Policy Analysis

CATO INSTITUTE

December 13, 2016 | Number 807

Surveillance Takes Wing

Privacy in the Age of Police Drones

By Matthew Feeney

EXECUTIVE SUMMARY

Unmanned aerial vehicles, commonly referred to as "drones," are being used in a range of industries, including conservation, journalism, archeaology, and policing. (In this paper I will use the word "drone" to apply to unmanned aerial vehicles, excluding unmanned aquatic vehicles and terrestrial robots.) Law enforcement drones have clear benefits: allowing police to more easily find missing persons, suspects, and accident victims, for example. They also allow police to investigate dangerous situations such as bomb threats and toxic spills. Yet without strict controls on their use, drones could present a very serious threat to citizens' privacy.

Regrettably, while the Supreme Court has tackled privacy issues amid the emergence of new technologies, the Court's rulings on aerial surveillance are not well suited for today, now that police are using drones.

Fortunately, lawmakers at the state and federal levels can implement policies that allow police to take advantage of drones while protecting privacy. These policies should not only address familiar issues associated with searches, such as warrant requirements, but also relatively new concerns involving weaponization, biometric software, and surveillance technology. Such controls and regulations will allow police to do their job and prevent drones from being used as tools for secretive and needlessly intrusive surveillance.

Matthew Feeney is a policy analyst at the Cato Institute.

"Not only are drones becoming increasingly prevalent, they are also being increasingly used by law enforcement agencies."

INTRODUCTION

If it can happen to the vice chair of the Senate Intelligence Committee, it can happen to anyone.

Speaking as a special witness at a Senate Commerce Committee hearing in January 2014, Sen. Dianne Feinstein (D-CA) revealed that a drone had once hovered inches from her face when she approached a window at her home to observe a nearby demonstration.[1] She went on to discuss the "significant" privacy concerns associated with drones and urged her colleagues to implement "strong, binding enforceable privacy policies that govern drone operations."[2] Although Feinstein may have been exaggerating the threat of the encounter, with reports suggesting that the drone may have been a remote-controlled toy helicopter, she was nonetheless right to recognize the potential privacy threat drones represent.[3]

While there is perhaps an irony to Senator Feinstein urging "strong" privacy policies, given her strong support of the National Security Agency's (NSA) surveillance programs, her concerns about drones are well founded.[4] Not only are drones becoming increasingly prevalent, they are also being increasingly used by law enforcement agencies.[5]

Police drones do have benefits. Drones allow police to more easily find missing persons, suspects, and accident victims. They also allow police to investigate dangerous situations such as bomb threats and toxic spills. Yet without strict controls on their use, they present a very serious threat to citizens' privacy.

In that respect drones have much in common with body cameras, another promising technology that raises privacy issues. Both body cameras and drones can store video footage showing private property, accidents, and violent crime.[6]

But there are features unique to drones that deserve particular attention. Among these are the wide varieties of technology that can now (or in the not-too-distant future) be attached to drones, including thermal scanners and biometric software. In addition, the potential surveillance made possible by police body cameras pales in comparison to the persistent surveillance of entire cities that is now possible thanks to advances in drone and camera technology.

The challenge for policymakers is to balance the benefits of police drones with the privacy concerns. Regrettably, while the Supreme Court has tackled privacy issues amid the emergence of new technologies, the Court's rulings on aerial surveillance offer little reassurance at a time when police will increasingly be using drones. However, neither the states nor the federal government have to wait for the Supreme Court to sort out the challenge of applying the Fourth Amendment to new technologies.[7] By imposing warrant requirements, banning weaponization, and enforcing policies that outline public access to footage, lawmakers can provide the protection necessary against armed drones engaging in persistent and warrantless surveillance.

This study begins with a look at current drone technology and that of the near future. After examining drones' capabilities we'll look at the Supreme Court's Fourth Amendment jurisprudence, noting that it has not adequately addressed the privacy implications of aerial surveillance. Then we'll turn to a discussion of policies that would allow law enforcement to take advantage of drones while also protecting privacy.

WHAT CAN DRONES DO?

Unmanned aerial vehicles (UAVs), commonly referred to as "drones," have proven remarkably versatile in their short history. Drones have been used for building inspection, firefighting, journalism, conservation, agriculture, aid delivery, archaeology, military missions, and law enforcement, among other uses.[8]

Drones come in a wide variety of sizes and can (although sometimes not legally) carry a range of payloads, whether they are missiles, cameras, or even beer.[9] Payload capacity and range varies widely depending on the drone. Perhaps the most notorious drone, the MQ-9 Reaper, which is used for U.S. military-targeted killings and surveillance, has a payload of 3,750 pounds, enough to carry several laser-guided Hellfire missiles.[10]

The MQ-4C Triton, an unmanned military aircraft designed for maritime surveillance, is capable of staying aloft for 30 hours and traveling at around 360 mph.[11] The Triton is outfitted with a surveillance sensor capable of persistent 360-degree observation from what its developer describes as "extremely long ranges."[12] It's also around 10 feet longer than the Reaper and at takeoff can be almost 22,000 pounds heavier.[13]

Drones available to the public are not nearly as large, nor can they carry payloads as bulky as missiles and complex surveillance equipment. The Phantom 4, a popular hobby drone, comes equipped with a camera and only weighs 3 pounds.[14]

With more funds at their disposal than the average hobbyist, law enforcement agencies at the federal and state levels can purchase drones with more capabilities than amateur photography drones. Customs and Border Protection (CBP), the country's largest law enforcement agency, began using drones in 2004.[15] The CBP uses Reapers and their maritime variant, the Guardian, for border surveillance.[16] In fact, it was a CBP drone that was involved in the first reported instance of a UAV being used to aid an arrest on U.S. soil.[17]

The Federal Aviation Administration (FAA) has authorized law enforcement agencies across the country to use a wide range of drones.[18] In 2011 the Arlington, Texas, police department got FAA approval to fly the Leptron Avenger, an 11-pound helicopter that can carry cameras and is equipped with autopilot.[19] In 2008 the FAA also authorized the Miami-Dade police department to test a T-Hawk, an aerial surveillance drone used by the U.S. military that weighs 16 pounds and is capable of reaching speeds of 45 mph.[20]

The types of surveillance equipment that can be attached to police drones make them potentially much more intrusive than hobbyist drones. Relatively small drones can carry thermal scanners and biometric tools not available to the public.[21] As these tools continue to improve they're likely to pose more significant privacy concerns.

One of the tools already with us allows a single drone to carry out the detailed and persistent surveillance of an area the size of a small city. In 2009 a Black Hawk helicopter successfully tested the Autonomous Real-Time Ground Ubiquitous Surveillance Imaging System (ARGUS-IS), a surveillance technology designed by BAE Systems.[22] The ARGUS-IS, whose acronym is derived from the mythical Greek 100-eyed giant, collects data from hundreds of cameras, each of which can capture 5 million pixels.[23] When put together the amalgamated image is 1.8 billion pixels and provides the observer with a view of up to 25 square kilometers.[24] This image is highly detailed, allowing ARGUS-IS users to see six-inch details from 20,000 feet.[25]

Another video technology that allows for widespread mass aerial surveillance is Gorgon Stare, the first iteration of which clocked more than 10,000 hours worth of combat support missions in Afghanistan while attached to Reaper drones.[26] This version of Gorgon Stare could keep about 16 square kilometers under surveillance.[27] In July 2014 the Sierra Nevada Corporation announced that Gorgon Stare had incorporated ARGUS-IS technology, thereby reportedly allowing for the surveillance of 100 square kilometers.[28]

American companies are also developing drones capable of staying aloft for extended periods. In 2014 Google bought Titan Aerospace, which was developing jet-sized drones capable of staying airborne for years.[29] In June 2016 Facebook successfully tested Aquila, an Internet-delivery drone with the wingspan of a Boeing 737.[30] Aquila will be solar powered and will reportedly be able to stay airborne for three to six months.[31] If combined with tools such as ARGUS-IS, these drones would allow for the kind of persistent snooping which, until recently, was reserved to the imagination of dystopian science fiction writers.

Of course, budget constraints make it unlikely that local police departments will be attaching surveillance equipment like ARGUS-IS or Gorgon Stare to huge solar-powered drones any time soon. A police department would have to be very well funded to use this kind of wide-area surveillance equipment attached to a

"The types of surveillance equipment that can be attached to police drones make them potentially much more intrusive than hobbyist drones."

