Drones and Privacy Just Got More Complicated (Table Included)

By: Kevin D. Pomfret

06.16.2016

As businesses seek to integrate into their workflows data collected from Unmanned Aircraft Systems (UAS), commonly known as drones, they are confronted with a very sensitive and complex issue: privacy.

Currently, there is no federal law that specifically governs the collection, use, storage, or distribution of data collected from UAS. In the absence of federal rules, several states have passed laws that do regulate UAS-collected data. While a number of other states have considered similar legislation, most states still have not passed UAS-specific privacy laws and are relying on existing laws and regulations to address any perceived privacy concerns.

President Obama issued a **Presidential Memorandum** on February 15, 2015 directing the National Telecommunications and Information Administration (NTIA) to convene a multi-stakeholder group with a goal of developing voluntary best practices for protecting privacy, civil rights, and civil liberties while using UAS. The group, which consisted of a number of UAS trade associations, civil liberty groups, academics, and a few potential users of UAS-collected data, held multiple meetings beginning in the summer of 2015. This past month, the NTIA announced that a consensus had been reached among a number of the participants. A copy of the ?Voluntary Best Practices for UAS Privacy, Transparency, and Accountability? (?Voluntary Best Practices?) document can be accessed **here**. The NTIA website also contains comments from several participants both supporting and disagreeing with the final document. These comments can be found **here**.

The ?Voluntary Best Practices? document contains recommendations that would have a significant impact on how businesses collect, use, and share data collected from UAS. For example, a business could be required to implement information security measures to protect an image inadvertently captured by a UAS of an individual in a public place. In addition, some businesses would be required to develop and post policies to receive, and presumably respond to, requests to ?delete, de-identify, or obfuscate? an image of an individual. Most of these provisions would not apply to the same data collected from sensors mounted on other platforms, such as manned aircraft, mobile devices, or security

cameras. As a result, businesses could have to develop separate information security policies and procedures for similar data collected from different platforms.

It is also important to note that while the recommendations in the ?Voluntary Best Practices? document are voluntary and not intended to have the force of law, some of the provisions could be integrated into law in the future at the federal or state level. For example, The Federal Aviation Administration (FAA) Reauthorization Act of 2016, passed by the Senate on April 19, 2016, would require the NTIA to report to Congress on the multi-stakeholder process and include legislative and regulatory policy recommendations.

As a result, businesses that are considering using UAS to collect data should review the ?Voluntary Best Practices? document to determine which provisions they can integrate into their existing workflow. If there are provisions that would be overly difficult to implement, businesses should consider documenting why the provisions should not apply to them. They may also want to consider implementing alternative measures that could provide adequate privacy protection. In addition, if a business hires a third party UAS operator to collect data, it should understand the steps the third party is taking to protect privacy during the data lifecycle ? collection, use, storage, and distribution.

Key Takeaways - How Businesses Can Address Privacy Concerns Related to Drone Use
1. Determine if there are any state/local laws that restrict collection of data from UAS.
2. Train UAS operators on privacy concerns associated with UAS and data collected from UAS.
3. Consider developing internal processes and controls for integrating data from UAS into business workflow while avoiding potential privacy concerns.
4. Continue to monitor UAS privacy legislation, regulation, and policies at federal, state, and local levels.
5. Make sure that agreements with vendors and customers contain applicable privacy-related terms and conditions.

Related People

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

Related Services

- Unmanned Systems