Testimony and Statement for the Record of

Amie Stepanovich
Association Litigation Counsel
Electronic Privacy Information Center

Hearing on "Using Unmanned Aerial Systems Within the Homeland: Security Game Changer?"

Before the

Subcommittee on Oversight,
Investigations, and Management
of the
U.S. House of Representatives,
Committee on Homeland Security

July 19, 2012
311 Cannon House Office Building
Washington, D.C.

Mister Chairman and Members of the Subcommittee, thank you for the opportunity to testify today concerning unmanned aerial systems, 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 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. We have urged the Federal Aviation Administration ("FAA"), as it considers new regulations to permit the widespread deployment of drones, to also develop new privacy safeguards.[3]

In my statement today, I will describe the unique threats to privacy posed by drone surveillance, the problems with current legal safeguards, the EPIC petition to the FAA, and the need for Congress to act.

We appreciate the Subcommittee's interest in domestic drone use and its substantial impact on the privacy of individuals in the United States.

I. Aerial Drones Pose 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 weaponized and deployed for military purposes.[4] Drones can also 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, and can provide "real-time video streams at a rate of 10 frames a second."[5] On some drones, sensors can track up to 65 different targets across a distance of 65 square miles.[6] Drones may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers.[7] Drones are currently being developed

---

[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] *Unmanned Aerial Vehicles (UAVs) and Drones*, EPIC, http://www.epic.org/privacy/drones (last visited July 16, 2012).
[4] *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).
[5] *US Army Unveils 1.8 Gigapixel Camera Helicopter Drone*, BBC News Technology (Dec. 29, 2011), http://www.bbc.co.uk/news/technology-16358851.
[6] *Id*.
[7] 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.

that will carry facial recognition technology, able to remotely identify individuals in parks, schools, and at political gatherings.[8]

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."[9] 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.[10] Drone manufacturers have recently announced new designs that would allow drones to operate for more than 48 consecutive hours,[11] and other technology could extend the flight time of future drones out into weeks and months.[12] Also, "by virtue of their design, size, and how high they can fly, [drones] can operate undetected in urban and rural environments."[13]

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, exacerbates the privacy risks.[14] Drones could be deployed to monitor individuals in a way that was not possible previously.

---

[8] 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.

[9] *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).

[10] 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.

[11] 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.

[12] 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.

[13] 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.

[14] *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,

Sensitive information collected by drones is particularly vulnerable to unlawful access. In comments addressing the issue of drone test site locations, EPIC observed, "'drone hacking,' or the process of remotely intercepting and compromising drone operations, poses a threat to the security of lawful drone operations. [15] Recent examples have highlighted the ease with which drones may be "hacked". The University of Texas was able to use GPS signals in order to gain full control of a drone.[16] The researchers indicated that the method could be use on any drone operated over the civilian GPS band, which include the majority of drones in the United States.[17] Hackers are also able to intercept video and audio feeds, as well as other information collected and transmitted by surveillance drones.[18]

Within DHS, the Bureau of Customs and Border Protection ("CBP") is the primary operator of unmanned aerial drones. CBP operates ten drones in the United States, including the Predator B and its maritime variant the Guardian, at a cost per unit of about $18 million each.[19] By 2016, CBP plans to operate twenty-four drones, with the ability to deploy one anywhere in the continental United States within three hours.[20]

But there are problems with the CBP program. According to a recent report of the DHS Inspector General, CBP "needs to improve planning of its unmanned aircraft systems program to address its level of operation, program funding, and resource requirements, along with stakeholder needs."[21] The Inspector General assessed CBP's practice of making the drones available for use by other federal and state agencies, including the Bureau of Land Management, the Department of Defense, the Federal Bureau of Investigation, the Texas Rangers, the United States Forest Service, the National Oceanic and Atmospheric Administration, the Office of Border Patrol, the United States Secret Service, the Immigrations and Customs Enforcement, the Federal Agency Management Agency, and local Law Enforcement Agencies.[22]

The Inspector General concluded that all purchases of new drones should be suspended until CBP develops a plan that addresses "necessary operations, maintenance,

---

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.

[15] Comments of EPIC to the FAA re: Request for Comments on Unmanned Aircraft System Test Sites (May 8, 2012), *available at* http://epic.org/privacy/drones/EPIC-FAA-2012-0252.pdf.

[16] Alex Fitzpatrick, *Researchers Prove Drones Can Be Hacked*, Mashable (June 29, 2012), *available at* http://mashable.com/2012/06/29/drone-hacking/.

[17] *Id*.

[18] Siobhan Gorman, Yochi Dreazen, and August Cole, *Insurgents Hack U.S. Drones*, Wall St. J. (Dec. 17, 2009), *available at* http://online.wsj.com/article/SB126102247889095011.html.

[19] *See DHS OIG Report, supra* note 11 at 2.

