Testimony and Statement for the Record of

Amie Stepanovich
Association Litigation Counsel
Electronic Privacy Information Center

Field Forum on the Impact of Domestic Use of Drone Technology on Privacy and Constitutional Rights of All Americans

Hosted by Congressman Ted Poe and
Sanctioned by the

Subcommittee on Crime, Terrorism,
and Homeland Security
of the
U.S. House of Representatives,
Committee on the Judiciary

October 25, 2012
Rice University
Houston, Texas

Congressman Poe, Members of the House Judiciary Committee, and distinguished guests, thank you for the opportunity to testify today concerning the privacy and the Constitutional rights of all Americans and the increasing use of unmanned aerial vehicles, or "drones," in the United States. My name is Amie Stepanovich. I am the Associate Litigation Counsel 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 are focused on the protection of individual privacy rights. In the last several years, EPIC has taken a particular interest in the unique privacy problems associated with aerial drones. EPIC and a broad coalition of organizations, has urged the Federal Aviation Administration ("FAA") to develop new privacy safeguards before drones are more widely deployed in the United States.[3]

EPIC supports H.R. 6199, the Preserving American Privacy Act of 2012. The bill is an important first step toward safeguarding fundamental privacy rights. We recommend additional provisions to protect privacy. In my statement today, I will describe the unique threats to privacy posed by domestic drone use and the need for a warrant requirement to protect against pervasive drone surveillance. I will further discuss the problems with the current state of privacy law in relation to domestic drone use and EPIC's petition to the Federal Aviation Administration ("FAA") asking for privacy regulations related to the use of drones.

We appreciate your efforts and the efforts of the cosponsors of your legislation to help address growing public concern about drone surveillance in the United States.

I. Law Enforcement Use of Drones Poses a Unique Threat to Privacy

An unmanned aircraft, or 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 equipped with sophisticated surveillance technology that makes it possible to identify individuals on the ground. Gigapixel cameras used to outfit drones are among the highest definition cameras available.[4] On some drones, sensors can track up to 65 different targets across a distance of 65 square miles.[5] Drones may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers.[6] Drones

---

[1] *About EPIC*, EPIC, http://www.epic.org/about (last visited Oct. 22, 2012).
[2] *EPIC Advisory Board*, EPIC, http://www.epic.org/epic/advisory_board.html (last visited Oct. 22, 2012).
[3] *Unmanned Aerial Vehicles (UAVs) and Drones*, EPIC, http://www.epic.org/privacy/drones (last visited Oct. 22, 2012).
[4] *US Army Unveils 1.8 Gigapixel Camera Helicopter Drone*, BBC News Technology (Dec. 29, 2011), http://www.bbc.co.uk/news/technology-16358851.
[5] *Id*.
[6] 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 ("UAVs are equipped with image recognition systems and sensors that can detect movement, read a license plate

are currently being developed that will carry facial recognition technology, able to remotely identify individuals in parks, schools, and at political gatherings.[7]

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."[8] Today, drones greatly increase the capacity for domestic surveillance.

Much of this surveillance technology could, in theory, be deployed in manned vehicles. However, drones present a unique threat to privacy. Drones are designed to undertake constant, persistent surveillance 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.[9] Drone manufacturers have recently announced new designs that would allow drones to operate for more than 48 consecutive hours,[10] and other technology could extend the flight time of future drones out into weeks and months.[11] Also, "by virtue of their design, size, and how high they can fly, [drones] can operate undetected in urban and rural environments."[12]

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

---

number, or even identify vehicle occupants from 15 miles away. Infrared sensors provide day and night imaging."); *see also* Congressional Research Service, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses* (Sept. 6, 2012), *available at* http://www.fas.org/sgp/crs/natsec/R42701.pdf ("Currently, drones can be outfitted with high-powered cameras, thermal imaging devices, license plate readers, and laser radar (LADAR).").

[7] 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.