> "We shouldn't be in any doubt that police will seize the opportunity to use affordable persistent surveillance tools on drones."

drone.[32] Indeed, according to Benjamin Miller, the unmanned aircraft program manager with the Mesa County, Colorado, sheriff's office, hours of persistent tracking with law enforcement drones is not affordable.[33]

But there is still cause for concern. Persistent Surveillance Systems (PSS), an unambiguously named company that makes surveillance tools, has shown off its cameras to police in Baltimore, Philadelphia, Dayton, and Compton.[34] The cameras, which are attached to manned aircraft, are not as powerful as ARGUS-IS. From about 10,500 feet above the ground, a person takes up only one pixel in an image that covers nearly 65 square kilometers.[35] Nonetheless, this bulky camera system, which weighs 137 pounds, is more affordable than military-grade surveillance systems, with PSS typically charging $1,500-$2,000 per hour.[36] While too heavy for many police drones, we shouldn't be in any doubt that police will seize the opportunity to use affordable persistent surveillance tools on drones. When speaking about the PSS aerial surveillance system in 2014, Dayton, Ohio, police chief Richard Biehl made it clear that he wants the pubic to feel watched, saying, "I want them to be worried that we're watching . . . I want them to be worried that they never know when we're overhead."[37]

Budgetary constraints might put Gorgon Stare beyond the reach of the Dayton, Ohio, police department, but the Department of Homeland Security (DHS), with its multibillion-dollar budget, has demonstrated an interest in military mass surveillance technology, despite the fact that its track record with drones is hardly an example of government efficiency.[38] In spite of access to funds for Reaper drones, a DHS Office of Inspector General audit found that the Customs and Border Protection's drone program did not achieve its expected results and "found little or no evidence" that the drones' flight missions had reduced the cost of border surveillance, improved efficiency, or increased apprehensions.[39]

Large drones aren't the only ones that ought to worry privacy advocates. Drones the size of small birds are capable of conducting surveillance. The AeroVironment Nano Hummingbird, funded by the Pentagon's Defense Advanced Research Projects Agency (DARPA), has a wingspan of only 6.5 inches and is equipped with a camera.[40] A smaller drone, the Black Hornet Nano Unmanned Air Vehicle, is only 4 inches long, can travel at 22 mph, and has been used by the British military to spot enemy snipers.[41] Drones the size of insects already exist, and we should expect surveillance equipment to be attached to such drones as technology improves.[42]

The sort of ubiquitous surveillance large and small drones may soon make possible would, one would think, implicate Americans' Fourth Amendment rights to be free from unreasonable searches. Unfortunately, Supreme Court rulings regarding the Fourth Amendment are not reassuring in the age of the drone.

THE FOURTH AMENDMENT AND DRONES

The Fourth Amendment, the U.S. Constitution's core guarantee of privacy and protection against warrantless surveillance, reads as follows:

> The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.[43]

The Supreme Court has addressed Fourth Amendment privacy questions raised by new technologies such as GPS locators, thermal scanners, and smartphones. However, the Court has yet to tackle the Fourth Amendment questions raised by the emergence of drones. Given drones' surveillance capabilities, it's worth examining the state of Fourth Amendment doctrine, which, although oftentimes unsatisfying, can nonetheless be improved by lawmakers.

One of the most important and influential Fourth Amendment doctrines is the "reasonable expectation of privacy" test, which was

promulgated in *Katz v. United States* (1967).[44] In *Katz*, the Court ruled that Charles Katz's Fourth Amendment rights had been violated when agents with the Federal Bureau of Investigation (FBI)—absent a warrant—attached an eavesdropping device to the outside of a public telephone booth Katz used to communicate illegal wagers across state lines.[45]

In a concurring opinion, Justice Harlan devised the two-part reasonable expectation of privacy test adopted by courts since as the prevailing doctrine for determining whether government agents have conducted a Fourth Amendment search.[46] Harlan wrote that a Fourth Amendment search occurs if state actors violate "an actual (subjective) expectation of privacy and [. . .] that the expectation be one that society is prepared to recognize as 'reasonable.'"[47]

At first glance this reasonable expectation of privacy test might look attractive, but it has many problems. The test is circular; after all, citizens' expectations of privacy are determined by court rulings, which are based on citizens' expectations, which in turn are determined by court rulings.[48] Aside from the test's circularity problem, it has been used by the Court to reach decisions not conducive to strong privacy protections.

One of the Fourth Amendment cases most relevant to drones, *California v. Ciraolo* (1986), which relied heavily on the reasonable expectation of privacy test, sets a worrying precedent for privacy advocates amid the proliferation of drones.[49] In a 5–4 decision the Court ruled that Santa Clara police officers, acting on an anonymous tip, did not need a warrant to use an airplane flying at 1,000 feet to look for marijuana plants in Dante Ciraolo's backyard. Having seen marijuana in the backyard from the plane, officers secured a search warrant and arrested Ciraolo, who pleaded guilty to the cultivation of marijuana.[50]

Despite the fact that, like homes, backyards have long been recognized as constitutionally protected areas, the Court held that the search did not violate Ciraolo's reasonable expectation of privacy. "We readily conclude that respondent's expectation that his garden was protected from such observation is unreasonable and is not an expectation that society is prepared to honor," Chief Justice Burger wrote.[51] Never mind that a 6-foot and 10-foot fence surrounded Ciraolo's yard, an indication that he at least expected that the contents of his yard would be private.

According to Burger, the fact that a policeman standing on a double-decker bus or a truck could perhaps have seen over the 10-foot fence made it unclear whether Ciraolo "manifested a subjective expectation of privacy from all observations of his backyard."[52]

In a similar case, *Florida v. Riley* (1989), decided a few years after *Ciraolo*, a plurality of the Supreme Court found that a Pasco County, Florida, police officer did not need a warrant to surveil a suspected marijuana grower's property from a helicopter flying at 400 feet.[53] In his dissent, Justice Brennan provided a hypothetical case that seems all too real today:

> Imagine a helicopter capable of hovering just above an enclosed courtyard or patio without generating any noise, wind, or dust at all—and, for good measure, without posing any threat of injury. Suppose the police employed this miraculous tool to discover not only what crops people were growing in their greenhouses, but also what books they were reading and who their dinner guests were. Suppose, finally, that the FAA regulations remained unchanged, so that the police were undeniably "where they had a right to be." Would today's plurality continue to assert that '[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures' was not infringed by such surveillance?[54]

Today, devices resembling this "miraculous tool" are routinely available to law enforcement. Such tools pose privacy risks more intrusive than the thought-police helicopters in George Orwell's novel *1984*, which were used to peep into people's windows. With today's surveillance technology police drones can be much more intrusive and stealthy than helicopters.

"In a 5–4 decision the Court ruled that Santa Clara police officers, acting on an anonymous tip, did not need a warrant to use an airplane flying at 1,000 feet to look for marijuana plants in Dante Ciraolo's backyard."

> "In the age of the drone, the *Riley*, *Ciraolo*, and *Dow Chemical* line of cases allows police a great deal of latitude when it comes to aerial surveillance."

A number of legal scholars have proposed legislative measures designed to provide protection from Brennan's "miraculous" tools. Troy Rule, a professor at Arizona State University's Sandra Day O'Connor College of Law, has proposed legislation allowing citizens the right to exclude drones 500 feet above the surface of their property in most locations.[55] Pepperdine's Gregory McNeal has argued that lawmakers should extend property owners' airspace rights so that they can exclude "aircraft, persons, and other objects" from a column of airspace up to 350 feet above the ground.[56]

However, even those reforms wouldn't address all privacy concerns. After all, the searches in *Ciraolo* and *Riley* were carried out with the naked eye at 1,000 feet and 400 feet, respectively. Even without powerful zoom lenses, such searches proved to be revealing.

In *Dow Chemical Co. v. United States*, decided the same year as *Ciraolo*, the Court suggested that aerial surveillance with "sophisticated technology" should not be treated the same as naked-eye surveillance. [57] A 5–4 majority in that case held that the Environmental Protection Agency did not need a warrant when it employed a photographer using a precision mapping camera to inspect a 2,000 acre chemical plant from the air. In his majority opinion, Chief Justice Burger remarked, "It may well be [...} that surveillance of private property by using highly sophisticated surveillance equipment not generally available to the public, such as satellite technology, might be constitutionally proscribed absent a warrant. But the photographs here are not so revealing of intimate details as to raise constitutional concerns."[58] Despite finding warrantless aerial surveillance in the *Ciraolo* and *Dow Chemical* cases constitutional, Burger was clearly skeptical of such searches being carried out with "highly sophisticated surveillance" tools. Today's Justices may well express similar skepticism if a case concerning sophisticated aerial surveillance technology makes its way before the Court.