[20] William Booth, *More Predator Drones Fly U.S.-Mexico Border*, WASH. POST (Dec. 21, 2011), *available at* http://www.washingtonpost.com/world/more-predator-drones-fly-us-mexico-border/2011/12/01/gIQANSZz80_story.html.

[21] *See DHS OIG Report, supra* note 11 at 1.

[22] *Id*. at 6-7.

and equipment."[23] Regarding privacy concerns, the DHS Inspector General said that a standardized process was needed to request CBP drones for non-CBP purposes, in order to "provide transparency."[24]

II. Current Privacy Safeguards are Inadequate

Current regulations permit civil organizations to operate a drone within the United States only pursuant to a special "experimental" designation.[25] However, government operators of drones do not have a similar restriction.[26] Recent policy changes at the FAA, the administrative agency in charge of licensing both governmental and non-governmental drones to operate in the National Airspace, are designed to "streamline" the process by which government agencies, including law enforcement, receive drone licenses.[27]

The CBP currently operates drones with few regulations concerning privacy. No current legislation limits the visual surveillance that a DHS drone may engage in. And while the Privacy Act of 1974 expressly prescribes the circumstances under which agencies can retain personally identifiable information, the Agency may still exempt itself from the Privacy Act provisions that limit the collection and use of personal information.[28] DHS has not sought public comment on or published any specific rules or guidelines that restrict the surveillance practices of its drone program. Also, despite recent releases of records, the FAA's process for the application for and approval of a drone license are still mostly opaque, preventing any transparency or accountability for operators.[29]

There are substantial legal and constitutional issues involved in the deployment of aerial drones by federal agencies that need to be addressed. And, as we have noted, no legislation currently provides adequate safeguards to protect privacy rights against the increased use of drones in the United States.

---

[23] *Id.* at 8

[24] *Id.* at 7.

[25] *See* Fact Sheet, FAA, Unmanned Aircraft Systems (UAS) (Dec. 1, 2010), *available at* http://www.faa.gov/news/fact_sheets/news_story.cfm?newsid=6287 ("A Special Airworthiness Certificate in the Experimental Category is the only certification available to civil operators of UAS.").

[26] *See Id.* ("The COA process is available to public entities, such as government agencies (including local law enforcement and state universities), who want to fly a UAS in civil airspace.").

[27] *See FAA Makes Progress with UAS Integration*, Federal Aviation Administration, (May 14, 2012, 3:09 PM) http://www.faa.gov/news/updates/?newsId=68004 ("The FAA has been working with its government partners to streamline COA procedures as part of the effort to ensure [drones] are safely integrated into the [national airspace system].").

[28] *See e.g.* 5 U.S.C. § 552a(j) (allowing agencies to exempt themselves from maintenance requirements pursuant to law enforcement reasons).

[29] *See FAA Releases Lists of Drone Certificates–Many Questions Left Unanswered*, Electronic Frontier Foundation, (Apr. 19, 2012) https://www.eff.org/deeplinks/2012/04/faa-releases-its-list-drone-certificates-leaves-many-questions-unanswered (listing information about the FAA's drone authorization process that remains unknown).

As drone technology becomes cheaper and more proliferate, 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 that the installation and deployment of the device was an unlawful search and seizure.[30] Justice Sotomayor in a concurrence pointed to broader problems associated with new forms of persistent surveillance.[31] 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."[32]

As you have indicated, Mister Chairman, the privacy and security concerns arising from the use of drones needs to be addressed.[33] Several of your colleagues in the House of Representatives have made efforts to address some of the privacy threats of drones, and we support these initiatives.

An amendment to the National Defense Authorization Act of 2013, introduced by Congressman Jeff Landry (R-LA) and passed by the House, would prohibit information collected by drones operated by the Department of Defense from being used in court as evidence if a warrant was not obtained.[34] In June, House Representative Austin Scott (R-FL) introduced legislation to expand this protection, requiring all law enforcement to first obtain a warrant before conducting any criminal surveillance.[35] Also, Congressman Markey (D-MA) and Congressman Barton (R-TX) sent a letter to the FAA raising concerns about the increased use of Drones in the United States, noting, "there is . . . potential for drone

---

[30] *United States v. Jones*, 132 S.Ct. 945, 949 (2012). See also U.S. v. Jones, EPIC, http://epic.org/amicus/jones/.
[31] *Id.* at 954-57.
[32] *Id.* at 964.
[33] Press Release, United States House of Representatives Committee on Homeland Security, A Look Ahead: House Committee on Homeland Security (July 13, 2012), *available at* http://homeland.house.gov/press-release/look-ahead-house-committee-homeland-security-34 ("However, no Federal agency is taking responsibility for creating comprehensive policies and regulations concerning the use of these systems domestically. Additionally, vulnerabilities to 'drone' hackers exist, as recently demonstrated by researchers at the University of Texas, raising concerns these vehicles could be commandeered by terrorists or others with ill intent.").
[34] *See* H.R. 4310, 112th Cong. § 1084 (2012), *available at* http://www.gpo.gov/fdsys/pkg/BILLS-112hr4310rfs/pdf/BILLS-112hr4310rfs.pdf; *see also* Pete Kasperowicz, *House Approves 20 en bloc Amendments to Defense Reauthorization, Including Satellite Language*, the Hill (May 17, 2012), *available at* http://thehill.com/blogs/floor-action/house/228147-ndaa-update-1-house-approves-20-en-bloc-amendments-including-satellite-language.
[35] Preserving Freedom from Unwarranted Surveillance Act of 2012, H.R. 5925, 112th Cong. (2012), *available at* http://thomas.loc.gov/cgi-bin/query/z?c112:H.R.5925:.

