Government Attacks on Private Drones

Congress should not give the Departments of Justice and Homeland Security sweeping new authority to destroy, commandeer, or intercept the communications of privately-owned drones.

The Preventing Emerging Threats Act of 2018 (S. 2836, H.R. 6401) would authorize DOJ and DHS to do so in extraordinarily and unnecessarily broad circumstances: whenever the agency deems it proper to "mitigate" a "credible threat" to a "covered facility or asset." The term "mitigate" is not defined at all. The definition of "credible threat" is left to the discretion of DOJ and DHS and requires neither an immediate threat, nor a threat to human life or physical safety. The term "covered facility or asset" could extend to all federal property.

This bill would intrude on the First Amendment right to use drones to gather news about government misconduct, and the Fourth Amendment right to private electronic communications. The bill also would exempt these agencies from following procedures that ordinarily govern electronic surveillance and hacking, such as the Wiretap Act, Electronic Communications Privacy Act, and the Computer Fraud and Abuse Act.

First Amendment Concerns

When government agencies hide their activities from the public, private drones can be a crucial tool for transparency. For example, DHS routinely denies reporters access to detention centers. Drones have provided crucial documentation of facilities constructed to hold children. The bill would also allow states to request federal support at "mass gatherings," which could include protests. If DHS or DOJ deem drone footage of police clashing with protesters a threat, they could destroy it before the public views it.

Fourth Amendment Concerns

The Fourth Amendment and numerous statutes protect the privacy of electronic communications. This includes messages sent between a drone and its operator, such as the images gathered by the drone, or communications among multiple operators. The bill would allow DOJ and DHS to ignore all of these privacy safeguards, whenever they wish to commandeer or track a drone that they deem a threat, by means of intercepting its communications. The bill's requirement for the agencies to develop privacy policies cannot undo these harms.

Broad Anti-Drone Proposals Give Agencies Dangerous Leeway

In some circumstances, the government may have legitimate reasons for engaging drones that pose an actual, imminent, and narrowly defined "threat." EFF is well aware of the threat that drones can pose to public safety and privacy—we have been concerned about government drones for a long time. But we don't think the solution requires handing the government such unfettered authority to destroy, commandeer, or eavesdrop on private drones.

If lawmakers want to give the government the power to hack or destroy private drones, then Congress and the public should have the opportunity to debate how best to provide adequate oversight and limit those powers to protect our right to use drones for journalism, activism, and recreation. This power should not be slipped into a must-pass spending bill.

Want more information?

Please contact India McKinney at **india@eff.org**.