In the age of the drone, the *Riley*, *Ciraolo*, and *Dow Chemical* line of cases allows police a great deal of latitude when it comes to aerial surveillance. However, a more recent Supreme Court case shows that some Justices are prepared to rethink Fourth Amendment doctrine at a time when technology makes long-term surveillance much easier than it used to be.

In *United States v. Jones* (2012) the Supreme Court unanimously ruled that fixing a GPS locator to a car and using the locator to track the car's public movements constitutes a search.[59] In *Jones*, police officers attached a GPS locator to a car belonging to the wife of a suspected drug trafficker, Antoine Jones, and monitored its position 24 hours a day for four weeks, producing more than 2,000 pages of data.[60] The GPS locator was installed pursuant to a warrant requiring that the locator be installed in Washington, D.C., within 10 days.[61] The locator was attached to the car in Maryland on the 11th day, thus outside the scope of the warrant. The District Court, which sentenced Jones to life imprisonment, suppressed only GPS data collected while the car was at Jones' residence, arguing that he did not have a reasonable expectation of privacy while he was driving on public streets. The Court of Appeals for the D.C. Circuit reversed the conviction, and the Supreme Court took up the case to resolve the disagreement.

While the justices were unanimous in deciding that police officers had carried out a Fourth Amendment search, they arrived at their decisions for different reasons. Justice Scalia, who delivered the opinion of the Court, wrote that the government "physically occupied private property for the purpose of obtaining information. We have no doubt that such a physical intrusion would have been considered a 'search' within the meaning of the Fourth Amendment when it was adopted."[62]

Justice Alito, in a concurring opinion joined by Justices Breyer, Kagan, and Ginsburg, wrote that Scalia's holding "strains the language of the Fourth Amendment."[63] Alito evaluated the question presented to the Court by "asking whether respondent's reasonable expectations of privacy were violated by the long-term monitoring of the movements of the vehicle he drove."[64] Alito's concurrence raises doubts about the continuing vitality of the reasonable

expectation of privacy test at a time when technology allows for the long-term observation of public behavior.[65]

It's not hard to see how a picture created with observations of individual movements, none of them "private," is more than the sum of its parts. A man has no reasonable expectation of privacy when he buys flowers from a store. He is in plain view of anyone who might pass by the store. The same man has no reasonable expectation of privacy when he picks up a young woman from a sidewalk downtown. After all, he and the woman are in public spaces. They are also in public spaces when they drive to a nearby motel. The next morning, when the man drives back to the home he shares with his wife, he is also almost exclusively in public and does not have a reasonable expectation of privacy. These incidents (buying the flowers, driving to the motel, etc.) by themselves are not indicative of much at all. When put together into a "mosaic," a rather different picture emerges.

Like the cheating husband, Jones was mostly driving on public roads and did not have a reasonable expectation of privacy while doing so. However, prolonged surveillance of activities in public can reveal intimate and private details. Under the so-called "mosaic theory" of the Fourth Amendment, the observation of a collection of public activities ultimately constitutes a search.[66] This approach differs from the traditional "sequential approach" to the Fourth Amendment, which involves a step-by-step examination of government activity in order to determine if any of these steps are Fourth Amendment searches or seizures.[67] Under the sequential approach, an officer inserting a key into a home and opening the door would be analyzed as two events: the insertion of the key and the opening of the door.[68]

Adoption of the mosaic theory would have a significant impact on when police would need a warrant before using a drone. Under that approach, police would have to request a warrant to observe an individual for days, weeks, or perhaps months with a drone, even if that individual was tracked only in areas where he or she had no reasonable expectation of privacy.

Justice Sotomayor's separate concurrence signaled sympathy to the mosaic theory. Noting the vast amount of data created by GPS locators, Sotomayor wrote, "I would take these attributes of GPS monitoring into account when considering the existence of a reasonable societal expectation of privacy in the sum of one's public movements. I would ask whether people reasonably expect that their movements will be recorded and aggregated in a manner that enables the Government to ascertain, more or less at will, their political and religious beliefs, sexual habits, and so on."[69]

Still, the mosaic theory is not without problems.[70] How is a judge supposed to determine when a mosaic has been made and which tiles constitute its parts? A judge who adheres to the mosaic theory would be put in the unenviable position of analyzing the metaphysics of events, determining when one event finishes and another begins, as well as when the observation of public events becomes a Fourth Amendment search.

Alito treated that problem dismissively in his *Jones* concurrence: "We need not identify with precision the point at which the tracking of this vehicle became a search, for the line was surely crossed before the 4-week mark."[71] But it's not clear why the line was crossed before police collected four weeks' worth of GPS location data. Why not three weeks, 12 days, or 40.3 hours?

George Washington University law professor Orin Kerr, a mosaic theory skeptic, has identified an additional problem posed by tracking devices turned off at regular intervals: "Imagine the police use a GPS device that is programmed to turn on and record the location of the car for only one hour a day. The device is otherwise dormant. If the police monitor that device over twenty-eight days, does that count as twenty-eight days of monitoring? Or is that only twenty-eight hours of monitoring?"[72]

On the other hand, this sort of judicial inquiry is hardly unique. Judges regularly have to consider when prolonged activities in public, which in isolation are harmless, become illegal. Walking quietly 15 feet behind someone on a public sidewalk for one block is hardly stalking, but it begins to look nefarious when that be-

"It's not hard to see how a picture created with observations of individual movements, none of them 'private,' is more than the sum of its parts."

"Clearly, current Fourth Amendment Supreme Court doctrine is underdeveloped and inadequate to the challenges presented by drones and other emerging technologies."

havior continues for miles and over significant periods of time. Although Justice Alito did not specify how long police could track someone without a warrant, his concurrence caused such a stir at the FBI that, according to the agency's then-general counsel, almost 3,000 GPS tracking devices were turned off.[73]

Clearly, current Fourth Amendment Supreme Court doctrine is underdeveloped and inadequate to the challenges presented by drones and other emerging technologies.[74] Georgetown University law professor Randy Barnett argues that the NSA's bulk collection of telephone metadata is the modern equivalent of the kind of general warrant that concerned the Founders.[75] According to Barnett, the reasonable expectation of privacy test needs to be revised at a time when the kind of bulk collection used by the NSA is possible. Bruce Schneier, a fellow at the Berkman Center for Internet and Society at Harvard Law School, agrees, arguing that in an age of significant technological advances, the reasonable expectation of privacy test will leave us with no privacy.[76] In the meantime, state and federal lawmakers should take it upon themselves to provide more privacy than the Supreme Court's aerial surveillance rulings and tackle the challenging task of allowing law enforcement to effectively use drones without threatening privacy.

LAWMAKERS CAN PROVIDE INCREASED PRIVACY PROTECTIONS

Lawmakers don't have to wait for the Supreme Court to reconsider aerial surveillance. They can pass legislation that protects privacy amid the rise of police drones. In fact, lawmakers have been urged to take this approach by at least one current Supreme Court Justice. In his *Riley v. California* (2014) concurrence, Justice Alito argued that legislatures are better positioned than courts to address privacy issues posed by new technology:

> Many forms of modern technology are making it easier and easier for both government and private entities to amass a wealth of information about the lives of ordinary Americans, and at the same time, many ordinary Americans are choosing to make public much information that was seldom revealed to outsiders just a few decades ago.
>
> In light of these developments, it would be very unfortunate if privacy protection in the 21st century were left primarily to the federal courts using the blunt instrument of the Fourth Amendment. Legislatures, elected by the people, are in a better position than we are to assess and respond to the changes that have already occurred and those that almost certainly will take place in the future.[77]

Lawmakers should take Alito's comments seriously and address the issues raised by drones head on rather than wait for Supreme Court rulings. The most pressing issues concern surveillance, data retention, warrant requirements, and weaponization.

