# The Drones Are Coming

by Harley Geiger [1]
December 21, 2011

Americans are used to reading about unmanned aircraft flying over the Middle East in search of militants. Soon those eyes will be over American skies as well. This coming spring, the Federal Aviation Administration (FAA) plans to propose rules that will enable civilians to obtain permits to fly drones over the national airspace.

Non-military drones can be very useful in a variety of ways – from dusting [2] crops to inspecting [3] dangerous disaster sites – but drones are also powerful surveillance tools. Before unleashing this technology, the FAA must establish basic privacy and transparency rules for domestic use of drones. The FAA should require applications for drone licenses to include a description of how the drone operator intends to handle any information the drone will collect about individuals, and the FAA should make approved drone licenses, along with the licensee's privacy statement, publicly available.

The largest initial U.S. market for drones is our roughly 20,000 civilian law enforcement agencies. Drones with video recording equipment allow law enforcement to patrol [4] the nation's borders, hunt down [5] suspects, and even monitor [6] "antisocial" driving. From high above, drones are capable [7] of watching an entire town at once, with no need to refuel [8] for a day or more. Drones can be outfitted with facial recognition cameras [9], license plate scanners [10], thermal imaging cameras [11], open WiFi sniffers [12], and other sensors.

Of course, law enforcement agencies will not be the only ones using drones. Potentially anyone from media companies [13] to homeowners' associations might one day obtain a permit to send a flying video camera into the air and stream the footage onto the Internet. Drones are not terribly expensive – some law enforcement models cost roughly as much as a police cruiser. The combination of effectiveness, low cost, and industry pressure is likely to spur widespread drone use in coming years.

The U.S. Supreme Court declared [14] long ago that individuals have no "expectation of privacy" in public places, making people on city streets or open fields fair game for aerial surveillance. The Supreme Court also held [15] that individuals on their own property have no expectation of privacy from police observation from public airspace, meaning that police do not presently need a warrant to peer into a fenced-in backyard with a drone. However, police do [16] need a warrant to use a unique sensory device – such as a thermal imaging camera – on an individual's home, and some state privacy laws [17] offer weak protection against video surveillance of individuals on private property. Taken as a whole, though, American law currently affords few clearly defined privacy protections when it comes to drones.

That is why it is important that the FAA's upcoming rules for civilian drones include fundamental privacy and transparency standards. The FAA's current, interim guidelines [18] for unmanned aircraft are silent on these issues. The FAA is charged [19] with managing flight within the domestic airspace "in the public interest." When aircraft are being used not for transport, but expressly to conduct aerial surveillance, the "public interest" should include basic privacy and transparency considerations.

When the FAA proposes new regulations in the spring, the agency should establish – at minimum – two basic requirements:

- All applications for an FAA drone license should include a data collection statement defining whether the drone will collect information about individuals and, if so, the circumstances under which it will be used and how the drone operator will handle any information collected

about individuals. To establish the outlines of a data collection statement, the FAA does not need to come up with its own privacy framework – it can use the one adopted [20] by the Department of Homeland Security (DHS) in 2008, which spells out the key questions in the planning of any information collection system. Using the DHS framework, an applicant should describe 1) the purpose for which the drone will be used and the circumstances under which its use will be authorized and by whom, 2) the specific kinds information the drone will collect about individuals, 3) the anticipated uses and disclosures of that information, 4) the possible impact on individuals' privacy, 5) the specific steps the applicant will take to mitigate the impact on individuals' privacy, such as protections against unauthorized disclosure, 6) the individual responsible for safe and appropriate use of the drone, and 7) an individual point of contact for citizen complaints.
- The FAA should make all approved licenses, with the associated privacy statement of the drone operator, available online to the public in a searchable format. This requirement may have an exception for national security, but not for law enforcement. (Transparency does not require disclosure of the names of targets or the exact times or places of deployment; rather it requires disclosure of the criteria and supervisory controls under which drones will be deployed.)

