Testimony and Statement for the Record of

Amie Stepanovich
Director of the Domestic Surveillance Project
Electronic Privacy Information Center

Hearing on "The Future of Drones in America:
Law Enforcement and Privacy Considerations"

Before the

Judiciary Committee
of the
U.S. Senate

March 20, 2013
226 Dirksen Senate Office Building
Washington, D.C.

Mister Chairman and Members of the Committee, thank you for the opportunity to testify today concerning the use of drones by law enforcement in the United States. My name is Amie Stepanovich. I am the Director of the Domestic Surveillance Project at the Electronic Privacy Information Center.

EPIC is a non-partisan research organization, established in 1994, to focus public attention on emerging privacy and civil liberties issues.[1] We work with a distinguished panel of advisors in the fields of law, technology, and public policy.[2] We have a particular interest in the protection of individual privacy rights against government surveillance. In the last several years, EPIC has taken a particular interest in the unique privacy problems associated with aerial drones.

The Federal Aviation Administration ("FAA") has been directed to fully integrate drones into the National Airspace by 2015.[3] In 2012 EPIC petitioned the FAA, as it considers new regulations to permit the widespread deployment of drones, to also develop new privacy safeguards.[4] The FAA heeded our warning, and is now considering privacy policies for drone operators. However, more must be done to protect the privacy of individuals in the United States.

We appreciate the Committee's interest in domestic drone use and its substantial impact on the privacy of individuals in the United States. In my statement today, I will describe the unique threats to privacy posed by drone surveillance, the problems with current legal safeguards, and the need for Congress to act.

I. Aerial Drones Pose a Unique Threat to Privacy

A drone is an aerial vehicle designed to fly without a human pilot on board. Drones can either be remotely controlled or autonomous. Drones can be weaponized and deployed for military purposes.[5] Drones can also be equipped with sophisticated surveillance technology that makes it possible to spy on individuals on the ground. In a report on drones published by EPIC in 2005, we observed, "the use of [drones] gives the federal government a new capability to monitor citizens clandestinely, while the effectiveness of the…surveillance planes in border patrol operations has not been proved."[6] Today, drones greatly increase the capacity for law enforcement to collect personal information on individuals.

---

[1] *About EPIC*, EPIC, http://www.epic.org/about (last visited July 16, 2012).
[2] *EPIC Advisory Board*, EPIC, http://www.epic.org/epic/advisory_board.html (last visited July 16, 2012).
[3] Federal Aviation Administration Modernization and Reform Act of 2012 ("FMRA"), Pub. L. 112-95 §§ 331-336 (2012), *available at* http://www.gpo.gov/fdsys/pkg/PLAW-112publ95/pdf/PLAW-112publ95.pdf.
[4] *Unmanned Aerial Vehicles (UAVs) and Drones*, EPIC, http://www.epic.org/privacy/drones (last visited July 16, 2012).
[5] *See, e.g., Predator B UAS*, General Atomics Aeronautical, http://www.ga-asi.com/products/aircraft/predator_b.php (last visited June 25, 2012); *X-47B UCAS*, Northrop Grumman, http://www.as.northropgrumman.com/products/nucasx47b/index.html (last visited July 16, 2012).
[6] *Spotlight on Surveillance: Unmanned Planes Offer New Opportunities for Clandestine Government Tracking* (August 2005), EPIC, http://epic.org/privacy/surveillance/spotlight/0805/ (last visited July 16, 2012).

We recognize that there are many positive applications for drones within the United States. With little to no risk to individual privacy, drones may be used to combat forest fires, conduct search and rescue operations, survey emergency situations, and monitor hurricanes and other weather phenomena.[7] In Dallas, a drone used by a hobbyist photographer was able to pinpoint an instance of gross environmental abuse at a nearby factory.[8] In Alabama, drones were recently used to assist in monitoring a hostage situation involving a young boy abducted off of the school bus.[9]

However, when drones are used to obtain evidence in a criminal proceeding, intrude upon a reasonable expectation of privacy, or gather personal data about identifiable individuals, rules are necessary to ensure that fundamental standards for fairness, privacy, and accountability are preserved.