Surveillance Equipment

Some law enforcement agencies use facial recognition technology, but facial characteristics are not our only identifiers.[78] We all have a host of unique features, such as irises, ears, noses, and vein patterns, all of which drone pilots could use to identify people with ease in the near future.[79]

Drones can already be programmed to recognize and track people.[80] Such capabilities are worrying enough when used by ARGUS-IS, which can automatically track moving objects, but the concerns are more pronounced when you consider tracking software on smaller and more nimble drones. Because of the rapid nature of technological change, hummingbird drones programmed to identify protesters, gun owners, mosque congregations, or visitors to abortion clinics are reasonable concerns, not paranoid fantasies.

Unless the Supreme Court revisits Fourth Amendment doctrine, whether police use of biometric software constitutes a search will depend on whether the subject has a reason-

able expectation of privacy. In 2012 testimony before a Senate judiciary subcommittee, Duke Law School professor Nita Farahany noted, "as a general matter, law enforcement use of [facial recognition technology] is not, in itself, a Fourth Amendment search, let alone an unreasonable one."[81] Moreover, courts would reject a man's claim that he had a reasonable expectation of privacy in "his personal identity associated with his facial features."[82] Similar arguments could be made for the features of that man's ears or the details of his irises.

In the face of current Fourth Amendment doctrine and advances in technology, state and federal lawmakers should restrict the use of biometric software on police drones. Doing so would limit the growth of a surveillance infrastructure that poses a risk to citizens' privacy.

Images of millions of citizens can be analyzed with facial recognition tools. According to a May 2016 Government Accountability Office report, the FBI has access to more than 411 million facial images, including driver's license photos from 16 states as well as visa application and passport photos from the State Department.[83] The same report stated that the FBI should "better ensure accuracy and privacy," finding that the FBI did not complete required privacy reports in a timely manner or adequately determine the accuracy of the facial recognition systems it and its external partners use.[84]

As biometric software improves and the number of images law enforcement can access grows, the risk of abuse will increase. That risk is especially pronounced considering that in 2016 the FBI requested that its Next Generation Identification (NGI) system (which uses iris scan, fingerprint, and facial recognition technology) be exempt from provisions of the Privacy Act.[85] The law requires that the FBI provide individuals with information about data it has on them and ensure NGI data is accurate.[86] Some state and local law enforcement agencies have access to the NGI's Interstate Photo System, which includes 30 million photos of almost 17 million people.[87] More than 80 percent of these images are photos "submitted as part of a lawful detention, an arrest, or incarceration," such as mug shots.[88] However, because not everyone who is arrested is later convicted, innocent people's photos are part of the NGI's Interstate Photo System.

In order to protect innocent people's privacy, state and federal lawmakers should pass laws that allow police drone footage to be analyzed with biometric software only if two conditions are met: 1) that biometric software is used exclusively in violent crime investigations, and 2) that biometric databases only include information related to citizens with a violent crime conviction.[89] These conditions would limit police use of biometric technology to investigations of the most serious crimes and preclude its employment to identify citizens engaged in lawful activity. They would also prevent law enforcement agencies from collecting innocent people's biometric data.

Biometric software is not the only surveillance tool available to the police. Thermal scanners employing infrared radiation analysis allow users to see body heat. Thermal scanners on drones should only be used for searches that are either pursuant to a warrant or for suspects and missing persons. Thermal scanning technology is sometimes used for these purposes from airplanes and helicopters, and it's reasonable for police to look to drones in such situations, given that drones are cheaper and easier to operate than manned aircraft. Fortunately, the Supreme Court ruled in *Kyllo v. United States* (2001) that police officers cannot use thermal scanners to search houses without a warrant.[90]

Footage Retention and Release

Few law enforcement operations legitimately require police drones to be routinely equipped with sophisticated surveillance tools. However, most police drone operations will involve drones equipped with cameras, which raises questions about what kind of drone footage should be made public.

Police departments and lawmakers have dealt with the privacy issues associated with cameras before. The most recent example of this can be seen in the ongoing debates over body cameras, and in some instances the best

"In the face of current Fourth Amendment doctrine and advances in technology, state and federal lawmakers should restrict the use of biometric software on police drones."

"A warrant requirement for drone surveillance will help guard against drone fleets carrying out persistent and indiscriminate surveillance of entire towns and cities."

practices for police body cameras can also be applied to cameras on drones.[91] In order to promote increased accountability and transparency while protecting privacy, lawmakers ought to consider legislation that allows for the public to request drone footage, but only under a narrow set of circumstances.

Citizens and journalists should only be able to access drone footage of events that are of public interest, such as arrests and use-of-force incidents. The public should not be able to access footage of an area where the subject expected privacy without the subject's permission. Footage of living rooms, bedrooms, and other intimate areas can reveal information homeowners want to keep private. Lawmakers at the state and local level can look to body camera policies for guidance in this area. For example, Washington, D.C.'s police body camera policy allows subjects to view body camera footage of themselves.[92] Members of the public seeking D.C., police body camera video can request footage in which they don't appear via the District of Columbia Freedom of Information Act, although officials can exempt such footage from release if it reveals "information of a personal nature."[93] Such a policy governing police drone footage will prevent nosy neighbors from accessing video of a Special Weapons and Tactics (SWAT) raid on their block. It also allows the targets of raids and their attorneys to access the relevant footage, thereby protecting privacy while increasing police accountability and transparency.

Police retention of footage should also be addressed. Drone footage that does not include information related to an arrest, a use-of-force incident, a search, or a police encounter under investigation should be deleted after 90 days. This would allow police departments to free up data storage space and provide citizens with time to consider a complaint and to seek legal advice before requesting the footage.

Footage of an arrest, a search, a use-of-force incident, or an incident under investigation should be kept longer. Keeping this footage for three years, for instance, would ensure the preservation of data related to issues of public interest and make it easier for journalists, attorneys, and investigators to find out if alleged misconduct is an isolated incident or part of a trend.

Require Warrants for Drone Surveillance

Some lawmakers have proposed drone legislation that grants citizens more privacy protections than the *Ciraolo* and *Riley* decisions. The Oklahoma House of Representatives passed a bill in March 2016 requiring that police not only secure a warrant before using a drone, but also that the officers show that "alternative methods of data collection are either cost-prohibitive or present a significant risk to any person's bodily safety."[94]

Proposed drone legislation in New Hampshire includes a warrant requirement. The bill also states that individuals have an expectation of privacy on private property where they are not observable at ground level, "regardless of whether he or she is observable from the air."[95] Identical language can be found in Florida statutes.[96]

If the Oklahoma and New Hampshire bills are passed they will join laws in states such as Montana, Florida, Indiana, Iowa, Tennessee, Idaho, Texas, Utah, Illinois, Virginia, Oregon, and Wisconsin, which also impose warrant requirements on police drones.[97]

There are, of course, situations where a police drone would be useful but would not be taking part in a Fourth Amendment search. If a hiker gets lost in the desert or a child is swept out to sea, a drone is an ideal tool for finding the missing person. In these situations a warrant is not necessary under current law, nor should it be.

A warrant requirement for drone surveillance will help guard against drone fleets carrying out persistent and indiscriminate surveillance of entire towns and cities. The cost of such observation makes it unlikely that a state or local police department would be able to use mass persistent surveillance systems discussed above, but persistent surveillance need not involve military-grade snooping tools. Police could treat drones like police cruisers, flying up and down streets on the lookout for crime, understandably prompting a sense of unease among citizens who may come

to feel as if they are under the ever-watchful eyes of the authorities.

This is an especially acute concern considering that police have already shown an interest in persistent snooping. In August 2016 reporting revealed that Baltimore police had been testing aerial persistent surveillance equipment in secret for months thanks to a donation from a billionaire couple.[98] The technology, designed by Persistent Surveillance Systems, was used without warrants.

Warrant requirements combined with a policy that only allows for the release of a narrow category of footage should reassure privacy advocates. Such policies will promote accountability and transparency while preventing police from using drones for warrantless or persistent surveillance.

Lawmakers should also aim to increase transparency by mandating that police departments release information about drone flights. Police departments using drones should be required by law to periodically publish information about what kind of drones they use, how many drones the department has, how often the drones were deployed, what kind of operations the drones were used for (searches, missing persons, etc.), and the total flight hours.

Weaponization

The American military regularly uses drones to carry out targeted strikes and surveillance in Somalia, Yemen, Pakistan, and Afghanistan as part of the ongoing War on Terror. While discussions about weaponized drones usually focus on events in foreign countries, military technology developed for use on foreign battlefields often has a way of migrating home.

