Statement of Jay Stanley, Senior Policy Analyst

American Civil Liberties Union

On

Drone Useage/Regulation

Before the Senate Judiciary and the House Civil Law and Judiciary

Committees

December 12, 2014

Thank you for the opportunity to testify on behalf of the American Civil Liberties Union and the ACLU of Minnesota. The ACLU has 8,500 members in Minnesota and more than half a million members nationwide, as well as countless additional activists and supporters. Our mission is to defend civil rights and liberties under the United States and Minnesota constitutions.

Today more than ever before, the American people are both aware of the powerful new surveillance technologies available to law enforcement agencies and concerned about how these technologies are being used. One of those technologies is Unmanned Aerial Vehicles (UAVs), or "drones."

So far, with the exception of our border regions, the use of drones within the United States is relatively limited. Under Federal Aviation Administration (FAA) rules, commercial use of drone technology is entirely banned. The few police agencies that are deploying them can only do so under very tight strictures: below 400 feet in altitude, line-of-sight only, during daylight hours only, not over densely populated areas, with a spotter present in addition to a pilot, and with both of those operators possessing certain certifications.[1] Most of the drones being used by police agencies are noisy and can only stay aloft for short periods of time (less than an hour).[2]

Nevertheless, the prospect of drones in US airspace has rightly attracted an enormous amount of attention and concern over privacy issues from across the political spectrum. In fact, this issue has led to an outpouring of legislative activity of the kind we rarely see in the area of privacy. Strong legislation to regulate this technology has been introduced in Congress[3] and in more than 42 state legislatures, with thirteen states having enacted bills into law.[4] Polls have found large majorities of Americans concerned over the privacy issues surrounding drones,[5] and the subject has attracted an enormous amount of media attention.

The significant gap between the amount of fuss that drones have generated and the limited nature of their current deployment has led some to suggest that concerns are based on paranoia and misinformation. Nothing could be further from the truth.

Drones are an enormously powerful surveillance technology. The biggest danger is that drones will come to be used for routine, pervasive surveillance and tracking. There are too many reasons to think that we may find ourselves living in such a reality.

Not only is the underlying technology evolving rapidly and almost certain to become even more powerful, but the legal strictures on their use are likely to loosen over time—perhaps radically. In the FAA Modernization and Reform Act of 2012[6], Congress has already required the FAA to simplify and accelerate the process by which it issues licenses to government agencies to use drones. The act requires the FAA to integrate drones into the national airspace no later than September 2015.[7] It is far from certain that the FAA will actually meet this deadline, but the gears are in

motion for a significant loosening of the rules surrounding the deployment of drones in American airspace.

Looking further into the future, it is possible that new approaches to air traffic management could eventually clear the way even further for the use of drones—for example through systems in which aircraft automatically alert one another to the other's presence and route around each other, like packets on the internet.

Police and government agencies, meanwhile, are likely to seek to use this technology for pervasive, suspicionless mass surveillance. To begin with, there is a long history of government agencies seeking to engage in mass surveillance, from the Cold War spying abuses to today's deployment of license plate scanners and surveillance cameras in our public places, to the sweeping NSA programs that were revealed by Edward Snowden. And when it comes to drones, it is already clear that some agencies would leap at the chance to deploy pervasive aerial surveillance. In 2011, the city of Ogden, Utah, sought FAA permission to deploy an autonomous unmanned blimp as "a deterrent to crime when it is out and about."[8] Similarly, Hawaii took steps toward federal approval to fly drones for surveillance over its harbors.[9] In both cases, permission was ultimately denied by the FAA, but the desire is clearly there.

As the FAA loosens strictures on the use of drones, it is probable that more and more police departments will begin using them, as there is pent-up demand among police departments for cheap aerial surveillance. Ownership of drones could quickly become common among departments large and small. From there, it's not hard to envision how things may develop in the absence of strong privacy protections. Organizations of police drone operators would be formed to exchange tips and advice. We would begin to hear about their deployment by federal agencies with increasing frequency. And we would start to hear more stories about how they're being used; most departments and agencies would be relatively careful at first, and we would hear of drones being put to use in specific, mostly unobjectionable police operations, such as raids, chases, and searches supported by warrants. Fairly quickly, however, we would begin to hear that a few departments are deploying drones for broader, more general uses: drug surveillance, marches and rallies, and generalized monitoring of troubled neighborhoods.

