LAW.COM
An ALM Website
July 8, 2015

Take Your Drone Privacy Policies for a Test Flight

By Michael Rhodes and Karen Burhans

Michael Rhodes

Karen Burhans

Unmanned Aerial Vehicles, commonly referred to as drones, are quickly being outfitted to capture unprecedented amounts and types of data that companies can use for diverse commercial applications. Though it is currently unlawful to operate UAVs for commercial purposes in the United States (unless you are one of the limited number of companies granted an exemption by the Federal Aviation Administration), companies eager to capitalize on this revolutionary technology are already making plans to integrate UAVs into their business model as soon as the FAA promulgates its final rules for commercial use. But as the prospect of widespread commercial use of UAVs looms, so too does the specter of engagement over privacy implications related to the proliferation of UAVs.

Pending adoption of the FAA final rules, companies should be proactive in formulating privacy practices and policies applicable to this developing technology. Companies making plans to use UAVs should take advantage of this "pre-UAVs" period to consider whether and how they will collect data and to make plans for the appropriate collection, storage, and use of that data to protect third parties' privacy interests and, moreover, protect the company from the reputational and economic exposure resulting from any actual or perceived misuse of third-party data. Disclosure regimes should be deliberated and implemented.

Privacy implications of potential data collection by UAVs have become a hot-button topic in the UAVs debate. Even though widespread commercial UAVs usage may not be legal for two years or more, there has been a flurry of activity at the federal level, with some calling for government regulation of privacy issues related to UAVs.

On March 3, 2015, bills entitled the "Drone Aircraft Privacy and Transparency Act of 2015" were introduced in both the House and the Senate. These bills propose that any civilian operating a UAV must submit and have approved a "data collection statement" that identifies, among other things, whether the UAV will collect information or data, whether such information or data might be sold or provided to third parties, the period during which the data will be retained, and guidelines for the deletion of such information. The bills would also provide a private right of action to any individual whose information was collected or used in violation of the "data collection statement," allowing the individual to recover actual damages or $1,000 for each violation, whichever is greater, as well as treble damages for intentional violations.

Privacy watchdog the Electronic Privacy Information Center, on the other hand, has taken issue with the FAA's position that privacy concerns related to UAVs' operation are outside the scope of its rulemaking regarding civilian UAVs. EPIC has asked the U.S. Court of Appeals for the D.C. Circuit to "hold unlawful the FAA's withholding of proposed drone privacy rules."

The outcome of these bills and EPIC's suit is difficult to predict and, thus, at this point, any regulation of UAVs' data collection is merely hypothetical. But in the absence of overt regulation, the federal government has still taken steps to address UAVs data collection. On February 15, 2015, President Obama issued a Presidential Memorandum

directing the National Telecommunications and Information Administration to initiate a multi-stakeholder engagement process to "develop a framework regarding privacy, accountability, and transparency for commercial … [UAVs] use" directed, in part, at data collection by UAVs. The NTIA is tasked with "develop[ing] and communicat[ing] best practices," including those relating to the collection, use, retention, and dissemination of data collected by UAVs.

As a preliminary step, the NTIA invited public comment as to the structure for the multi-stakeholder process and the substantive issues that stakeholders wished to address. Commenters generally agreed that the NTIA process would be helpful to companies planning to operate UAVs and urged the NTIA to develop general, flexible principles capable of adaptation to future technological development, as well as to the FAA's final rules. The NTIA will next hold a public meeting on an as-yet-undisclosed date. It is unclear when the NTIA will complete the multi-stakeholder process and propound guidelines.

Companies' adherence to any "best practices" arising out of the NTIA multi-stakeholder process will be voluntary, and whether these guidelines will actually prove useful to companies trying to create a UAVs-privacy program remains to be seen. But regardless of the outcome of the NTIA process, companies planning to use UAVs in a manner that may result in the collection of third-party data—intentionally or not—should take it upon themselves to consider the privacy implications arising therefrom.

One of the biggest concerns with UAVs' data collection—mentioned in several comments to the NTIA—is data security. In the age of highly-publicized data breaches affecting hundreds of millions of consumers there is, understandably, a concern that UAVs may be particularly vulnerable to attack. Perhaps this is because UAVs are not only susceptible to "traditional" electronic hacking, but pose the unique problem of being small enough to be physically hijacked. Companies operating commercial UAVs must therefore consider implementing effective controls against both hackers and hijackers.

Also important are companies' internal guidelines and external transparency regarding use, storage, and deletion of data collected by UAVs. This could include privacy or data use policies that inform third parties when data is collected, what is done with that data, how long the data is stored, and other information about the company's use of collected data. Companies already collecting data through other platforms will undoubtedly be familiar with these measures and may be able to use the same or similar measures with relation to data collected by UAVs. However, companies should consider how to best adapt measures currently in place to accommodate UAVs' unique characteristics. For example, some companies allow third parties to opt out of certain data collection. But opting out of data collection by a UAV may present logistical hurdles, including that a third party may not directly interface with the UAV collecting his or her data and, therefore, may not be immediately aware, if ever, that data has been collected.

For purposes of both data security and internal data policies, companies planning to operate UAVs should first take stock of whether and how that operation may result in collection of third-party data. The particular circumstances of a company's use of UAVs will bear heavily on what privacy measures are appropriate and will be effective in protecting both third parties and the company, and, therefore, these measures will likely change as UAVs technology evolves. But with a solid privacy framework from which to grow, a company will be well poised to meet evolving privacy concerns head-on.

Michael G. Rhodes is Chair of Cooley's Privacy and Data Protection practice that won The Recorder's "Privacy Litigation Practice of the Year" award in 2015. Rhodes, who served as the firm's national litigation department chair, specializes in all areas of law concerning privacy and data protection and has been at the forefront of developing and implementing novel legal theories to address related issues for the most innovative companies in the world.

Karen Burhans is an associate in Cooley's litigation department and a member of the Commercial Litigation practice group. She represents individuals and companies in complex civil litigation in state and federal courts throughout the country, with a focus on class action matters involving technology and privacy issues.

Reprinted with permission from the July 8, 2015 edition of LAW.COM © 2015 ALM Media Properties, LLC. This article appears online only. All rights reserved. Further duplication without permission is prohibited. For information, contact 877-257-3382 or reprints@alm.com. # 087-07-15-01

Cooley