Key Considerations in Addressing Privacy Concerns During Drone Operations

07.05.2017

Imagine that one of your employees uses his or her iPhone to take some pictures of work being done at a construction site. The employee captures several images that include teenagers sunbathing by a pool on the adjacent property. Several faces can be identified in the picture. Should you be concerned that your employee has violated the privacy of the teenagers? No, because as long as you or the employee did not publish or otherwise distribute the image, a court almost certainly would find that their privacy was not violated. Now, imagine that, instead of using an iPhone, the employee captured the same image of the adjacent property using an unmanned aircraft system ("UAS," commonly known as drones). In some states, capturing the same image from a drone could be found to have violated the teenagers' privacy. In addition, under voluntary guidelines recently published by the National Telecommunications and Information Administration (NTIA), a business might also be required take steps to secure and either blur or delete the image.

The reason for this difference is that increased privacy concerns associated with UAS is resulting in a unique legal and regulatory framework with regard to the information that they can collect. For example, several states have passed laws that restrict the collection of images that can identify individuals if they are on private property and if they have not given their consent to being imaged.

Background

Generally in the U.S., individuals did not have a reasonable expectation of privacy while they were outside, even if they were on private property. For example, in Dow Chemical Co. v U.S,[1] the court found that the Environmental Protection Agency (EPA) did not violate Dow Chemical's Fourth Amendment rights when it used an airplane, without obtaining a warrant, to collect aerial photographs to inspect the company's premises under the Clean Air Act. Similarly, in California v Ciraolo ,[2] the Supreme Court ruled that the data obtained from a plane hired by the police to fly over a private home, again without a warrant, could be used as evidence in a trial.

However, with the rapid growth in UAS being used for both commercial and recreational purposes, lawmakers and regulators across the country have begun to respond to the public's media-driven privacy concerns. As a result, in addition to complying with the Federal Aviation Administration's (FAA's) regulations regarding safe UAS operations, businesses will also need to determine whether they need to comply with any federal, state and even local laws designed to protect privacy.

Status of Federal Law

Currently, there is no one federal government agency responsible for privacy in the U.S. The Federal Trade Commission (FTC) has played the primary role in protecting consumer online privacy, but thus far it has not tried to assert its limited authority to cover drone operations.[3] Some have suggested that the FAA should be responsible for regulating privacy issues associated with UAS. However, in December 2015, the FAA published a Fact Sheet on State and Local Laws that stated in part that "[l]aws traditionally related to state and local police power – including land use, zoning, privacy, trespass, and law enforcement operations – generally are not subject to federal [FAA] regulation. (emphasis added)[4]

In February 2015, the Obama Administration attempted to fill this void at the federal level by issuing a Presidential Memorandum titled, "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft System[s]." The Presidential Memorandum, which consists of two parts, was an effort by the White House to address the concerns of a very vocal privacy community while also protecting the drone industry from having to comply with a patchwork of 50 (or more) privacy laws.

The first part of the Presidential Memorandum directs each federal agency to develop a policy on data collected from UAS to protect privacy, civil rights and civil liberties. Such policies are to address the collection, use, retention and dissemination of the data. Moreover, although this section does not apply directly to commercial enterprises, it does direct agencies to ensure that federal contractors have adequate training and rules of conduct in place with regard to the use of UAS.

The second part of the Presidential Memorandum pertains to the use of UAS for commercial purposes. It directs the NTIA to bring together stakeholders from industry, academia, and the privacy community to develop voluntary "best practices" for commercial use of UAS. Beginning in August 2015, the NTIA held a series of meetings on the issue, and in May of 2016 it published "Voluntary Best Practices for UAS Privacy, Transparency, and Accountability" (the "Voluntary Best Practices"). The Voluntary Best Practices provides in part that:

"[w]hen a drone operator anticipates that a drone use may result in collection of covered data, the operator should provide a privacy policy for such data appropriate to the size and complexity of the operator, or incorporate such a policy into an existing privacy policy. The privacy policy should be in place no later than the time of collection and made publicly available."[5]

"Covered data" means information collected by a UAS that identifies a particular person, such as an image of a face.