Meanwhile the technology for carrying out mass surveillance with drones will be improving. Innovations will likely allow for drones to stay aloft for longer periods of time more cheaply—involving blimps, perhaps, or solar-powered flight—which could become key in permitting their use for persistent surveillance. They will develop the ability to mutually coordinate, so that multiple drones deployed over neighborhoods can be linked together (the technologies for doing this are already surprisingly advanced).[10] This could allow a swarm of craft to form a single, distributed wide-area surveillance system. Meanwhile, "wide-area surveillance" systems that can monitor a wide area from a single craft will also likely improve.

At the same time, drones and the computers behind them will become more intelligent and capable of analyzing the video feeds they are generating. Without privacy protections, what we could see is that drones could be used not only to track multiple vehicles and pedestrians as they move around a city or town, but also to store that data for an extended period of time. And increasingly, the data would be mined. With individuals' comings and goings routinely monitored, databases would build up records of where people live, work, and play; what friends they visit, bars they drink at, doctors they visit; and what houses of worship, political events, or sexually oriented establishments they attend—and who else is present at those places at the same time. Computers would comb through this data looking for "suspicious patterns." This could mean anything from looking for the extremely remote possibility that someone is planning a terrorist attack, to looking for someone planning a protest, to someone who, because of the places they've been, is suspected of having a higher-than-average possibility of driving under the influence. When the algorithms kick up the alarm that someone is "out of the ordinary," the person involved would become the subject of much more extensive surveillance.

At least one important part of this scenario is already rapidly becoming reality: the technology that allows drones to engage in "wide-area persistent surveillance" is already here. The government has developed a system dubbed ARGUS-IS, which is basically a super-high, 1.8 gigapixel resolution camera that can be mounted on a drone. ARGUS is able to simultaneously photograph a 38-square-mile area with a resolution high enough to make out a pedestrian waving his arms. The technology, its developer boasted, is "equivalent to having up to a hundred Predators look at an area the size of a medium-sized city at once."[11]

ARGUS does not merely photograph a city. It also automatically detects moving vehicles and pedestrians to track their movements—where they start and finish each journey and the path they take in between. The surveillance potential of such a tracking algorithm attached to such powerful cameras should give us pause. To identify an individual, it is not necessary to use technologies such as face or license-plate recognition, cell phone tracking, or gait recognition. Just knowing where a set of moving pixels starts and finishes its day can reveal a lot, because even relatively rough location information about a person will often identify them uniquely. For example, according to one study, just knowing the zip code (actually census tract, which is basically equivalent) of where you work, and where you live, will uniquely identify 5 percent of the population. If you know the "census blocks" where somebody works and lives (an area roughly the size of a block in a city, but larger in rural areas), the accuracy is much higher, with at least half the population being uniquely identified.[12] And of course once a person's home address is identified, little doubt as to their identity remains.[13]

In fact, these kinds of capabilities have already been deployed in the United States. A company called "Persistent Surveillance Systems" is trying to sell a similar capability to domestic police agencies. The city of Dayton, Ohio, actually tested and considered deploying a system that is in many respects similar to ARGUS. And although it

shares many of the features that are causing so much concern over drones, it has escaped all the limits placed on drones simply by using a manned aircraft rather than unmanned drones. Manned aircraft are more expensive than drones and so are unlikely to be used as widely as drones may eventually be, but this deployment shows the desire of some police departments for this capability and points toward what we could see in the future.

In the United States it does not accord with our tradition, law, or Constitution to allow the government to look over everybody's shoulders (literally or figuratively) *just in case* they engage in wrongdoing. We require the police to have individualized suspicion of wrongdoing before they invade our privacy in that way.[14]

What would be the effect on our public spaces, and our society as a whole, if everyone felt the keen eye of the government on their backs whenever they ventured outdoors? Psychologists have repeatedly found that people who are being observed tend to behave differently, and make different decisions, than when they are not being watched. This effect is so great that a recent study noted that "merely hanging up posters of staring human eyes is enough to significantly change people's behavior."[15] Ultimately, the chilling effects of mass drone surveillance would lead to an oppressive atmosphere in which people learn to think twice about everything they do, knowing that it will be recorded, charted, scrutinized by increasingly intelligent computers, and possibly used to target them.