[8] *Spotlight on Surveillance: Unmanned Planes Offer New Opportunities for Clandestine Government Tracking* (August 2005), EPIC, http://epic.org/privacy/surveillance/spotlight/0805/ (last visited Oct. 22, 2012).

[9] 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 Oct. 22, 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.

[10] 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.

[11] 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.

[12] 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.

of biometric data in the world, exacerbates the privacy risks.[13] Drones can be deployed to monitor individuals in a way that was not previously possible.

II. A Warrant Should Be Necessary For All Targeted Drone Surveillance

Law enforcement offices across the country have expressed interest in the purchase and use of drone technology to assist with official operations. Records released earlier this year by the Federal Aviation Administration show that over sixty public entities have already received approval to operate drones over the United States, including Police departments from Texas, Florida, Kansas, Washington, and other states. News reports demonstrate that these departments are not only interested in invasive surveillance equipment, but in some cases have also voiced interest in outfitting drones with both lethal and non-lethal weapons.

A. Sophisticated Drone Technology Erodes Privacy Rights Within the United States

Widespread use of drone technology increases the potential for pervasive mass surveillance of the American public by law enforcement. In order to prevent abuses associated with the use of this technology, a strict warrant requirement needs to be implemented for all drone surveillance, including both felony and non-felony crimes. Requiring a warrant would safeguard privacy without preventing the use of drones in emergency situations. In addition, public reporting requirements, such as those mandated by the Wiretap Act, would increase the transparency and accountability of law enforcement drone operations.[14]

The Supreme Court has not yet tested the limits of drone surveillance under the Fourth Amendment, though the current constitutional standard allows law enforcement to conduct aerial surveillance operations from as low as 400 feet without a warrant.[15] In addition, no statute currently provides adequate safeguards to protect privacy against increased drone use in the United States.

As drone technology becomes cheaper and more prolific, the threat to privacy will become even more substantial. High-rise apartments, security fences, and even the walls of a building are not barriers to increasingly common drone technology. [16] Without the protection of a warrant requirement, individuals in the United States will find that the

---

[13] *See Next Generation Identification*, Federal Bureau of Investigation, http://www.fbi.gov/about-us/cjis/fingerprints_biometrics/ngi/ngi2/ (last visited Oct. 22, 2012); Privacy Impact Assessment, 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.

[14] *See* 18 U.S.C. § 2519.

[15] *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).

[16] The Supreme Court has emphasized the public availability of invasive surveillance technology in order to determine if law enforcement may use it to conduct surveillance without a warrant under the Fourth Amendment. *See Kyllo v. United States*, 533 U.S. 27 (2001); *Dow Chemical Co. v. U.S.*, 476 U.S. 227 (1986).

intimate details of their daily activities are freely available to the roving eyes of the government.

B. Current Warrant Exceptions Are Sufficient to Allow Law Enforcement Drones To Operate In Emergency Situations

Requiring a warrant would safeguard privacy while still ensuring that drones can be used when necessary. The courts have carefully developed and cultivated the warrant requirement over time. This process has crafted a set of exceptions to ensure that warrants do not hinder effective law enforcement.[17] Because of this robust and evolving backdrop of constitutional law and precedent, there is no need for Congress to create new warrant exceptions alongside warrant requirements for drones.

Chief among the warrant exceptions relevant to drone surveillance are the border crossing exemption and the exigent circumstances exception. The exigent circumstances exception allows a search or seizure to take place without a warrant in certain emergency situations. The law displaces the warrant requirement when there is an imminent danger to a person, property, or evidence, or when there is the risk of a suspect escaping.[18]

Law enforcement officials point to the use of drones to combat fires, conduct search and rescue operations, survey hostage situations, and monitor high-speed pursuits without placing the life or safety of a first responder in jeopardy. The exigent circumstances exception to the warrant requirement would allow law enforcement to use drone technology when necessary in each of these emergency situations.[19] Further, because current law gives broad deference to the Customs and Border Patrol to regulate border crossings, no new exceptions are needed for the use of drone surveillance of U.S. borders.[20]

III. Broad, Untargeted Drone Surveillance Must Be Prohibited

---

[17] Recognized warrant exceptions include: consent; exigent circumstances; motor vehicle exceptions; border searches; searches incident to arrest; administrative searches; limited public school searches; and stop and frisk.