Concern over domestic weaponized drones achieved nationwide attention in March 2013 when Sen. Rand Paul (R-KY) filibustered the nomination of John Brennan, President Obama's pick for CIA director.[99] In his almost 13-hour filibuster, Paul demanded to know whether Obama believed he had the authority to order a drone strike against an American not engaged in combat on American soil, something then attorney general Eric Holder had earlier ruled out except in an "extraordinary circumstance" such as an attack similar to 9/11 or Pearl Harbor:

> It is possible, I suppose, to imagine an extraordinary circumstance in which it would be necessary and appropriate under the Constitution and applicable laws of the United States for the President to authorize the military to use lethal force within the territory of the United States. For example, the President could conceivably have no choice but to authorize the military to use such force if necessary to protect the homeland in the circumstances of a catastrophic attack like the ones suffered on December 7, 1941, and September 11, 2001.[100]

After the filibuster, Holder wrote to Paul, saying that the president does not have the authority to order a drone strike against an American not engaged in combat on American soil.[101]

Even so, law enforcement agencies across the country have demonstrated a willingness and eagerness to use technology designed for the military. In fact, the use of military equipment is encouraged; law enforcement agencies that receive military equipment from the Department of Defense are required to use it for law enforcement activities within a year of acquisition.[102]

That trend toward police militarization is long-standing and well documented. It's evident in the increased use of Mine-Resistant Ambush Protected vehicles (MRAPs), flash-bang grenades, battle dress uniforms, and in the widespread deployment of SWAT teams.[103]

In July 2016 police in Dallas, Texas, took an unprecedented step, using explosives attached to a bomb disposal robot to kill a barricaded suspect.[104] Police have also shot weapons from helicopters.[105] At a time when police have fired weapons from the air and have used a robot to kill a suspect, it's worth asking if there is a substantial difference between a police officer firing a weapon from a helicopter and that same officer remotely shooting a weapon attached to a drone.

Several of the states that have considered the issue have rejected weaponized drones. Law-

"At a time when police have fired weapons from the air and have used a robot to kill a suspect, it's worth asking if there is a substantial difference between a police officer firing a weapon from a helicopter and that same officer remotely shooting a weapon attached to a drone."

> "The fact that supposedly nonfatal weapons can sometimes be deadly is one reason why lawmakers at the federal and state levels should ban nonlethal as well as lethal weapons on law enforcement drones."

makers in Tennessee debated and ultimately rejected a proposal that would have allowed police to use weaponized drones.[106] A similar bill was introduced to the South Carolina House of Representatives' judiciary committee in late 2015.[107] Laws in Virginia and Oregon ban weapons being attached to police drones.[108] Florida law, however, explicitly defines law enforcement drones as devices that "can carry a lethal or nonlethal payload."[109] Police departments across the U.S. deal with a range of different crime patterns and concerns, and there are situations where a weaponized drone may seem appropriate. Nonetheless, police drones should not be equipped with lethal or nonlethal weapons.

It is important to remember that nonlethal weapons can sometimes be lethal. In 2015 alone, Tasers, which are designed to subdue uncooperative suspects, caused dozens of deaths in police encounters with citizens.[110] The fact that supposedly nonfatal weapons can sometimes be deadly is one reason why lawmakers at the federal and state levels should ban nonlethal as well as lethal weapons on law enforcement drones.

Moreover, armed drones can be knocked down, either deliberately or accidently, and present a threat on the ground. It would be dangerous if a drone outfitted with tear gas and lethal weapons were to crash or be brought down thanks to citizen interference. Perhaps more worrying, hackers could target a weaponized drone.[111]

Under the theory that "it takes a good guy with a drone to take down a bad guy with a drone," some law enforcement officials have argued that weaponized UAVs are necessary to counter potential threats from private drones. For example, Berlin, Connecticut, police chief Paul Fitzgerald has said that police might need weaponized drones to deal with citizens arming their own drones: "If someone were to put an explosive on a drone and say, 'I'm going to crash it into an aircraft in the Northeast,' . . . what does law enforcement do in a situation like that?"[112]

Still, Fitzgerald himself admitted the scenario was far-fetched. Even in the unlikely event that drones carrying bombs became a regular threat, there are ways to meet this threat without weaponizing drones.

Tools currently exist that allow users to halt intrusive or dangerous drones from up to six miles away.[113] These tools, referred to as death rays, can be pointed at errant drones and block signals from their operators. Anti-drone net guns can also be used to take down dangerous drones.[114] Positioning these tools on the perimeters of airports, where bomb-laden drone attacks are the most feasible, would help deter drone bombings.[115] Drone manufacturers can also play a role in preventing such attacks. At least one drone manufacturer has installed software that automatically grounds drones that approach airports.[116] Even when assuming the possibility of "far-fetched" scenarios, it's far from clear that weaponized drones are the best response.

Fortunately, the law enforcement community has not strongly pushed for armed drones. While testifying before the Senate Judiciary Committee, Benjamin Miller, the unmanned aircraft program manager with the Mesa County, Colorado, sheriff's office, said that it would absolutely not be appropriate for drones to be equipped with lethal weapons.[117] Miller was also skeptical of drones using nonlethal weapons: "In our experience, considering the risks of unmanned aircraft and then also the risks of use of less-than-lethal munitions [. . .] combining those two risks together is probably not the most responsible thing to do."[118]

Drones can play a valuable role when police are searching for a suspect or missing person, covering areas of treacherous terrain faster than officers on foot. Drones have also surveyed dangerous areas, such as property barricaded by armed suspects, and can inspect suspicious packages.[119] It is these kinds of operations where police drones can be the most useful, and they do not require weapons.

CONCLUSION

Drones are an exciting technology and will undoubtedly have a lasting and positive impact on a range of industries such as photography, farming, archaeology, engineering, filmmaking, journalism, and many other areas.

Law enforcement also stands to benefit from drone technology; however, as drone technology continues to improve the risk of intrusive surveillance grows and continued vigilance will be necessary. The Supreme Court can, if the right case emerges, revisit aerial surveillance, but until it does it's up to the states to pass drone policies that protect privacy while increasing police transparency and accountability.

These policies should not only address familiar issues associated with searches, such as warrant requirements and video recording, but also relatively new concerns involving weaponization, biometric software, and surveillance technology. With the right controls in place, police drones can serve legitimate law enforcement goals without becoming tools of unnecessary and intrusive surveillance.

NOTES

1. Kathryn A. Wolfe, "Feinstein: Drone Inches from Face," *Politico*, January 15, 2014, http://www.politico.com/story/2014/01/senator-dianne-feinstein-encounter-with-drone-technology-privacy-surveillance-102233.

2. Ibid.

3. Philip Bump, "Was the Drone That Scared Feinstein at Her House This Tiny Pink Helicopter?," *The Wire*, January 15, 2014, http://www.thewire.com/politics/2014/01/was-drone-feinstein-encountered-her-house-tiny-pink-helicopter/357061/.

4. It was Feinstein who said of the National Security Agency's telephone metadata collection program, "It's not a surveillance program, it's a data-collection program." Kate Tummarello, "Feinstein Blasts Critics of NSA Phone Program," *The Hill*, May 18, 2014, http://thehill.com/policy/technology/206434-a-surveillance-program-or-not.

5. Kelsey D. Atherton, "The FAA Says There Will Be 7 Million Drones Flying over America by 2020," *Popular Science*, March 24, 2016, http://www.popsci.com/new-faa-report-stares-in-face-drone-filled-future. See the ACLU "Domestic Drones" page, which states, "U.S. law enforcement is greatly expanding its use of surveillance drones." American Civil Liberties Union, "Domestic Drones," https://www.aclu.org/issues/privacy-technology/surveillance-technologies/domestic-drones.

6. Matthew Feeney, "Watching the Watchmen: Best Practices for Police Body Cameras," Cato Institute Policy Analysis no. 782, October 27, 2015, http://www.cato.org/publications/policy-analysis/watching-watchmen-best-practices-police-body-cameras.