Supporters of surveillance drones sometimes ask why there should be such a fuss over drones, given that the police and federal government have used manned helicopters for aerial surveillance for decades. For one thing, drones erase the "natural limits" that have always applied to aerial surveillance using manned aircraft. Manned helicopters and fixed-wing aircraft are expensive to acquire, staff, and maintain. A police helicopter costs from $500,000 to $3 million to acquire, and $200–$400 an hour to fly. Manned aircraft are large, complex machines requiring expert ground crews, multiple shifts of pilots and co-pilots, and (unlike drones which can often be hand-launched) runways or helipads. Such expenses mean there are inevitably going to be far fewer of them—which in turn means the police are likely to use them only where they are most needed. With drones, on the other hand, it's easy to foresee a day when even a professional police drone could be acquired for less than a hundred dollars, including maintenance costs. And if technology and laws eventually reach the point where drones can fly autonomously, they would become even cheaper because police departments wouldn't even have to pay staff to control or monitor them.

In addition, police helicopters *do* raise privacy issues. Because of the expense of using manned police aircraft, privacy invasions have not risen to the level that our legal system has felt compelled to address them. But incidents do happen. In 2004, a couple making love at night on a pitch-black rooftop balcony in New York, where they had every reason to expect they enjoyed privacy, were filmed for nearly four minutes by a New York Police Department (NYPD) helicopter using night vision.

And any police helicopter that followed a citizen around town for no reason, or hovered over the backyard of an innocent homeowner whose daughter was sunbathing with her friends, would probably draw complaints. With drones, scenarios like those are bound to happen much more frequently because unmanned flight is so much less expensive. In addition, technologies like ARGUS have now emerged and could be attached to a helicopter; the nation simply hasn't had the chance yet to confront that possibility.

Commercial Use

The issues raised by the private use of drones are different and more complex than those raised by police and other government use. While a push by police and government agencies to use drones for broad surveillance purposes is entirely predictable and inevitable, it's probably too early to know to what extent drones will be used to invade privacy by the private sector, or how.

In addition, there are important countervailing values when it comes to private drones, such as the right to photography. We have seen photographers questioned, harassed, and arrested around the country for such activities as photographing bridges, trains, and government buildings, and for photographing police carrying out their public duties. Some photographers have had their cameras (or camera-phones) seized, and photographs destroyed.[16] The ACLU has challenged such interference with photographers, and the courts have all but unanimously held that photography of things visible from a public place where a photographer has a right to be is protected by the First Amendment.[17]

What happens when photographers—whether certified reporters or citizen photographers—seek to exploit drone technology for similar purposes? While we don't want the government watching citizens without suspicion of wrongdoing, it is important to preserve the right of citizens to watch their government, and such uses of drones implicate First Amendment rights.

Drones will certainly have positive uses on the government side—helping with search and rescue missions, wildfires, environmental or geological surveys, or disaster relief, for example—and they will have beneficial uses on the private-sector side as well. In fact, the technology is likely to become the subject of incredible innovation as thousands of hobbyists, tinkerers, and companies explore the technology and invent helpful and imaginative ways of exploiting it. Ideally we can protect our privacy without curbing such innovation or interfering with First Amendment-protected uses of the technology.

That said, there are several foreseeable ways in which drones could be used by private actors to invade privacy. Voyeurism is an obvious one; state "Peeping Tom laws" already exist in every state to prevent surveillance,[18] and trespass and nuisance laws may also be used to exclude low-flying drones from property. However, the language and scope of these laws varies widely from state to state.