The technology in use today is far more sophisticated than most people understand. Cameras used to outfit drones are among the highest definition cameras available. The Argus camera, featured on the PBS Nova documentary on drones, has a resolution of 1.8 gigapixels and is capable of observing objects as small as six inches in detail from a height of 17,000 feet.[10] On some drones, sensors can track up to 65 different targets across a distance of 65 square miles.[11] Drones may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers.[12]

Recent records received by EPIC under the Freedom of Information Act demonstrate that the Bureau of Customs and Border Protection procured drones outfitted

---

[7] *See, e.g.*, Tim Wall, *Flying Drones Fight Fires*, Discovery News (Nov. 10, 2011), *available at* http://news.discovery.com/earth/flying-drones-fight-fires-111110.html; Meghan Keneally, *Drone Plane Spots a River of Blood Flowing From the Back of a Dallas Meat Packing Plant*, Daily Mail Online (Jan. 24, 2012), *available at* http://www.dailymail.co.uk/news/article-2091159/A-drone-plane-spots-river-blood-flowing-Dallas-meat-packing-plant.html; Sean Holstege, *Drones' Good Flies Hand in Hand with Bad, Experts Fear*, AZCentral (July 7, 2012), *available at* http://www.azcentral.com/12news/news/articles/2012/07/07/20120707arizona-unmanned-drones-concerns.html.

[8] Meghan Keneally, *Drone Plane Spots a River of Blood Flowing From the Back of a Dallas Meat Packing Plant*, Daily Mail Online (Jan. 24, 2012), *available at* http://www.dailymail.co.uk/news/article-2091159/A-drone-plane-spots-river-blood-flowing-Dallas-meat-packing-plant.html.

[9] *See Military Tactics, Equipment Helped Authorities End Alabama Hostage Standoff*, Fox News (Feb. 7, 2013), http://www.foxnews.com/us/2013/02/07/alabama-kidnapper-was-killed-in-firefight-during-storming-bunker-fbi-says/.

[10] Ryan Gallagher, *Could the Pentagon's 1.8 Gigapixel Drone Camera Be Used for Domestic Surveillance*, Slate (Feb. 6, 2013), http://www.slate.com/blogs/future_tense/2013/02/06/argus_is_could_the_pentagon_s_1_8_gigapixel_drone_camera_be_used_for_domestic.html.

[11] *Id*.

[12] Customs and Border Protection Today, Unmanned Aerial Vehicles Support Border Security (July/Aug. 2004), *available at* http://www.cbp.gov/xp/CustomsToday/2004/Aug/other/aerial_vehicles.xml.

with technology for electronic signals interception and human identification.[13] Following receipt of these documents, EPIC and a broad coalition of privacy and civil liberties organizations petitioned the CBP to suspend the domestic drone program, pending the establishment of privacy safeguards.[14]

Much of this surveillance technology could, in theory, be deployed on manned vehicles. However, drones present a unique threat to privacy. Drones are designed to maintain a constant, persistent eye on the public to a degree that former methods of surveillance were unable to achieve. Drones are cheaper to buy, maintain, and operate than helicopters, or other forms of aerial surveillance.[15] Drone manufacturers have recently announced new designs that would allow drones to operate for more than 48 consecutive hours,[16] and other technology could extend the flight time of future drones into spans of weeks and months.[17] Also, "by virtue of their design, size, and how high they can fly, [drones] can operate undetected in urban and rural environments."[18]

Drones are currently being developed that will carry facial recognition technology, able to remotely identify individuals in parks, schools, and at political gatherings.[19] The ability to link facial recognition capabilities on drones operated by the Department of Homeland Security ("DHS") to the Federal Bureau of Investigation's Next Generation Identification database or DHS' IDENT database, two of the largest collections of biometric data in the world, further exacerbates the privacy risks.[20]

---

[13] Declan McCullagh, *DHS Built Domestic Surveillance Tech into Predator Drones*, CNET (Mar. 2, 2013), http://news.cnet.com/8301-13578_3-57572207-38/dhs-built-domestic-surveillance-tech-into-predator-drones/.

[14] Letter from the Electronic Privacy Information Center, et al. to David V. Aguilar, Deputy Commissioner, U.S. Bureau of Customs and Border Protection (Mar. 19, 2013), *available at* http://epic.org/drones_petition/.

