SEARCH

JANUARY 10, 2012 | BY JENNIFER LYNCH

Are Drones Watching You?

Today, EFF filed suit against the Federal Aviation Administration seeking information on drone flights in the United States. The FAA is the sole entity within the federal government capable of authorizing domestic drone flights, and for too long now, it has failed to release specific and detailed information on who is authorized to fly drones within US borders.

Up until a few years ago, most Americans didn't know much about drones or unmanned aircraft. However, the U.S. military has been using drones in its various wars and conflicts around the world for more than 15 years, using the Predator drone for the first time in Bosnia in 1995, and the Global Hawk drone in Afghanistan in 2001. In the Iraq and Afghanistan wars, the US military has used several different types of drones to conduct surveillance for every major mission in the war. In Libya, President Obama authorized the use of armed Predator drones, even though we were not technically at war with the country. And most recently in Yemen, the CIA used drones carrying Hellfire missiles to kill an American citizen, the cleric Anwar al-Awlaki. In all, almost one in every three U.S. warplanes is a drone, according to the Congressional Research Service. In 2005, the number was only 5%.

Now drones are also being used domestically for non-military purposes, raising significant privacy concerns. For example, this past December, U.S. Customs and Border Protection (CBP) purchased its ninth drone. It uses these drones inside the United States to patrol the U.S. borders—which most would argue is within its agency mandate—but it also uses them to aid state and local police for routine law enforcement purposes. In fact, the *Los Angeles Times* reported in December that CBP used one of its Predators to roust out cattle rustlers in North Dakota. The *Times* quoted local police as saying they "have used two unarmed Predators based at Grand Forks Air Force Base to fly at least two dozen surveillance flights since June." State and local police are also using their own drones for routine law enforcement activities from catching drug dealers to finding missing persons. Some within law enforcement have even proposed using drones to record traffic violations.

Drones are capable of highly advanced and almost constant surveillance, and they can amass large amounts of data. They carry various types of equipment including live-feed video cameras, infrared cameras, heat sensors, and radar. Some newer drones carry super high resolution "gigapixel" cameras that can "track people and vehicles from altitudes above 20,000 feet[,] . . . [can] monitor up to 65 enemies of the State simultaneously[, and] . . . can see targets from almost 25 miles down range." Predator drones can eavesdrop on electronic transmissions, and one drone unveiled at DEFCON last year can crack Wi-Fi networks and intercept text messages and cell phone conversations—without the knowledge or help of either the communications provider or the customer. Drones are also designed to carry weapons, and some have suggested that drones carrying weapons such as tasers and bean bag guns could be used domestically.

Many drones, by virtue of their design, their size, and how high they can fly, can operate undetected in urban and rural environments, allowing the government to spy on Americans without their knowledge. And even if Americans knew they were being spied on, it's unclear what laws would protect against this. As Ryan Calo, the ACLU (pdf) and many others have noted, Supreme Court case law has not been friendly to privacy in the public sphere, or even to privacy in areas like your backyard or corporate facilities that are off-limits to the public but can be viewed from above. The Supreme Court has also held that the Fourth Amendment's protections from unreasonable searches and seizures may not apply when it's not a human

that is doing the searching. None of these cases bodes well for any future review of the privacy implications of drone surveillance.

However, there are some reasons to hope that the courts will find the ability of drones to monitor our activities constantly, both in public and—through the use of heat sensors or other technology—inside our homes, goes too far. For example, in a 2001 case called *Kyllo v. United States*, the Supreme Court held the warrantless search of a home conducted from outside the home using thermal imaging violated the Fourth Amendment. The Court held that, "in the sanctity of the home, all details are intimate details"—it didn't matter that the officers did not need to "enter" the home to "see" them. *United States v. Jones*, argued before the Supreme Court this term, could also have ramifications for drones. The D.C. Circuit Court of Appeal's opinion in this case held that warrantless GPS-enabled 24/7 surveillance of a car violated the Fourth Amendment, noting, "When it comes to privacy . . . the whole may be more revealing than the parts." Though the outcome of the case at the Supreme Court is far from clear, the Court did seem surprised during oral argument that, under the government's theory of the case, the justices themselves could be tracked without a warrant and without probable cause. Drones that use heat sensors to "see" into the home and that can track one or many people around the clock wherever they go are not much different from the technologies at issue in *Kyllo* and *Jones.*