[18] *See, e.g., People v. Ramey*, 545 P.2d 1333, 1341 (Cal. 1976) ("'[E]xigent circumstances' means an emergency situation requiring swift action to prevent imminent danger to life or serious damage to property, or to forestall the imminent escape of a suspect or destruction of evidence. There is no ready litmus test for determining whether such circumstances exist, and in each case the claim of an extraordinary situation must be measured by the facts known to the officers."); *See also Tamez v. City of San Marcos*, 118 F.3d 1089, 1093-1094 (5th Cir. 1997); *Minnesota v. Olson*, 495 U.S. 91, 100 (1990); *Brigham City v. Stuart*, 547 U.S. 398 (2006) (holding that police officers can enter a home without a warrant under exigent circumstances doctrine when physical injury or threat of physical injury exists); *Michigan v. Tyler*, 436 U.S. 499 (1978) (holding that no warrant is required to enter property to fight a fire or investigate immediately thereafter); *Warden v. Hayden*, 387 U.S. 294 (1967) (holding that no warrant is required when officers are in "hot pursuit").

[19] For a further discussion of the warrant exceptions as they pertain to potential drone surveillance, *see* Congressional Research Service, *Drones in Domestic Surveillance Operations: Fourth Amendment Implications and Legislative Responses* (Sept. 6, 2012), *available at* http://www.fas.org/sgp/crs/natsec/R42701.pdf.

[20] Under existing authority, the Border Patrol can use drones to surveil actual borders and functional equivalents, such as airports and seaports. *See, e.g., United States v. Ramsey*, 431 U.S. 606 (1977).

Drones should not be used as robotic patrol officers for law enforcement. The invasiveness of drone technology increases privacy risks to individuals as they pursue their daily activities. Broad, untargeted drone surveillance would have a chilling effect on the speech and expression rights of individuals in the United States.

A. Widespread Drone Surveillance Should Be Considered a Search Under the Fourth Amendment

The use of drones to survey broad, populated areas should be considered a search under the Fourth Amendment. Until recently there have been effective practical limitations operating as a constraint on persistent law enforcement surveillance. A drone, with the capability of staying aloft for hours or days at a time, could monitor a person's daily life as they go from home to work to school to the store and back. Even if law enforcement is not able to 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.[21]

The Supreme Court is aware of the growing risks to privacy resulting from new surveillance technology but has yet to tackle 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 for a prolonged period, the Court found that the installation and deployment of the device was an unlawful search and seizure.[22] In a concurring opinion, Justice Sotomayor pointed to the broader problems associated with new forms of persistent surveillance.[23] 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."[24]

The use of drones to conduct broad surveillance would also discourage individuals in the United States from engaging in lawful speech and expression.[25] Law enforcement surveillance of peaceful protests in the United States is increasingly common.[26] Justice