[15] Nick Wingfield and Somini Sengupta, *Drones Set Sights on U.S. Skies*, NY Times (Feb. 17, 2012), *available at* http://www.nytimes.com/2012/02/18/technology/drones-with-an-eye-on-the-public-cleared-to-fly.html?pagewanted=all; http://www.wired.com/autopia/2012/05/drone-auto-vids/; Sabrina Hall, *Shelby County Sheriff's Department Wants Drones*, WREG (May 3, 2012), *available at* http://wreg.com/2012/05/03/shelby-county-sheriffs-department-wants-drones/. Drones can run from $300 for the most basic drone, able to record and transmit video, to $18 million for a General Atomics Predator B drone, the model owned by the United States Bureau of Customs and Border Protection. *See Parrot AR.Drone 2.0*, Apple, http://store.apple.com/us/product/H8859ZM/A (last visited July 16, 2012); Office of the Inspector Gen., Dep't Homeland Security, OIG-12-85, *CBPs Use of Unmanned Aircraft Systems in the Nation's Border Security* (May 2012), *available at* http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-85_May12.pdf [hereinafter *DHS OIG Report*] at 2.

[16] Mark Brown, *Lockheed Uses Ground-Based Laser to Recharge Drone Mid-Flight* (July 12, 2012), *available at* http://www.wired.co.uk/news/archive/2012-07/12/lockheed-lasers.

[17] Steven Aftergood, *Secret Drone Technology Barred by "Political Conditions"* (Mar. 22, 2012), *available at* http://www.fas.org/blog/secrecy/2012/03/sandia_drone.html.

[18] Jennifer Lynch, *Are Drones Watching You?*, Electronic Frontier Foundation (Jan. 10, 2012), *available at* https://www.eff.org/deeplinks/2012/01/drones-are-watching-you.

[19] Clay Dillow, *Army Developing Drones that Can Recognize Your Face From a Distance*, PopSci (Sept. 28, 2011, 4:01 PM), http://www.popsci.com/technology/article/2011-09/army-wants-drones-can-recognize-your-face-and-read-your-mind.

[20] *See Next Generation Identification*, Federal Bureau of Investigation, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2/ (last visited July 16, 2012); Privacy Impact Assessment,

Law enforcement offices across the country have expressed interest in the purchase and use of drone technology to assist with law enforcement operations. Records released in 2012 by the Federal Aviation Administration show that over 220 public entities have already received approval to operate drones over the United States, including Police departments from Texas, Kansas, Washington, and other states.[21] The Florida Police Chiefs Association expressed a desire to use drones to conduct general crowd surveillance at public events.[22] News reports demonstrate that other police departments are not only interested in invasive surveillance equipment, but have also voiced interest in outfitting drones with non-lethal weapons.[23]

II. Current Privacy Safeguards are Inadequate

The Supreme Court has not yet considered the limits of drone surveillance under the Fourth Amendment, though the Court held twenty years ago that law enforcement may conduct manned aerial surveillance operations from as low as 400 feet without a warrant.[24] In addition, no federal statute currently provides adequate safeguards to protect privacy against increased drone use in the United States. Accordingly, there are substantial legal and constitutional issues involved in the deployment of aerial drones by law enforcement and state and federal agencies that need to be addressed. Technologist and security expert Bruce Schneier observed earlier this year at an event hosted by EPIC on Drones and Domestic Surveillance, "today's expensive and rare is tomorrow's commonplace."[25] As drone technology becomes cheaper and more common, the threat to privacy will become more substantial. High-rise buildings, security fences, or even the walls of a building are not barriers to increasingly common drone technology.

The Supreme Court is aware of the growing risks to privacy resulting from new surveillance technology but has yet to address the specific problems associated with drone surveillance. In *United States v. Jones*, a case that addressed whether the police could use a GPS device to track the movement of a criminal suspect without a warrant, the Court found

---

Department of Homeland Security, Automated Biometric Identification System (IDENT) (July 31, 2006), http://www.dhs.gov/xlibrary/assets/privacy/privacy_pia_usvisit_ident_final.pdf.

[21] *See* letter from Michael Huerta, Acting Administrator, Federal Aviation Administration to the Honorable Edward J. Markey (Sept. 21, 2012), *available at* http://markey.house.gov/sites/markey.house.gov/files/documents/FAA%20drones%20response.pdf; *see also* Jennifer Lynch, *Just How Many Drone Licenses Has the FAA Really Issued*, Electronic Frontier Foundation (Feb. 21, 2013), https://www.eff.org/deeplinks/2013/02/just-how-many-drone-licenses-has-faa-really-issued (providing details on contradictory statements made by the Federal Aviation Adminstration regarding the issuance of drone licenses).