technology to enable invasive and pervasive surveillance without adequate privacy protections."[36]

However, these measures are not sufficient to protect the myriad of privacy interests implicated by increased drone use.

III. EPIC Has Urged the Administrative Action to Address Drone Use

The FAA has been directed by Congress to developed regulations in order to permit more widespread deployment of drones in the United States.[37] The forthcoming regulations will address licensing and procedures for both public and private drone operators, including DHS and CBP. 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..[38]

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.[39] 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 more widely deployed until privacy safeguards are established.[40]

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 DHS, utilize drone technology in a privacy-protective manner. To the extent that DHS, as well as other agencies, chooses to operate drones within the United States, we believe that the DHS should also develop appropriate regulations to safeguard privacy.

Specifically, the Department of Homeland Security must utilize its Privacy Office, one of the most robust, well-funded Privacy Offices in the federal government. The Privacy Office at DHS "conducts [Privacy Impact Assessments] on technologies, rulemakings,

---

[36] Letter from Congressmen Edward J. Markey and Joe Barton to Michael Huerta, Acting Federal Aviation Administration Administrator (Apr. 19, 2012) available at http://markey.house.gov/sites/markey.house.gov/files/documents/4-19-12.Letter%20FAA%20Drones%20.pdf.

[37] *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:.

[38] *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.

[39] 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 [hereinafter *EPIC Petition to FAA*].

[40] *Id.*

programs, and activities . . . to ensure that privacy considerations and protections are incorporated into all activities of the Department."[41]

However, despite a DHS component operating one of the largest, and definitely the most well publicized drone fleet in the United States for the past seven years, a Privacy Impact Assessment has never been conducted on the privacy impact of drone surveillance. At a minimum, we believe that if the CPB plans to continue the drone program, the DHS privacy office must assess the privacy impact of the program and publish a report for public review.

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

There are several strategies to provide meaningful privacy protections that address the increased use of drones in our domestic skies. First, Congress should pass targeted legislation, based on principles of transparency and accountability. A first step would be the consideration and passage of Congressman Scott's bill to limit the use of drone surveillance in criminal investigations without a warrant.

State and local governments have also considered laws and regulations to further prevent abuses of drone technology.[42] These proposals would serve as a good basis for federal legislation. 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 sharing surveillance data collected by drones, with emphasis on identifiable images of individuals;
- Transparency –Requiring notice of drone surveillance operations to the extent possible while allowing law enforcement to conduct effective investigations. In addition, requiring notice of all drone surveillance policies through the Administrative Procedure Act.

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.

---

[41] Guide to Implementing Privacy, Department of Homeland Security (June 2010), http://www.dhs.gov/xlibrary/assets/privacy/dhsprivacyoffice-guidetoimplementingprivacy.pdf at 14

[42] *See, e.g.,* Erika Neddenien, *ACLU Teams with Lawmaker to Push Regulation of Unmanned Drones in VA*, WTVR (July 12, 2012http://wtvr.com/2012/07/12/aclu-working-with-lawmaker-to-push-regulation-of-unmanned-drones-in-va/ (last visited July 16, 2012); 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/.

Second, Congress should act to expressly require federal agencies that choose to operate drones, such as DHS and its components, 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.[43] The Court observed that there was "no justification for having failed to conduct a notice-and-comment rulemaking."[44] 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.

Finally, Congress must clarify the circumstances under which the drones purchased by the CBP in pursuit of its mission may be deployed by other agencies for other purposes. The failure to make clear the circumstances when federal and state agencies may deploy drones for aerial surveillance has already raised significant concerns about the agency's program.[45]

V. Conclusion

The increased use of drones to conduct surveillance in the United States must be accompanied by increased privacy protections. We recognize that drone technology has the potential to be used in positive ways. For example, drones may be used to monitor for environmental abuse, prevent the spread of forest fires, and assist in the rescue of individuals in dangerous situations.[46]

However, 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.

---

[43] *See EPIC v. DHS*, 653 F.3d 1 (D.C. Cir. 2011).
[44] *Id.* at 8.
[45] *See* Jason Koebler, *First Man Arrested with Drone Evidence Vows to Fight Case*, US News (Apr. 9, 2012), *available at* http://www.usnews.com/news/articles/2012/04/09/first-man-arrested-with-drone-evidence-vows-to-fight-case.
[46] *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.

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