Companies are not required to follow the Voluntary Best Practices. But if they choose to do so, they should also:

- establish a process (appropriate to the size and complexity of the operator) for receiving privacy or security concerns, including requests to delete, de-identify or obfuscate the data subject's covered data. Commercial operators should make this process easily accessible to the public, such as by placing points of contact on a company website;
- have a written security policy with respect to the covered data, appropriate to the size and complexity of the operator and the sensitivity of the data;
- make a reasonable effort to regularly monitor systems for breach and data security risks;
- make a reasonable effort to provide security training to employees with access to covered data; and
- make a reasonable effort to permit only authorized individuals to access covered data.

Status at State & Local Level

Over the past several years, UAS-related legislation has been introduced in almost every state. So far, 32 states have enacted laws addressing UAS issues and an additional five states have adopted resolutions. Many laws restrict the use of UAS by state agencies for law enforcement and regulatory purposes. Others restrict the use of UAS for hunting or make it a crime to operate a drone near critical infrastructure. However, several states that also have passed laws that restrict the use of UAS to collect information about an individual on private property, even if the same information could be collected using other means.

For example, in Florida it is illegal to capture an image of a person with the intent to conduct surveillance in violation of a person's reasonable expectation of privacy, without his or her written consent. Surveillance is defined as the observation of an individual with sufficient clarity to identify that individual. Moreover, the law provides that a person is presumed to have a reasonable expectation of privacy on his or her property if he or she is not observable by persons located at ground level. Similarly, in North Carolina, a person may not use a drone to conduct surveillance of a person without his or her consent.

Thus far only a few states have passed drone-specific privacy laws, although many expect the privacy community to push for more legislation at the state level given the lack of federal oversight. Some cities also have introduced drone-specific ordinances intended to protect citizens concerns regarding privacy, including bans. In addition, the National League of Cities recently published a model ordinance (the "Model Ordinance") on UAS that cities can use. The Model Ordinance requires a drone operator to register with a city before operations. In addition, it states that:

"[t]he City Manager may adopt reasonable restrictions on the time, place and manner in which a person may land, launch or otherwise operate an Unmanned Aircraft so as not to interfere with the health, safety, and welfare of City residents."[6]

What This Means for Businesses

As a result of the evolving nature of laws around the data collected by UAS, there are several steps that businesses should take. These include:

- consider using UAS with geofencing that can minimize the collection of data outside of aprescribed area;
- ensure that your drone operators understand the privacy concerns associated with UAS and instruct them to avoid collecting data on persons or properties outside the scope of work;
- when practical, provide notice (signs, flyers, etc.) that a UAS is being used to collect imagery around a certain area; and
- if you are likely to be collecting data that could raise privacy concerns, develop a written policy that outlines how the data should be stored, outlines a reasonable retention period and limits access to the data to employees that have a need.

[1] 476 U.S. 227 (1986)

[2] 476 US 207 (1986)

[3] However it is important to note that the FTC recently held a forum on drones and privacy. See e.g. https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones (accessed on October 17, 2016).

[4] FAA Fact Sheet on State and Local Laws https://www.faa.gov/news/updates/?newsId=84369 (accessed on October 17, 2016)

[5] Voluntary Best Practices for UAS Privacy, Transparency, and Accountability https://www.ntia.doc.gov/files/ntia/publications/uas_privacy_best_practices_6-21-16.pdf (accessed October 17, 2016)

[6] A Model for Cities: Ordinance for the Promotion of Drone Innovation & Accountability http://www.nlc.org/Documents/Find%20City%20Solutions/City-Solutions-and-Applied-Research/FA_drone_ordinance_brief.pdf (accessed on October 17, 2016)

Related People

- Kevin D. Pomfret – 703.760.5204 – kpomfret@williamsmullen.com

Related Services

- Construction
- Unmanned Systems