It is likely a court will be forced to address this issue in the not-to-distant future. The market for unmanned aircraft in the United States is expanding rapidly, and companies, public entities, and research institutions are developing newer, faster, stealthier, and more sophisticated drones every year. According to a July 15, 2010 FAA Fact Sheet (pdf), "[i]n the United States alone, approximately 50 companies, universities, and government organizations are developing and producing some 155 unmanned aircraft designs." According to one market research firm, approximately 70% of global growth and market share of unmanned aircraft systems is in the United States (pdf). In 2010 alone, expenditures on unmanned aircraft "reached more than US $3 billion (pdf) and constituted a growth of more than 12%." The market for these systems is only expected to increase: over the next 10 years the total expenditure for unmanned aircraft "is expected to surpass US $7 billion." And some have forecast that by the year 2018 there will be "more than 15,000 [unmanned aircraft systems] in service in the U.S., with a total of almost 30,000 deployed worldwide."

In 2011, Congress, the Defense Department, state and local governments, industry and researchers all placed significant pressure on the FAA to review and expand its current "Certificate of Authorization or Waiver (COA)" program. The FAA is also reviewing its own rules for small unmanned aircraft systems. The agency is expected to announce an expansion of the COA program this month. If it does, we may see (or be seen by) many more drones in the very near future.

EFF will keep monitoring this issue. We hope to learn from our lawsuit against the FAA which entities in the United States—whether they are government agencies, state or local law enforcement, research institutions or private companies—are currently authorized to fly drones and which entities are seeking or have been denied authorization. Once we have that information we will be better able to define the scope of the problem and can further assess and address the privacy issues at stake.

Privacy | Locational Privacy | Transparency | FOIA

Related Cases

FAA Drone Authorizations

MORE DEEPLINKS POSTS LIKE THIS

JANUARY 2012
Texas Cancels Its Drone Program For Maintenance Issues

APRIL 2012
FAA Releases Lists of Drone Certificates—Many Questions Left Unanswered

APRIL 2012

RECENT DEEPLINKS POSTS

JUN 7, 2012
World's Largest Organization for Computer Professionals Comes Out Against CISPA

JUN 7, 2012
Open Access Victory in Successful Access2Research Petition

JUN 7, 2012

Miami-Dade PD Releases Information about Its Drone Program; Will the FAA Follow Suit?

MARCH 2012

Sunshine Week: EFF's Current Freedom of Information Act Lawsuits

MAY 2012

Local Governments Have the Power to Restrict Drone Surveillance in the US

The Cybersecurity Act (S. 2105) Threatens Online Rights - a Handout for Your Senator

JUN 7, 2012

What What!: Appeals Court Affirms South Park Parody Was Obvious Fair Use

JUN 7, 2012

US Government Still Insisting It Can't Be Sued Over Warrantless Wiretapping

DEEPLINKS TOPICS

Analog Hole
Anonymity
Anti-Counterfeiting Trade Agreement
Biometrics
Bloggers Under Fire
Bloggers' Rights
Broadcast Flag
Broadcasting Treaty
CALEA
CDA 230
Cell Tracking
Coders' Rights Project
Content Blocking
Copyright Trolls
Council of Europe
Cyber Security Legislation | CISPA, SECURE IT, Cybersecurity Act
CyberSLAPP
Development Agenda
Digital Books
Digital Radio
Digital Video
DMCA
DMCA Rulemaking
Do Not Track
DRM
E-Voting Rights
EFF Europe
EFF Software Projects
FAQs for Lodsys Targets
File Sharing
FOIA
Free Speech
FTAA
Health Privacy
Hollywood v. DVD
How Patents Hinder Innovation (Graphic)
Innovation
Intellectual Property
International
International Privacy Standards
Internet Blacklist Legislation
Internet Governance Forum
Locational Privacy
Mandatory Data Retention
Mandatory National IDs and Biometric Databases
Mass Surveillance Technologies
National Security Letters
Net Neutrality
No Downtime for Free Speech
NSA Spying
OECD
Online Behavioral Tracking
Patent Busting Project
Patent Trolls
Patents
PATRIOT Act
Pen Trap
Policy Analysis
Printers
Privacy
Reading Accessibility
Real ID
RFID
Search Engines
Search Incident to Arrest
Security
Social Networks
Terms Of (Ab)Use
Test Your ISP
The Global Network Initiative
Trans-Pacific Partnership Agreement
Transparency
Travel Screening
Trusted Computing
Uncategorized
Video Games
Wikileaks
WIPO
Broadcast Flag