retention and de-identification practices;
- the types of entities with whom the data will be shared;
- information on how to submit a privacy or security complaint; and
- the organization's practices with respect to responding to law enforcement requests for data.

In addition to considering voluntary privacy best practices, operators should comply with federal, state and local drone laws.

Reasonable Expectation of Privacy: Absent a compelling need, drone operators should avoid collecting covered data when the subject has a reasonable expectation of privacy. Operators should avoid intentional, persistent and continuous collection of covered data about individuals. Further, operators should make reasonable efforts to minimize flights over private property without consent of the owner or without appropriate legal authority.

Data Sharing and Use Limits: Drone operators should only use covered data for those purposes identified in their privacy policy. Without consent, the data should not be shared for marketing purposes or publicly disclosed without reasonable efforts to obfuscate (*e.g.*, blur) the data. Further, without consent, operators should not use covered data for employment eligibility, promotion or retention, credit eligibility or healthcare treatment eligibility, unless expressly permitted by a sector-specific regulatory framework.

Data Storage: Covered data should not be stored longer than necessary for the purposes for which it was collected (and disclosed to the public in a privacy policy). Further, organizations should develop easily accessible processes to receive privacy or security complaints about the organization's use of drones. These processes should include mechanisms by which individuals can request that an organization delete, de-identify or otherwise obfuscate a person's covered data.

Data Security: Organizations storing covered data should implement a program to address and manage cybersecurity risks. The program should have reasonable administrative, technical and physical safeguards appropriate to the organizations size and the nature of the covered data. Appropriate safeguards include those described in guidance from the Federal Trade Commission, the National Institute of Standards and Technology Cybersecurity Framework and the International Organization for Standardization's 27001 standard for information security management. Corporations should consider the below practices to secure covered data:

- a written security policy detailing the collection, use, storage, and dissemination of covered data;
- regularly monitor systems for breach and data security risks;
- provide security training to employees with access to covered data; and
- limit access to covered data.

In addition to considering the above voluntary best practices, operators should comply with federal, state and local drone laws (an overview of the current and proposed federal rules can be found here). In the next few months, the federal government should finalize the Federal Aviation Administration's proposed rules for drones weighing less than 50 pounds, which will not address privacy issues. Drone laws are constantly evolving, and there are hundreds of proposed laws across the country. For example, California has over a dozen active bills related to drones. Operators should closely follow the legal developments regarding drone laws within every jurisdiction they operate. Regulations will eventually address privacy issues, but until then, operators should consider following the voluntary best practices.

  PVLR ISSN 1538-3423