Another privacy threat from private drones includes the persistent observation of landowners' back yards or other areas of private property. While the Supreme Court ruled in the 1986 case *California v. Ciraolo*[19] that police flying a fixed-wing aircraft did not need a warrant to look for marijuana plants in a private, fenced back yard because "any member of the public flying in this airspace who glanced down could have seen everything that these officers observed," it is not clear such logic would apply in the case of persistent, prolonged surveillance of private property. Many homeowners who don't think twice about having an occasional Cessna fly overhead would react strongly if they were to learn an aerial camera was trained on their yard for weeks at a time.

For that matter, private-sector persistent surveillance of public spaces would also raise many of the same privacy issues as public surveillance by the government. Imagine a live version of Google Earth. Location tracking by private companies would be just as serious an invasion of privacy as by the government, as would the simple act of blanket 24/7 aerial photography of all our public spaces.

But it's not clear that such uses will be realized, and given the important countervailing interests of the First Amendment and the benefits of protecting innovation, the bottom line is that because of the different issues they raise, private drones should be approached by policy makers separately.

Recommendations

At a minimum, we recommend enactment of the following core measures to ensure that our society can enjoy the public safety benefits of this technology without having to worry about its darker potential:

- **Usage restrictions.** UAVs should be subject to strict regulation to ensure that their use does not eviscerate the privacy that Americans have traditionally enjoyed and rightly expect. Innocent Americans should not have to worry that police will scrutinize their activities with drones. To this end, the use of drones should be prohibited for indiscriminate mass surveillance, for example, or for spying based on First Amendment-protected activities. In general, drones should not be deployed by the government except:

    - where there are specific and articulable grounds to believe that the drone will collect evidence relating to a specific instance of criminal wrongdoing or, if the drone will intrude upon non-public spaces where the government has obtained a warrant based on probable cause; or

- where there is a geographically confined, time-limited emergency situation in which particular individuals' lives are at risk, such as a fire, hostage crisis, or person lost in the wilderness; or

- for reasonable non-law enforcement purposes by non-law enforcement agencies, where privacy will not be substantially affected, such as geological inspections or environmental surveys, and where the surveillance will not be used for secondary law enforcement purposes.

- **Image retention restrictions.** Images of identifiable individuals captured by aerial surveillance technologies should not be retained or shared unless there is reasonable suspicion that the images contain evidence of criminal activity or are relevant to an ongoing investigation or pending criminal trial.

- **Public notice.** The policies and procedures for the use of aerial surveillance technologies should be explicit and written, and should be subject to public review and comment. While it is legitimate for the police to keep the details of particular investigations confidential, policy decisions regarding overall deployment policies—including the privacy trade-offs they may entail—are a public matter that should be openly discussed.

- **Democratic control.** Deployment and policy decisions surrounding UAVs should be democratically decided based on open information—not made on the fly by police departments simply by virtue of federal grants or other autonomous purchasing decisions or departmental policy fiats.

- **Auditing and effectiveness tracking.** Investments in UAVs should only be made with a clear, systematic examination of the costs and benefits involved. And if aerial surveillance technology is deployed, independent audits should be put in place to track the use of UAVs by government, so that citizens and other watchdogs can tell generally how and how often they are being used, whether the original rationale for their deployment is met, whether they represent a worthwhile public expenditure, and whether they are being used for improper or expanded purposes.

- **Ban on weaponization.** Weapons developed on the battlefield in Iraq and Afghanistan have no place inside the U.S. The national consensus on this issue is reflected by the fact that the Heritage Foundation and the

International Association of Chiefs of Police join us in supporting sharp limits on weaponized drones.[20]

Ultimately this powerful new technology should only be used by the government if subject to an equally powerful framework that regulates its use in order to avoid abuse and invasions of privacy.

A Crossroads

We as a society must make a fundamental decision: whether we are to become a "collect it all" society, in which records of our activities are collected and stored by the government "just in case." This is the vision of those pushing for persistent wide-area surveillance, and we are now in the early stages of a broad debate over whether to allow such surveillance. If we accede to the "collect it all" vision in some contexts such as drones, we should not be surprised when that same philosophy is extended to everything—to our financial transactions, hotel records, Internet searches, medical information, and every other possible source of data.

Storage of all this information gives the government a frightening new power it has never had before: the power to hit "rewind" on our life and see the history of our movements, transactions, and communications—to turn our life into an open book. Such "retroactive surveillance" is an enormous power that no government has ever had or should have over its people.