Law enforcement agencies and their contractors should be subject to extra disclosure requirements. In addition to the above items, law enforcement agencies and their contractors should also disclose 1) the officials who can authorize use of the drone, 2) the applicable data minimization policies barring the collection of information unrelated to the investigation of crime and requiring the destruction of information that is no longer relevant to the investigation of a crime, and 3) the applicable audit and oversight procedures that ensure agencies and their contractors use drones only as authorized, within the scope of the data collection statement, and in compliance with data minimization policies.

These requirements alone will not fully protect Americans' privacy from drones. Drone surveillance – whether it is carried out by law enforcement or not – raises significant legal and constitutional issues that deserve serious discussion. However, it is highly unlikely that the FAA will thoroughly address these issues in its proposed rulemaking, nor does the FAA have adequate authority to solve them. The baseline recommendations CDT outlines above are, by comparison, less complex and controversial – essentially we are urging the FAA to require drone users to have a public privacy policy. Considering the magnitude of the privacy risks posed by drones, there is scarcely any good reason not to include such basic requirements in the FAA rulemaking.

Drones represent just one of many emerging technologies [21] that pose critical challenges to privacy and for which current U.S. law provides inadequate protection. One area ripe for reform is the Electronic Communications Privacy Act (ECPA), which sets standards for government surveillance of digital communications. CDT has organized a coalition – called Digital Due Process [22] – that is urging Congress to update ECPA by clarifying and strengthening standards for government tracking of cell phones, as well as government access to email and private documents stored in the cloud. Unless Congress and the courts update the law, Americans will find themselves with virtually no privacy protection in any practical sense.

In the meantime, the FAA should do what it can with its rulemaking this spring. Without going so far as to say what legal standard should apply to the use of drones, and without awaiting legislative or judicial action, the FAA can establish a basic framework for domestic use of drones, providing some transparency into the practices of those proposing to put eyes in the sky over our homes.



**Links:**

[1] https://www.cdt.org/personnel/harley-geiger
[2] http://tradevv.com/chinasuppliers/unmannedhelicopter_p_10aae4/china-Crop-dusting-Unmanned-Helicopter.html
[3] http://theatlantic.com/technology/archive/2011/04/inside-the-drone-missions-to-fukushima/237981/
[4] http://wired.com/dangerroom/2011/03/u-s-drones-are-now-sniffing-mexican-drugs/
[5] http://latimes.com/news/nationworld/nation/la-na-drone-arrest-20111211,0,324348.story
[6] http://guardian.co.uk/uk/2010/jan/23/cctv-sky-police-plan-drones
[7] http://washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html
[8] http://wired.com/dangerroom/2011/11/navy-killer-drone-refuel/
[9] http://wired.com/dangerroom/2011/09/drones-never-forget-a-face/
[10] http://foxnews.com/us/2011/11/16/drone-gives-texas-law-enforcement-birds-eye-view-on-crime/#ixzz1dw9bVOh8/
[11] http://draganfly.com/uav-helicopter/draganflyer-x6/features/flir-camera.php
[12] http://suasnews.com/2010/08/587/wi-fi-aerial-surveillance-platform-wasp/
[13] http://forbes.com/sites/kashmirhill/2011/08/02/faa-looks-into-news-corps-daily-drone-raising-questions-about-who-gets-to-fly-drones-in-the-u-s/
[14] http://supreme.justia.com/us/389/347/case.html
[15] http://supreme.justia.com/us/488/445/case.html
[16] http://supreme.justia.com/us/533/27/case.html
[17] http://law.onecle.com/california/civil/1708.8.html
[18] http://faa.gov/about/office_org/headquarters_offices/ato/service_units/systemops/aaim/organizations/uas/coa/faq/media/uas_guidance08-01.pdf
[19] http://fsims.faa.gov/PICDetail.aspx?docId=72F30BFA598B24F18525734F00766532
[20] http://dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf
[21] http://cdt.org/blogs/harley-geiger/612facial-recognition-and-privacy
[22] http://digitaldueprocess.org