[22] *See Florida Ban on Drones Advances Despite Law Enforcement Objections*, Fox News (Feb. 7, 2013), http://www.foxnews.com/politics/2013/02/07/fla-police-want-to-use-drones-for-crowd-control/.

[23] *See* Conor Friedersdorf, *Congress Should Ban Armed Drones Before Cops in Texas Deploy One*, the Atlantic (May 24, 2012), http://www.theatlantic.com/national/archive/2012/05/congress-should-ban-armed-drones-before-cops-in-texas-deploy-one/257616/.

[24] *See Florida v. Riley*, 488 U.S. 445 (1989) (holding that a police helicopter flying more than 400 feet above private property is not a search).

[25] Drones and Domestic Surveillance, EPIC, http://epic.org/events/drones/ (last visited Mar. 15, 2013).

that the installation and deployment of the device was an unlawful search and seizure.[26] Justice Sotomayor in a concurrence pointed to broader problems associated with new forms of persistent surveillance.[27] And Justice Alito, in a separate concurrence joined by three other Justices, wrote, "in circumstances involving dramatic technological change, the best solution to privacy concerns may be legislative."[28]

Regarding the invasive use of drones by commercial operators, current law does not anticipate the use of mobile devices that can hover outside a bedroom window or follow a person down a street. Legal standards should be established to protect people from a violation of reasonable expectations of privacy, including surveillance in public spaces. In consideration legislation to address law enforcement use of drones, it would be appropriate also to establish privacy standards for the commercial use of drones.

III. Congress Should Establish Safeguards Related to the Use of Drones

As the Chairman has indicated, the privacy and security concerns arising from the use of drones needs to be addressed.[29] In order to mitigate the risk of increased use of drones in our domestic skies, Congress must pass targeted legislation, based on principles of transparency and accountability.

State and local governments have considered a wide array of laws and regulations to prevent abuses associated with drone technology.[30] A current survey demonstrates that over 30 states have proposed legislation to protect against unregulated drone surveillance of individuals.[31] Most of these bills mandate a warrant requirement for the collection of information by drones operated by law enforcement officials.[32] Other bills require

---

[26] *United States v. Jones*, 132 S.Ct. 945, 949 (2012). See also U.S. v. Jones, EPIC, http://epic.org/amicus/jones/.
[27] *Id.* at 954-57.
[28] *Id.* at 964.
[29] Press Release from Senator Patrick Leahy, *The Agenda of the Senate Judiciary Committee for the 113th Congress* (Jan. 16, 2013), *available at* http://www.leahy.senate.gov/press/113-sjc-agenda-speech (I am concerned about the growing use of drones by federal and local authorities to spy on Americans here at home. This fast-emerging technology is cheap and could pose a significant threat to the privacy and civil liberties of millions of Americans.").
[30] *See, e.g.,* Erika Neddenien, *ACLU Teams with Lawmaker to Push Regulation of Unmanned Drones in VA*, WTVR (July 12, 2012), http://wtvr.com/2012/07/12/aclu-working-with-lawmaker-to-push-regulation-of-unmanned-drones-in-va/; Press Release, Seattle City Council, Seattle City Council Committee to Discuss Drones in Seattle and the Issues they Present (May 1, 2012), *available at* http://council.seattle.gov/2012/05/01/seattle-city-council-committee-to-discuss-drones-in-seattle-and-the-issues-they-present/.
[31] Allie Bohm, *Status of Domestic Drone Legislation in the States*, American Civil Liberties Union (Mar. 14, 2013), http://www.aclu.org/blog/technology-and-liberty/status-domestic-drone-legislation-states.
[32] Allie Bohm, *Drone Legislation:What's Being Proposed in the States?*, American Civil Liberties Union (Mar. 6, 2013), http://www.aclu.org/blog/technology-and-liberty-national-security/drone-legislation-whats-being-proposed-states (Noting that states that have introduced a bill to require a warrant for police drone surveillance include Arizona, California, Florida, Georgia, Idaho, Illinois, Kentucky, Maryland, Massachusetts, Minnesota, Missouri, Montana, New Hampshire, New Mexico, North Dakota, Oklahoma, Oregon, Rhode Island, South Carolina, Tennessee, Texas, Washington, and Wyoming.).