As Justice John Harlan observed in 1971, words are "measured a good deal more carefully and communication inhibited" when we suspect we're being monitored, and if we allow such monitoring to become prevalent, "it might well smother that spontaneity—reflected in [the] frivolous, impetuous, sacrilegious, and defiant discourse—that liberates daily life."[21] If we allow ourselves to become a society in which our every move is recorded, we'll find ourselves living in another country, one that we might not much like.

Unfortunately, there are many uncertainties about how our Constitution will be applied by the courts to pervasive aerial surveillance. The legal system has always been slow to adapt to new technology. For example, it took the Supreme Court 40 years to apply the Fourth Amendment to telephone calls. At first, the court found in a 1928 decision that because telephone surveillance did not require entering the home, the conversations that travel over telephone wires are not protected.[22] It was not until 1967 that this literal-minded hairsplitting about "constitutionally protected areas" was overturned, with the court declaring that the Constitution "protects people, not places."[23] Today, technology is moving much faster than it did in the telephone era—but the gears of justice turn just as slowly as they ever have, and maybe even slower.

Just as the new technology of the telephone broke the court's older categories of understanding, so too will drones with all their new capabilities create new situations that will not fit neatly within existing jurisprudential categories of analysis. For example, how will the courts view the use of drones for routine location tracking? The Supreme Court started to grapple with such questions in its recent decision in the *Jones* GPS case, but it is far from clear what the ultimate resolution will be. The court ruled in *Ciraolo* that the Fourth Amendment provides no protection from aerial surveillance, and while the new factors that drones bring to the equation could shift that judgment, we cannot be certain. Legislators should not wait for cases to come before the courts; they should act to preserve our values now.

We're at a crossroads today – a highly significant moment in the history of technology. If we do nothing, there should be little doubt that new technological capabilities will be exploited by government agencies in ways that could have potentially profound consequences for our lives. But there is no reason we can't enjoy the benefits of amazing new technologies like drones, while protecting our privacy. We can have our cake and eat it too, if we just take a little care and put in place some basic, commonsense protections to preserve our values.

[1] Federal Aviation Administration, Unmanned Aircraft Systems (UAS) Operational Approval [N 8900.227] (proposed July 30, 2013), *available at* www.faa.gov/documentLibrary/media/Notice/N_8900.227.pdf.

[2] *See, e.g., Draganflyer X6 Helicopter Tech Specs*, DRAGANFLY INNOVATIONS INC. (last visted Sept. 22, 2013), www.draganfly.com/uav-helicopter/draganflyer-x6/specifications/.

[3] *See Reps. Zoe Lofgren and Ted Poe Introduce Bipartisan Bill to Protect Americans' Privacy Rights from Domestic Drones*, CONGRESSWOMAN ZOE LOFGREN (last visted Sept. 22, 2013), lofgren.house.gov/index.php?option=com_content&view=article&id=785&Itemid=130.

[4] Allie Bohm, "Status of 2014 Domestic Drone Legislation in the States," ACLU Free Future blog, April 22, 2014, at https://www.aclu.org/blog/technology-and-liberty/status-2014-domestic-drone-legislation-states.

[5] *U.S. Supports Some Domestic Drone Use: But public registers concern about own privacy*, MONMOUTH UNIVERSITY POLL (June 12, 2012), *available at* www.monmouth.edu/assets/0/32212254770/32212254991/32212254992/32212254994/32212254995/30064771087/42e90ec6a27c40968b911ec51eca6000.pdf.

[6] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-95, § 213, 126 Stat 11 (2012).

[7] Jay Stanley, *Congress Trying to Fast-Track Domestic Drone Use, Sideline Privacy*, ACLU FREE FUTURE BLOG (Feb. 6, 2012, 2:39 PM), www.aclu.org/blog/technology-and-liberty-national-security/congress-trying-fast-track-domestic-drone-use-sideline.