---

[21] *See* EPIC: Locational Privacy, https://epic.org/privacy/location_privacy/default.html.
[22] *United States v. Jones*, 132 S.Ct. 945, 949 (2012). See also U.S. v. Jones, EPIC, http://epic.org/amicus/jones/.
[23] *Id.* at 954-57.
[24] *Id.* at 964.
[25] *See United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.,* 407 U.S. 297(1972).
[26] *See e.g.*, Martine Powers, *Boston Police Accused of Spying on Antiwar Groups*, Boston Globe (Oct. 18, 2012), http://bostonglobe.com/metro/2012/10/17/boston-police-accused-surveillance-antiwar-protesters/7P0iOs86Q637BGYxI1ARBJ/story.html; Colin Moynihan, *Accusations of Police Misconduct Documented in Lawyers' Report on Occupy Protests*, N.Y. Times City Room Blog (Jul. 25, 2012), http://cityroom.blogs.nytimes.com/2012/07/25/accusations-of-police-misconduct-documented-in-lawyers-report-on-occupy-protests/; Jennifer Sullivan, *ACLU protests UW police surveillance on student social-justice group*, Seattle Times (Jul. 8 2010), http://seattletimes.com/html/localnews/2012312486_surveillance09m.html; Ben Nuckols*, Files show Md. police watched variety of activists*, InfoWars (Nov. 19, 2008), http://www.infowars.com/files-show-md-police-watched-variety-of-activists/; Jim Dwyer*, Police Infiltrate Protests, Videotapes Show*, N.Y. Times (Dec. 22, 2005), http://www.nytimes.com/2005/12/22/nyregion/22police.html?pagewanted=all&_r=0; David Johnston and William K. Rashbaum, *Vast Force is Deployed for Security at Convention,* N.Y. Times (Aug. 25,

Powell discussed the chilling effect of pervasive surveillance: "[t]he price of lawful public dissent must not be a dread of subjection to an unchecked surveillance power. Nor must the fear of unauthorized official eavesdropping deter vigorous citizen dissent and discussion of Government action in private conversation. For private dissent, no less than open public discourse, is essential to our free society."[27]

B. Environmental or Regulatory Monitoring Using Drones Must Protect Privacy

In some cases, federal agencies may wish to use drones for monitoring purposes that do not include the surveillance of individuals, such as monitoring for compliance with environmental regulations. In these cases, the agencies should be required to take all precautions to avoid populated areas and to comply with the Privacy Act of 1974 for any incidental collection of personal information.

The Privacy Act of 1974 expressly prescribes circumstances under which federal agencies can retain personally identifiable information. The Act's provisions should expressly be applied to any database that includes information collected by drones and should require that only the minimum amount of information necessary can be retained. Whenever possible, personally identifiable information captured by drones incident to other monitoring should be immediately purged.

IV. The FAA, in Conjunction with other Federal Agencies, Should Be Charged with Oversight of Domestic Drone Use

Congress has directed the FAA to develop regulations to permit wider deployment of drones in the United States.[28] The forthcoming regulations will address licensing and procedures for both public and private drone operators, including law enforcement. Experts, including Professor Ryan Calo, the former Director of Privacy and Robotics at the Center for Internet and Society at Stanford Law School, have noted that this effort will have significant privacy implications.[29]

2004), http://www.nytimes.com/2004/08/25/world/threats-responses-investigation-vast-force-deployed-for-security-convention.html?pagewanted=all&src=pm; *Denver Police Settle Lawsuit Over Secret Files*, St. Louis Post-Dispatch (Apr. 18, 2003), http://nl.newsbank.com/nl-search/we/Archives?p_product=SL&p_theme=sl&p_action=search&p_maxdocs=200&p_topdoc=1&p_text_direct-0=0FA8172957C04DC1&p_field_direct-0=document_id&p_perpage=10&p_sort=YMD_date:D&s_trackval=GooglePM; *Cameras Cover D.C. protests*, Pittsburgh Post-Gazette, Dec. 21, 2002, at A5, *available at* http://news.google.com/newspapers?nid=1129&dat=20021221&id=M_ANAAAAIBAJ&sjid=1HADAAAAIBAJ&pg=6057,25373.

[27] *United States v. U.S. Dist. Court for E. Dist. of Mich., S. Div.,* 407 U.S. 297, 314 (1972).

[28] *See* FAA Modernization and Reform Act of 2012, Pub. L. 112-95 §324(c)(1) (2012), available at http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.658:.