7. U.S. Const. amend. IV.

8. For the various ways drones are used, see, for example, Rae Johnston, "Australian Architects Are Using Drones for Building Inspections," *Gizmodo Australia*, May 31, 2016, http://www.gizmodo.com.au/2016/05/australian-architects-are-using-drones-for-building-inspections/; Newley Purnell and Jack Nicas, "Chinese Drone Maker Plows into Agriculture," *Wall Street Journal*, November 26, 2015, http://www.wsj.com/articles/chinese-drone-maker-plows-into-agriculture-1448573490; Christina Beck, "Archeol ogists Find Massive Monument in Petra, Jordan," *Christian Science Monitor*, June 10, 2016, http://www.csmonitor.com/Science/2016/0610/Archeologists-find-massive-monument-in-Petra-Jordan; Kelsey D. Atherton, "Manchester Firemen Use Drones with Infrared Cameras to Fight Fires," *Popular Science*, October 14, 2015, http://www.popsci.com/manchester-firemen-use-drones-with-infrared-cameras; Benjamin Mullin, "Why 2016 Could Be a Breakout Year for Drone Journalism," *Poynter*, January 11, 2016, http://www.poynter.org/2016/why-2016-could-be-a-breakout-year-for-drone-journalism/390386/; Olivia Bailey, "Conservation Drone Reveals Uncharted Seagrass Habitat in Cambodia," *Phys.org*, May 26, 2016, http://phys.org/news/2016-05-drone-reveals-uncharted-seagrass-habitat.html; and Rohini Nambiar, "How Rwanda Is Using Drones to Save Millions of Lives," CNBC, May 27, 2016, http://www.cnbc.com/2016/05/27/how-rwanda-is-using-drones-to-save-millions-of-lives.html.

9. Liz Fields, "FAA Slaps Down Drone Beer Delivery Service to Ice Fishermen," *ABC News*, January 31, 2014, http://abcnews.go.com/US/faa-slaps-drone-beer-delivery-service-ice-fishermen/story?id=22314625.

10. United States Air Force, "MQ-9 Reaper," September 23, 2015, http://www.af.mil/AboutUs/FactSheets/Display/tabid/224/Article/104470/mq-9-reaper.aspx.

11. Naval Air Systems Command, "MQ-4C Triton," http://www.navair.navy.mil/index.cfm?fuseaction=home.displayPlatform&key=F685F52A-DAB8-43F4-B604-47425A4166F1.

12. Northrup Grumman, "AN/ZPY-3 Multi-Function Active Sensor (MFAS)," http://www.northropgrumman.com/Capabilities/mfas/Pages/default.aspx.

13. United States Air Force, "MQ-9 Reaper"; and Naval Air Systems Command, "MQ-4C Triton."

14. DJI, "Phantom 4," https://www.dji.com/product/phantom-4/info.

15. U.S. Customs and Border Protection, "Concept of Operations for CBP's Predator B Unmanned Aircraft System: Fiscal Year 2010 Report to Congress," June 29, 2010, https://www.eff.org/document/customs-border-protection-2010-drone-concept-operations-report-congress; Jennifer Lynch, "Customs & Border Protection Logged Eight-Fold Increase in Drone Surveillance for Other Agencies," Electronic Frontier Foundation, July 3, 2013, https://www.eff.org/deeplinks/2013/07/customs-border-protection-significantly-increases-drone-surveillance-other; Shawn Musgrave, "The US Spent $360 Million on Border Drones Thanks to This Flimsy Report," *Motherboard*, January 12, 2015, http://motherboard.vice.com/read/the-us-spent-360-million-on-border-drones-thanks-to-this-flimsy-report.

16. "Privacy Impact Assessment for the Aircraft Systems," U.S. Customs and Border Protection/Department of Homeland Security (CBP/DHS), September 9, 2013, http://www.dhs.gov/sites/default/files/publications/privacy-pia-cbp-aircraft-systems-20130926.pdf.

17. James Vincent, "First Drone-assisted Arrest in America Began with a Dispute over Six Cows," *The Independent* (London), January 30, 2014, http://www.independent.co.uk/life-style/gadgets-and-tech/first-drone-assisted-arrest-in-america-began-with-a-dispute-over-six-cows-9097090.html.

18. Jennifer Lynch, "FAA Releases Lists of Drone Certificates—Many Questions Left Unanswered," Electronic Frontier Foundation, April 19, 2012, https://www.eff.org/deeplinks/2012/04/faa-releases-its-list-drone-certificates-leaves-many-questions-unanswered.

19. Based on documents provided to the Electronic Frontier Foundation (EFF) pursuant to Freedom of Information Act requests. The Arlington documents can be viewed via EFF's map of drone authorizations: Electronic Frontier Foundation, "Drone Flights in the U.S.," https://www.eff.org/foia/faa-drone-authorizations.

20. Based on documents provided to the Electronic Frontier Foundation pursuant to Freedom of Information Act requests. The Miami-Dade documents can be viewed via EFF's map of drone authorizations: Electronic Frontier Foundation, "Drone Flights in the U.S.," https://www.eff.org/foia/faa-drone-authorizations.

21. See "Up in the Sky! It's a Drone, Looking at You," NPR, December 5, 2011, http://www.npr.org/2011/12/05/143144146/drone-technology-finding-its-way-to-american-skies; and Eric Roper, "Aug. 17, 2012: City Cameras Track Anyone, Even Minneapolis Mayor Rybak," *StarTribune*, September 19, 2014, http://www.startribune.com/aug-17-2012-city-cameras-track-anyone-even-minneapolis-mayor-rybak/166494646/.

22. "BAE has Success with ARGUS-IS," UPI, February 9, 2010, http://www.upi.com/Business_News/Security-Industry/2010/02/09/BAE-has-success-with-ARGUS-IS/UPI-78931265744037/.

23. Stephen Trimble, "Sierra Nevada Fields ARGUS-IS Upgrade to Gorgon Stare Pod," *FlightGlobal*, July 2, 2014, https://www.flightglobal.com/news/articles/sierra-nevada-fields-argus-is-up grade-to-gorgon-stare-400978/.

24. Sebastian Anthony, "DARPA Shows Off 1.8-gigapixel Surveillance Drone, Can Spot a Terrorist from 20,000 Feet," *ExtremeTech*, January 28, 2013, http://www.extremetech.com/extreme/146909-darpa-shows-off-1-8-gigapixel-surveillance-drone-can-spot-a-terrorist-from-20000-feet.

25. Ibid.

26. Sierra Nevada Corporation press release, "Sierra Nevada Corporation Achieves Milestone for USAF's Advanced Wide-Area Airborne Persistent Surveillance (WAPS) System—Gorgon Stare Increment 2," July 1, 2014, http://www.prweb.com/releases/2014/07/prweb11988406.htm.

27. Trimble, "Sierra Nevada Fields ARGUS-IS Upgrade to Gorgon Stare Pod."

28. Ibid.

29. Alistair Barr and Reed Albergotti, "Google to Buy Titan Aerospace as Web Giants Battle for Air Superiority," *Wall Street Journal*, April 14, 2014, http://www.wsj.com/articles/SB10001424052702304117904579501701702936522.

30. Jessica Guynn, "Facebook's Aquila Drone Completes First Test Flight," *USA Today*, July 21, 2016, http://www.usatoday.com/story/tech/news/2016/07/21/facebooks-aquila-completes-first-test-flight/87368910/.

31. Dave Gershgorn, "Facebook's Enormous Internet Drone Is Almost Ready for Primetime," *Popular Science*, February 23, 2016, http://www.popsci.com/facebooks-full-scale-internet-drone-is-almost-ready-for-primetime.

32. According to *Washington Post* reporting each Gorgon Stare pod costs $17.5 million. See Ellen Nakashima and Craig Whitlock, "With Air Force's Gorgon Drone 'We Can See Everything,'" *Washington Post*, January 2, 2011, http://www.washingtonpost.com/wp-dyn/content/article/2011/01/01/AR2011010102690.html.

33. Benjamin Miller, unmanned aircraft program manager, Mesa County Sheriff's Office, Testimony before the Committee on Judiciary, United States Senate, 113th Cong., 1st sess., March 20, 2013, https://fas.org/irp/congress/2013_hr/drones.pdf.

34. Craig Timberg, "New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time," *Washington Post*, February 5, 2014, https://www.washingtonpost.com/business/technology/new-surveillance-technology-can-track-everyone-in-an-area-for-several-hours-at-a-time/2014/02/05/82f1556e-876f-11e3-a5bd-844629433ba3_story.html.

35. Ibid. The specifications for Persistent Surveillance Systems' HawkEye II Wide Area Surveillance system can be found at Persistent Surveillance Systems, "Hawkeye II Specifications," http://www.pss-1.com/#!hawkeye-ii-specifications/c1a3i.