[8] James Nelson, *Utah city may use blimp as anti-crime spy in the sky*, REUTERS (Jan. 16, 2011), www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116; Tim Gurrister, *Ogden blimp may be patrolling by Christmas*, STANDARD-EXAMINER (Aug. 31, 2011), www.standard.net/stories/2011/08/29/ogden-blimp-may-be-patrolling-christmas; James Nelson, *Utah city may use blimp as anti-crime spy in the sky*, REUTERS (Jan. 16, 2011), www.reuters.com/article/2011/01/16/us-crime-blimp-utah-idUSTRE70F1DJ20110116.

[9] Jim Dooley, *State Surveillance Drones 'Under Review'*, HAWAII REPORTER (Feb. 1, 2011), www.hawaiireporter.com/state-surveillance-drones-under-review/123.

[10] *See, e.g.*, Rebecca Searles, *Flying Robots Called 'Nano Quadrotor' Drones Swarm Lab (Video)*, HUFFINGTON POST (Feb. 2, 2012), www.huffingtonpost.com/2012/02/02/flying-robots-nano-quadrotor-drones-swarm_n_1249442.html.

[11] *NOVA: Rise of the Drones* (PBS television broadcast,Jan. 23, 2013), *available at* www.pbs.org/wgbh/nova/military/rise-of-the-drones.html; See also Jay Stanley, *Report Details Government's Ability to Analyze Massive Aerial Surveillance Video*

Streams, ACLU FREE FUTURE BLOG (Apr. 5, 2013), www.aclu.org/blog/technology-and-liberty-free-speech-national-security/report-details-governments-ability-analyze.

[12] Philippe Golle & Kurt Partridge, *On the Anonymity of Home/Work Location Pairs, in* PROCEEDING PERVASIVE '09 PROCEEDINGS OF THE 7TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING (2009), *available at* crypto.stanford.edu/~pgolle/papers/commute.pdf.

[13] *See, e.g.*, John Krumm, *Inference Attacks on Location Tracks, in in* PROCEEDING PERVASIVE '07 PROCEEDINGS OF THE 5TH INTERNATIONAL CONFERENCE ON PERVASIVE COMPUTING (2007), *available at* research.microsoft.com/en-us/um/people/jckrumm/Publications%202007/inference%20attack%20refined02%20distribute.pdf.

[14] "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." U.S. CONST. amend. IV.

[15] Sander van der Linden, *How the Illusion of Being Observed Can Make You a Better Person*, SCIENTIFIC AMERICAN (May 3, 2011), www.scientificamerican.com/article.cfm?id=how-the-illusion-of-being-observed-can-make-you-better-person; M. Ryan Calo, *People Can Be So Fake: A New Dimension to Privacy and Technology Scholarship*, 114 PENN ST. L. REV. 809, 836 (2010), *available at* www.pennstatelawreview.org/articles/114/114%20Penn%20St.%20L.%20Rev.%20809.pdf.

[16] *See* Jay Stanley, *You Have Every Right to Photograph That Cop*, ACLU (Sept. 7, 2011), www.aclu.org/free-speech/you-have-every-right-photograph-cop.

[17] *E.g.*, Glik v. Cunniffe, 655 F.3d 78, 85 (1st Cir. 2011).

[18] *See NDAA Voyeurism Compilation*, NDAA.ORG (updated July 2010), www.ndaa.org/pdf/Voyeurism%202010.pdf.

[19] 476 U.S. 207, 213-14 (1986).

[20] International Assocation of Cheifs of Police, Aviation Committee, Recommended Guidelines for the use of Unmanned Aircraft. August 2012, see: http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf; Paul Rosenzweig, Steven P. Bucci, Ph.D., Charles "Cully" Stimson and James Jay Carafano, Ph.D., *Drones in U.S. Airspace: Principles for Governance*, The Heritage Foundation, September 20, 2012, see: http://www.heritage.org/research/reports/2012/09/drones-in-us-airspace-principles-for-governance.

[21] United States v. White, 401 U.S. 745, 787 (1971) (Harlan, J., dissenting).

[22] Olmstead v. United States, 277 U.S. 438 (1928), *overruled by* Katz v. United States, 389 U.S. 347 (1967).

[23] Katz v. United States, 389 U.S. 347, 351 (1967).