News Article

Mind the Gap: Drone Privacy Falling Through Regulatory Cracks

- FAA says privacy not its responsibility; states step into gap
- Worries about data harvesting, law enforcement surveillance

By Avery Ellfeldt | August 4, 2018 7:04AM ET

The growing popularity of drones among hobbyists, businesses, and law enforcement is exposing a gap in privacy regulation that threatens to leave Americans vulnerable to nosy neighbors and data-harvesting technology companies.

States and localities that have traditionally protected people from peeping toms and unwanted surveillance are hampered, analysts say, by the federal government's "exclusive sovereignty" over the skies. The Federal Aviation Administration, meanwhile, says its regulatory jurisdiction is limited to safety concerns and doesn't extend to privacy.

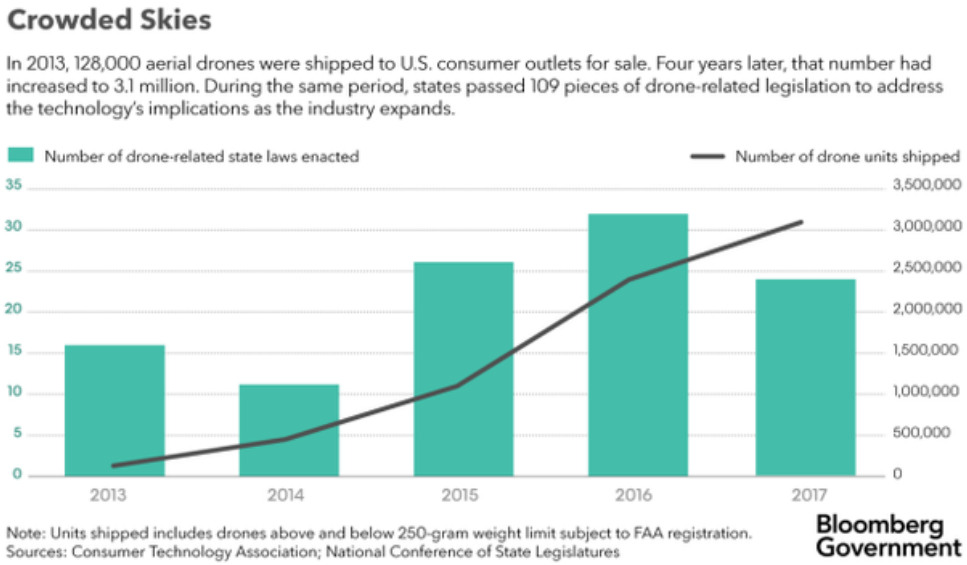
Privacy concerns have become more urgent, with total U.S. drone shipments projected to increase to a record 3.4 million in 2018, worth $1.1 billion in revenue, according to a report by the Consumer Technology Association.

Cheaper, easier-to-use drones that are nearly always equipped with cameras put the technology "within reach of people who might want to use or violate someone's privacy," said Jeremy Gillula, tech policy director with the digital rights group Electronic Frontier Foundation. And high-tech drone usage by data-hungry companies may pose a greater privacy risk to Americans than an over-curious neighbor, according to analysts.

As recently as July 20, the FAA said, "Congress has provided the FAA with exclusive authority to regulate aviation safety, the efficiency of the navigable airspace, and air traffic control, among other things. State and local governments are not permitted to regulate any type of aircraft operations, such as flight paths or altitudes, or the navigable airspace."

However, even in restating its power over air regulation, the FAA also said, "Laws traditionally related to state and local police power – including land use, zoning, privacy, and law enforcement operations – generally are not subject to federal regulation."

That still left a lot of questions, for privacy advocates.



"The FAA has basically disclaimed any authority or responsibility for writing any regulations about privacy when it comes to drones," Gillula said. "That makes it tricky if a state or locality wants to write regulations because they have to figure out how to thread this needle that doesn't infringe on the FAA's domain."