[29] *See,* M. Ryan Calo, *The Drone as a Privacy Catalyst*, 64 Stan. L. Rev. Online 29 (2011), *available at* http://www.stanfordlawreview.org/online/drone-privacy-catalyst; *see also* Ryan Calo and John Villasenor, *Ten Myths About Drones*, Huffington Post (May 22, 2012), http://www.huffingtonpost.com/ryan-calo/drones-myths_b_1537040.html; *Drones Over America: What Can They See,* NPR (Mar. 12, 2012), *available at* http://www.npr.org/2012/03/12/148293470/drones-over-america-what-can-they-see.

Earlier this year, in a formal petition to the agency, EPIC urged the FAA to conduct a privacy rulemaking on the use of drones, with the aim of creating regulations to ensure baseline privacy protections.[30] EPIC's petition was joined by more than one hundred organizations, experts, and members of the public who also believe that drones should not be further deployed until privacy safeguards are established.[31]

Among other recommendations, EPIC urged the FAA to promulgate rules that require all domestic drone operators to report specific information about their intended operations, including the technology the drone would carry, the specific purpose of the drone, and the geographic area within which the drone will operate. As the administrative agency with the statutory authority to issue drone operation licenses and maintain order in the national airspace, the FAA is the most appropriate agency to oversee these regulations.

The FAA has thus far failed to respond to EPIC's request for agency action. The FAA's failure to act means that there is no framework in place that ensures that civilian operators and federal agencies, such as local law enforcement agencies, use drone technology in a privacy-protective manner. To the extent that public entities choose to operate drones within the United States, we believe that those entities should also develop appropriate regulations to safeguard privacy.

V. Congressional Safeguards to Limit Drones Should Include Measures to Ensure Transparency and Accountability of Drone Operations

There are several meaningful privacy protections that can address the increased use of drones in our domestic skies. Congress should pass comprehensive legislation based on principles of transparency and accountability. H.R. 6199, the Preserving American Privacy Act of 2012, introduced by Congressman Poe, aims to limit drone surveillance by mandating a strict warrant requirement for most drone surveillance conducted for law enforcement purposes. H.R. 6199 also prevents drones from being used to monitor private property without consent of the owner.

EPIC supports H.R. 6199. However, EPIC also recommends additional provisions in order to protect the privacy of individuals in the United States from growing drone surveillance. Additional drone legislation should include:

- Use Limitations – Prohibitions on general surveillance that limit 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 – Prohibitions on retaining or disclosing surveillance data collected by drones, with emphasis on identifiable images of individuals;

[30] Petition from EPIC, *et al.*, to Michael P. Huerta, Acting Administrator, FAA (Feb. 24, 2012), *available at* http://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.
[31] *Id.*

- Transparency –Requirements for notice of drone surveillance operations to the extent possible while allowing law enforcement to conduct effective investigations and notice of all drone surveillance policies through the Administrative Procedure Act. Also, reporting requirements for warrants issued for law enforcement use of drones to conduct surveillance operations.

These three principles would help protect the privacy interests of individuals. In addition, the law should provide for accountability, including third party audits and oversight for federally operated drones and a private right of action against private entities that violate statutory privacy rights.

Finally, all federal agencies that choose to operate drones, such as DHS and its components, must be required to implement regulations, subject to public notice and comment, that address the privacy implications of drone use. Recently, in *EPIC v. DHS,* the D.C. Circuit Court of Appeals ruled that the Department of Homeland Security violated the Administrative Procedure Act when it chose to deploy body scanners as the primary screening technique in U.S. airports without the opportunity for public comment.[32] The Court observed that there was "no justification for having failed to conduct a notice-and-comment rulemaking."[33] We believe that the public has a similar right to comment on new surveillance techniques, such as unmanned aerial vehicles, undertaken by federal agencies within the United States.

VI. 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. We support H.R. 6199 and a warrant requirement for all drone surveillance in the United States. We also support public reporting requirements for all drone warrants and privacy regulations for drones, accompanied by meaningful agency oversight.

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

[32] *See EPIC v. DHS*, 653 F.3d 1 (D.C. Cir. 2011).
[33] *Id.* at 8.