reporting requirements for drone operators.[33] A bill in Georgia restricts law enforcement use of drones strictly to felony investigations,[34] and a bill circulating in Oregon would require state approval for all drones, including federal drones, that would fly over the state's airspace.[35]

Even as states consider these various measures, it would be appropriate for Congress to establish privacy standards for the operation of drones in the United States. First, Congress should require all drone operators, both public and commercial, to submit, prior to receipt of a drone license, a detailed report on the drones' intended use. This report should describe, the specific geographic are where the drone will be deployed, the mission that the drone is expected to fulfill, and the surveillance equipment with which the drone will be outfitted. Each of these reports should be made publicly available at a publicly accessible web site. A private right of action and, in certain instances, federal prosecution authority should be included to ensure that drone operators comply with the terms of these statements.

In order to prevent abuses associated with the use of this technology, a strict warrant requirement needs to be implemented for all drone surveillance conduct by law enforcement. A warrant requirement would establish a presumption that evidence obtained by means of an aerial search should require judicial approval. Statutory exceptions could be created for exigency in order to address drone use in emergency situations or when necessary to protect human life. In addition, mandatory public reporting requirements, similar to those required by the Wiretap Act, would increase the transparency and accountability of law enforcement drone operations.[36]

Ongoing surveillance of individuals by aerial drones operating in domestic airspace should be prohibited. The invasiveness of drone technology represents a privacy risks to individuals as they pursue their daily activities. A drone, with the capability of staying aloft for hours or days at a time, could monitor a person's entire life as they go from home to work to school to the store and back. Even if law enforcement is not able to immediately discern exactly what a person says or does or buys at a particular location, simply tracking an individual's public movements in a systematic fashion for extended periods of time can create a vivid description of their private life.[37] Broad, unregulated drone surveillance would have a chilling effect on the speech and expression rights of individuals in the United States. Drones should not be used as robotic patrol officers for law enforcement.

Finally, drone surveillance technology may allow the collection of information and images that would otherwise be inaccessible to prying eyes, such as activities within the home. Congress should prohibit drone operators from conducting surveillance of

---

[33] *See id.* (Noting that states that have introduced a bill that includes a reporting requirement include Hawaii, Illinois, Maine, Mass, Rhode Island, Washington.).
[34] *See id.*
[35] Oregon SB 71 (2013), *available at* www.leg.state.or.us/13reg/measures/sb0001.dor/sb0071.intro.html.
[36] *See* 18 U.S.C. § 2519.
[37] *See* EPIC: Locational Privacy, https://epic.org/privacy/location_privacy/default.html.

individuals that infringes on property rights. A federal "Peeping Tom" statute, recognizing the enhanced capabilities of aerial drones, would provide baseline privacy protection for individuals within the home. Additional provisions should prevent against any use of drones to collect information that would not otherwise be retrievable without a physical trespass.

Additional drone legislation should include:

- Use Limitations – Prohibitions on general surveillance that limit law enforcement drone surveillance to specific, enumerated circumstances, such as in the case of criminal surveillance subject to a warrant, a geographically-confined emergency, or for reasonable non-law enforcement use where privacy will not be substantially affected;

- Data Retention Limitations – Restrictions on retaining or sharing surveillance data collected by drones, with emphasis on personally identifiable information;

- Transparency and Public Accountability – A requirement for all federal agencies that choose to operate drones to promulgate privacy regulations, subject to the notice and comment provisions of the Administrative Procedure Act. In addition, the law should provide for third party audits and oversight for law enforcement drone operations.

These three principles would further help protect the privacy interests of individuals against both government and commercial drone operators.

IV. Conclusion

The increased use of drones to conduct surveillance in the United States must be accompanied by increased privacy protections. The current state of the law is insufficient to address the drone surveillance threat. EPIC supports legislation aimed at strengthening safeguards related to the use of drones as surveillance tools and allowing for redress for drone operators who fail to comply with the mandated standards of protection. We also support compliance with the Administrative Procedure Act for the deployment of drone technology and limitations for federal agencies and other organizations that initially obtain a drone for one purpose and then wish to expand that purpose.

Thank you for the opportunity to testify today. I will be pleased to answer your questions.