The Federal Trade Commission has also been largely silent on the issue. The FTC has not disclosed any drone privacy enforcement actions and doesn't have direct rulemaking authority absent Congressional legislation. "If companies operate drones in a manner that causes or is likely to cause substantial injury to consumers, we may be able to bring actions in certain instances, after considering the costs and benefits of such conduct," a spokeswoman told Bloomberg Government.

State governments recognize the FAA's airspace authority but believe "it is imperative to preserve the authority of state governments to issue reasonable restrictions on the time, manner and place of [umanned aerial systems] operations as they relate to states' traditional police powers," said Ben Husch, the National Conference of State Legislatures (NCSL) infrastructure committee director.

The Information Age

Developing technologies like facial recognition and the ability to "sniff" MAC Internet addresses remotely "could be leveraged to create a record of who was where at what time," Jeramie Scott, national security counsel at the Electronic Privacy Information Center, said.

"It's a surveillance issue, in the sense that [corporations] will be using drones to collect information on individuals but for the purposes of leveraging that information for monetary gain," Scott said. "In this age of information, the risk is that they will just collect lots of data on people in public without their knowledge."

The National Telecommunications and Information Administration (NTIA) in 2016 tried to address that issue. It brought together privacy advocates, industry, and government to craft voluntary privacy best practices for commercial drone, such as notifying people when they are being surveilled, the types of data collected and how the data would be be stored and used.

Privacy groups should wait to see how well the NTIA's recommendations work before asking for more regulation, said Lisa Ellman, co-executive director of the Commercial Drone Alliance, a drone advocacy group that includes Ford Motor Co., CNN, a part of Time Warner Inc..

EPIC disagrees, because "NTIA's voluntary best practices are just that, voluntary," Scott said.

“Without safeguards, we could get a similar industry like we have for license plate readers, where a company aggregates massive amounts of data through the use of drones to create services sold to law enforcement and other interested parties,” Scott said.

States Step In

Worried about drone use by hobbyists and law enforcement, states and cities have begun passing their own restrictions.

In 2017, 338 bills regarding drones were considered across the country, according to the Association for Unmanned Vehicle Systems International (AUVSI). Thirty-three of those bills, in 17 states, regarded drone privacy. About 120 localities have also pursued drone ordinances, said Brittney Kohler, the director of transportation and infrastructure at the National League of Cities.

Eighteen states passed legislation requiring law enforcement to obtain such warrants if they plan to use drones for surveillance or searches, according to a 2017 report by the NCSL.

“If it is a public actor, like law enforcement, generally we’ve said that if you’re going to be surveilling someone’s property using a drone, you should get a warrant. That is the goal that we think states and localities should aspire to,” Gillula said.

At least 19 states have also aimed at preventing abuse by hobbyists, “providing privacy protections from other citizens that are specific to drones,” according to the NCSL.

A New Industry

Ellman and Gillula said existing state legislation addressing peeping-tom and harassment concerns likely have drone use covered.

“There is a whole web of existing, technology-neutral privacy laws and rules on the books whether you’re using a drone or a cell phone or a helicopter or any other type of technology,” Ellman said. “This is a brand-new industry just getting off the ground and we don’t have data indicating more than anecdotally what exactly the concerns are.”

EPIC favors FAA regulation, saying it should require remote identification of all drones. The technology would broadcast drone’s registration numbers, which could be used by the public or law enforcement to find information about the device’s purpose, course and operator through an online database.

“This would keep companies accountable for the information they try to collect,” EPIC’s Scott said.

The FAA is currently working with state and local governments on the UAS Integration Pilot Program, meant to test expanded drone use in the national airspace. The FAA says the program will help it eventually develop rules to address security and privacy risks, while balancing local and federal authority.

To contact the reporter on this story: Avery Ellfeldt in Washington at aellfeldt@bgov.com

To contact the editors responsible for this story: Paul Hendrie at phendrie@bgov.com; Jonathan Nicholson at jnicholson@bgov.com; John R. Kirkland at jkirkland@bgov.com