36. Timberg, "New Surveillance Technology Can Track Everyone in an Area for Several Hours at a Time."

37. Ibid.

38. "Gorgon Stare is being tested now, and officials hope it will be fielded within two months. Each $17.5 million pod weighs 1,100 pounds and, because of its configuration, will not be mounted with weapons on Reaper aircraft, officials said. They envision it will have civilian applications, including securing borders and aiding in natural disasters. The Department of Homeland Security is exploring the technology's potential, an industry official said." See Nakashima and Whitlock, "With Air Force's Gorgon Drone 'We Can See Everything.'"

39. "U.S. Customs and Border Protection's Unmanned Aircraft System Program Does Not Achieve Intended Results or Recognize All Costs of Operations," Office of Inspector General, De-

cember 24, 2014, https://www.oig.dhs.gov/assets/Mgmt/2015/OIG_15-17_Dec14.pdf.

40. "Artificial Hummingbird Developed," *Press Association*, February 18, 2011, http://www.independent.ie/world-news/and-finally/artificial hummingbird-developed-26706343.html.

41. Elbert Chu, "British Troops Deploy the Teeniest Recon Drone," *Popular Science*, February 6, 2013, http://www.popsci.com/technology/article/2013-02/meet-baby-drone.

42. Adam Piore, "Rise of the Insect Drones," *Popular Science*, January 29, 2014, http://www.popsci.com/article/technology/rise-insect-drones.

43. U.S. Const. amend. IV.

44. *Katz v. United States* 389 U.S. 347 (1967).

45. Ibid.

46. Ibid. at 361 (Harlan, J., concurring).

47. Ibid.

48. Richard A. Posner, "The Uncertain Protection of Privacy by the Supreme Court," *Supreme Court Review* (1979): 173–216, http://www.jstor.org/stable/3109570. "It is circular to say that there is no invasion of privacy unless the individual whose privacy is invaded had a reasonable expectation of privacy; whether he will or will not have such an expectation will depend on what the legal rule is." See also Michael Abramowicz, "Constitutional Circularity," *UCLA Law Review* 49 (2001): 1–91, http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2282586. "Fourth Amendment doctrine, moreover, is circular, for someone can have a reasonable expectation of privacy in an area if and only if the Court has held that a search in that area would be unreasonable." And see *Minnesota v. Carter* 525 U.S. at 97 (1998) (Scalia, J., concurring). "In my view, the only thing the past three decades have established about the Katz test (which has come to mean the test enunciated by Justice Harlan's separate concurrence in Katz, [...]) is that, unsurprisingly, those that 'actual (subjective) expectation[s] of privacy' 'that society is prepared to recognize as "reasonable,"' [...] bear an uncanny resemblance to those expectations of privacy that this Court considers reasonable."

49. *California v. Ciraolo* 476 U.S. 207 (1986).

50. Ibid. at 210 (Burger, C. J., majority).

51. Ibid. at 214 (Burger, C. J., majority).

52. Ibid. at 211–12 (Burger, C. J., majority).

53. *Florida v. Riley* 488 U.S. 445 (1989).

54. Ibid. at 462 (Brennan, J., dissenting).

55. Troy A. Rule, "Airspace in an Age of Drones," *Boston University Law Review* 95, no. 155 (2015): 155–208, http://ssrn.com/abstract=2482567.

56. Gregory McNeal, "Drones and Aerial Surveillance," Brookings Institution Project on Civilian Robotics, November, 2014, http://www.brookings.edu/research/reports2/2014/11/drones-and-aerial-surveillance.

57. *Dow Chemical Co. v. United States*, 476 U.S. 227 (1986).

58. Ibid. at 238 (Burger, C. J., majority) .

59. *United States v. Jones* 565 US _ (2012). Page numbers refer to slip opinion.

60. Ibid. at 2 (Scalia, J., majority).

61. Ibid.

62. Ibid. at 4 (Scalia, J., majority).

63. Ibid. at 2 (Alito, J., concurring).

64. Ibid.

65. Ibid. at 10 (Alito, J., concurring). "The Katz test rests on the assumption that this hypotheti-

cal reasonable person has a well-developed and stable set of privacy expectations. But technology can change those expectations. Dramatic technological change may lead to periods in which popular expectations are in flux and may ultimately produce significant changes in popular attitudes."

66. Orin Kerr, "The Mosaic Theory of the Fourth Amendment," *Michigan Law Review* 111 (2012): 311. "Before *Jones*, Fourth Amendment decisions had always evaluated each step of an investigation individually. *Jones* introduced what we might call a "mosaic theory" of the Fourth Amendment, by which courts evaluate a collective sequence of government activity as an aggregated whole to consider whether the sequence amounts to a search."

67. Ibid.

68. Ibid.

69. *Jones* at 4 (Sotomayor, J., concurring).

70. Kerr, "The Mosaic Theory of the Fourth Amendment."

71. *Jones* at 13 (Alito, J., concurring).

72. Kerr., "The Mosaic Theory of the Fourth Amendment."

73. Ariane de Vogue, "Supreme Court Ruling Prompts FBI to Turn Off 3,000 Tracking Devices," *ABC News*, March 7, 2012, http://abcnews.go.com/blogs/politics/2012/03/supreme-court-ruling-prompts-fbi-to-turn-off-3000-tracking-devices/.

74. A revision of Fourth Amendment doctrine has been proposed by my colleague Jim Harper. See Jim Harper, "Escaping Fourth Amendment Doctrine after *Jones*: Physics, Law, and Privacy Protection," *Cato Supreme Court Review 2011–2012*, edited by Ilya Shapiro (Washington: Cato Institute, 2013), 219–55, http://object.cato.org/sites/cato.org/files/serials/files/supreme-court-review/2012/9/scr-2012-harper.pdf.

75. Randy E. Barnett, "Why the NSA Data Seizures Are Unconstitutional," Georgetown Law Faculty Publications and Other Works, Paper no. 1659 (2015), http://scholarship.law.georgetown.edu/facpub/1659.

76. Bruce Schneier, "It's Time to Drop the 'Expectation of Privacy' Test," *Wired*, March 26, 2009, http://archive.wired.com/politics/security/commentary/securitymatters/2009/03/securitymatters_0326.

77. *Riley v. California* 573 U.S. (2014).

78. Timothy Williams, "Facial Recognition Software Moves from Overseas Wars to Local Police," *New York Times*, August 12, 2015, http://www.nytimes.com/2015/08/13/us/facial-recognition-software-moves-from-overseas-wars-to-local-police.html?_r=0.

79. See Sandee LaMotte, "The Other 'Fingerprints' You Don't Know About," CNN, December 4, 2015, http://www.cnn.com/2015/12/04/health/unique-body-parts/; and Dan Moren, "7 Surprising Biometric Identification Methods," *Popular Science*, December 30, 2014, http://www.popsci.com/seven-surprising-biometric-identification-methods.

80. Carl Franzen, "How to Teach Your Drone to Track Things," *Motherboard*, January 26, 2015, http://motherboard.vice.com/read/how-to-teach-your-drone-to-track-things; and Clay Dillow, "Army Developing Drones that Can Recognize Your Face From a Distance," *Popular Science*, September 28, 2011, http://www.popsci.com/technology/article/2011-09/army-wants-drones-can-recognize-your-face-and-read-your-mind.

81. Nita Farahany, Professor of Law, Duke University, Testimony before the Senate Committee on the Judiciary Subcommittee on Privacy, Technology and the Law, 112th Cong. 1., July 18, 2012, https://www.judiciary.senate.gov/imo/media/doc/12-7-18FarahanyTestimony.pdf.

82. Ibid. "An individual who is scanned in public cannot reasonably claim that facial recognition technology captures something he has sought to

seclude from public view. Instead, he must argue that he has a reasonable expectation of privacy in his personal identity associated with his facial features. Under current doctrine, courts would properly reject such a claim."

83. Government Accountability Office, "Facial Recognition Technology: FBI Should Better Ensure Privacy and Accuracy," May 2016, http://www.gao.gov/assets/680/677098.pdf.

84. Ibid.

85. Jay Stanley, "FBI Wants to Exempt Biometric Mega-Database from Privacy and Accuracy Rules," *ACLU*, May 31, 2016, https://www.aclu.org/blog/free-future/fbi-wants-exempt-biometric-mega-database-privacy-and-accuracy-rules.

86. Ibid.

87. Government Accountability Office, "Facial Recognition Technology: FBI Should Better Ensure Privacy and Accuracy."

88. Ibid.

89. For the purpose of these conditions, lawmakers should use the FBI's Uniform Crime Report (UCR) Program "violent crime" definition. According to the UCR, "violent crime" includes murder, rape, robbery, and aggravated assault. See FBI, "Preliminary Semiannual Uniform Crime Report, January–June 2015," https://ucr.fbi.gov/crime-in-the-u.s/2015/preliminary-semiannual-uniform-crime-report-januaryjune-2015.

90. *Kyllo v. United States* 533 U.S. 27 (2001).

91. Feeney , "Watching the Watchmen: Best Practices for Police Body Cameras."

92. "Police Body Worn Cameras: A Policy Scorecard" compiled by the Leadership Conference and Upturn, August 2016, https://www.bwcscorecard.org/.

93. DC Code § 2-534.

94. 2016 OK HB 2337.

95. 2016 NH HB 602.

96. Fla. Stat. § 934.50.(3)(b). See "The 2016 Florida Statutes," http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&URL=0900- 0999/0934/Sections/0934.50.html.

97. American Civil Liberties Union, "Warrant Requirement for Drone Usage Now Law: ACLU of Virginia Celebrates Key Victory," May 1, 2015, https://www.aclu.org/news/warrant-requirement-drone-usage-now-law-aclu-virginia-celebrates-key-victory.

98. Monte Reel, "Secret Cameras Record Baltimore's Every Move from Above," *Bloomberg Businessweek*, August 23, 2016, https://www.bloomberg.com/features/2016-baltimore-secret-surveillance/.

99. Philip Ewing, "Rand Paul Pulls Plug on Nearly 13-hour Filibuster," *Politico*, March 6, 2013, http://www.politico.com/story/2013/03/rand-paul-filibuster-john-brennan-cia-nominee-088507.

100. Paul Harris, "Rand Paul Filibuster Joined by Others in Bid to Block Brennan Appointment," *The Guardian*, March 7, 2013, https://www.theguardian.com/world/2013/mar/06/rand-paul-filibuster-drones-brennan.

101. Rachel Weiner, Aaron Blake, and Philip Rucker, "Eric Holder Responds to Rand Paul with 'No,' Paul Satisfied," *Washington Post*, March 7, 2013, https://www.washingtonpost.com/news/post-politics/wp/2013/03/07/white-house-obama-would-not-use-drones-against-u-s-citizens-on-american-soil/.

102. ACLU, "War Comes Home: The Excessive Militarization of American Policing," July 2014, https://www.aclu.org/report/war-comes-home-excessive-militarization-american-police.

103. Radley Balko, "Shedding Light on the Use of SWAT Teams," *Washington Post*, February 17, 2014,

https://www.washingtonpost.com/news/the-watch/wp/2014/02/17/shedding-light-on-the-use-of-swat-teams/; and Radley Balko, "Overkill: The Rise of Paramilitary Police Raids in America," Cato Institute White Paper, July 17, 2006, http://www.cato.org/publications/white-paper/overkill-rise-paramilitary-police-raids-america.

104. Sara Sidner and Mallory Simon, "How Robot, Explosives Took Out Dallas Sniper in Unprecedented Way," CNN, July 12, 2016, http://www.cnn.com/2016/07/12/us/dallas-police-robot-c4-explosives/.

105. Richard Winton and Garrett Therolf, "Police Shooting from Helicopters—Rare but Not Unheard Of," *Los Angeles Times*, September 19, 2015. http://www.latimes.com/local/lanow/la-me-ln-police-shooting-from-helicopters-rare-but-not-unheardof-20150919-story.html.

106. 2015 TN HB 1456.

107. 2015 SC H 4425.

108. Va. Acts H.B 2012, Ch. 755 (2013) and OR. REV. STAT. ANN. § 837.365 (West Supp. 2014).

109. Fla. Stat. § 934.50.(2).

110. The *Guardian* (London) collected data on American police killings in 2015 as part of its "The Counted" project. According to the *Guardian*, Tasers killed 50 of the 1,146 people who died as a result of an interaction with police in 2015. See "The Counted: People Killed by Police in the US," http://www.theguardian.com/us-news/ng-interactive/2015/jun/01/the-counted-police-killings-us-database.

111. Andy Greenberg, "Hacker Says He Can Hijack a $35K Police Drone a Mile Away," *Wired*, March 2, 2016, http://www.wired.com/2016/03/hacker-says-can-hijack-35k-police-drone-mile-away/.

112. Neil Vigdor, "Connecticut Could Break Ground on Armed Police Drones," *Government Technology*, March 10, 2016, http://www.govtech.com/public-safety/Connecticut-Could-Break-Ground-on-Armed-Police-Drones.html.

113. Mark Blunden, "'Death Ray' Could Be Used at Heathrow to Shut Down Flying Drones," *Evening Standard* (London), April 25, 2016, http://www.standard.co.uk/news/london/death-ray-could-be-used-at-heathrow-to-shut-down-flying-drones-a3232581.html; and "AUDS Team to Showcase Counter-UAV System at Farnborough Airshow," Blighter Surveillance Systems, July 11, 2016, http://www.blighter.com/news/press-releases/132-auds-team-to-showcase-counter-uav-system-at-farnborough-airshow.html.

114. Steve Annear, "Drone-Detection Firm Brought Net Guns to Marathon," *Boston Globe*, April 21, 2015, https://www.bostonglobe.com/metro/2015/04/21/boston-marathon-drone-detection-firm-brought-net-guns/20Sp9Brfn5rFOIYqRJmP3H/story.html.

115. The legality of these tools is an issue that lawmakers and federal regulatory bodies such as the FAA and the Federal Communications Commission will have to clarify as drones become more common. Under current federal law, users of anti-drone tools run the risk of violating 18 U.S. Code § 32, which outlaws the disabling of a civil aircraft. In addition, those wishing to install such devices would have to first obtain FCC approval. Battelle, a company that makes an anti-drone device, states on its website, "This device has not been authorized as required by the rules of the Federal Communications Commission. This device is not, and may not be, offered for sale or lease, or sold or leased in the United States, other than to the United States government and its agencies, until authorization is obtained. Under current law, the DroneDefender may be used in the United States only by authorized employees of the Federal government and its agencies, and use by others may be illegal." However, in May 2016 it was announced that the FAA would be testing anti-drone devices at selected airports, and according to Harvard's Bruce Schneier, law enforcement can use anti-drone technology. See Battelle, "Battelle Drone

Defender," http://www.battelle.org/our-work/national-security/tactical-systems/battelle-dronedefender; "British Drone-freezing Ray Gets US Airports Trial," *BBC News*, June 1, 2016, http://www.bbc.com/news/technology-36425879; and Bruce Schneier, "Is It OK to Shoot Down a Drone over Your Backyard?," CNN, September 9, 2015, http://www.cnn.com/2015/09/09/opinions/schneier-shoot-down-drones/.

116. Video released by DJI explains the firmware update installed on its Phantom drones. See DJI, "DJI—Phantom Firmware Update Safety Feature Integration," YouTube video, 3:11, posted April 9, 2014, https://www.youtube.com/watch?v=YoXAMRQoIAA.

117. Benjamin Miller, unmanned aircraft program manager, Mesa County Sheriff's Office, Testimony before the Committee on Judiciary, United States Senate, 113th Cong., 1st sess., March 20, 2013, https://www.judiciary.senate.gov/imo/media/doc/CHRG-113shrg81775.pdf.

118. Ibid.

119. FBI drones "constantly monitored" a 2013 standoff in Alabama involving a man holding a 5-year-old boy hostage in his bunker. See Victor Blackwell and Michael Pearson, "FBI: Bombs Found in Alabama Kidnapper's Bunker," CNN, February 5, 2013, http://www.cnn.com/2013/02/05/us/alabama-child-hostage/.

CATO INSTITUTE

Published by the Cato Institute, Policy Analysis is a regular series evaluating government policies and offering proposals for reform. Nothing in Policy Analysis should be construed as necessarily reflecting the views of the Cato Institute or as an attempt to aid or hinder the passage of any bill before Congress. Contact the Cato Institute for reprint permission. All policy studies can be viewed online at www.cato.org. Additional printed copies of Cato Institute Policy Analysis are $6.00 each ($3.00 each for five or more). To order, please email catostore@cato.org.