epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

Testimony and Statement for the Record of

Jeramie D. Scott
Director of the Domestic Surveillance Project
Electronic Privacy Information Center

Public Hearing on the "Use of Unmanned Aerial Vehicles (Drones)"

Before the

Majority Policy Committee

of the

Pennsylvania State Senate

March 15, 2016
Hearing Room No. 1, North Office Building
Harrisburg, PA 17120

Chairman Argall, Vice-Chair Reschenthaler, and members of the Senate Majority Policy Committee, thank you for the opportunity to testify today concerning the use of unmanned aerial vehicles or, as they are more commonly referred to, drones. My name is Jeramie Scott, and I am the Director of the Domestic Surveillance Project at the Electronic Privacy Information Center or simply EPIC.

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.

EPIC has contributed to the government's understanding of the privacy implications of domestic drone use through amicus briefs,[3] federal and state testimony,[4] and comments to federal agencies.[5] Immediately after Congress directed the Federal Aviation Administration ("FAA") to fully integrate drones into the National Airspace by 2015,[6] EPIC petitioned[7] the FAA to conduct a public rulemaking on the privacy impact of domestic drones. After the FAA denied our petition, EPIC filed a lawsuit for the agency's failure to establish privacy rules for commercial drones.[8]

---

[1] *About EPIC*, EPIC, http://www.epic.org/about (last visited March 11, 2016).
[2] *EPIC Advisory Board*, EPIC, http://www.epic.org/epic/advisory_board.html (last visited March 11, 2016).
[3] *See, e.g.*, Brief for EPIC as Amicus Curiae Supporting Respondent, *State v. Davis* (No. 34,548) *available at* https://epic.org/amicus/drones/new-mexico/davis/EPIC-Amicus-Brief.pdf.
[4] *See, e.g.*, *The Future of Drones in America: Law Enforcement and Privacy Considerations Before S. Judiciary Comm.*, 113th (2013) (statement of Amie Stepanovich, Director of the Domestic Surveillance Project, EPIC), *available at* https://epic.org/privacy/testimony/EPIC-Drone-Testimony-3-13-Stepanovich.pdf.
[5] *See, e.g.*, Comments of EPIC on Operation and Certification of Small Unmanned Aircraft Systems (Apr. 24, 2015), *available at* https://epic.org/privacy/litigation/apa/faa/drones/EPIC-FAA-NPRM.pdf; Comments of EPIC on Aircraft Registration Requirements for Unmanned Aircraft Systems (UAS) (Nov. 12, 2015), *available at* https://epic.org/privacy/drones/EPIC-FAA-Drone-Reg-Comments.pdf.
[6] *See* Federal Aviation Administration Modernization and Reform Act of 2012, Pub. L. 112-95 §§ 331-336 (2012), *available at* http://www.gpo.gov/fdsys/pkg/PLAWU112publ95/pdf/PLAWU112publ95.pdf.
[7] Letter to Michael P. Huerta, Acting Administrator of the FAA, from EPIC, *et al*. (Feb. 24, 2012), *available at* https://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.
[8] *EPIC v. FAA*, No. 15-1075 (D.C. Cir. Filed Mar. 31, 2015).

Aerial Drones: A Unique Privacy Threat

Drones pose a unique threat to privacy. The technical and economic limitations to aerial surveillance change dramatically with the advancement of drone technology. Small, unmanned drones are already inexpensive; the surveillance capabilities of drones are rapidly advancing; and cheap storage is readily available to maintain repositories of surveillance data. This combination of factors will make pervasive and indiscriminate aerial surveillance feasible.

EPIC recognizes that there may be beneficial uses 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 weather phenomena. However, when drones are used by police for surveillance, to intrude upon a reasonable expectation of privacy, or to gather personal data about individuals, rules are necessary to ensure that fundamental standards of 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.[9] On some drones, sensors can track up to 65 different targets across a distance of 65 square miles.[10] Drones may also carry infrared cameras, heat sensors, GPS, sensors that detect movement, and automated license plate readers.[11]

Drones with advance surveillance capabilities are readily available to the public. The DJI Inspire 1 is a high-end, commercially available hobbyist drone about the size of a small desktop printer and weighs less than seven pounds, yet it can transmit high definition video to an operator over a mile away.[12] The camera system on the Inspire 1 can shoot video up to 4K resolution at 24-30 frames per second and can capture 12 megapixel photos.[13] 4K is an ultra-high definition resolution that exceeds most HD televisions sold today. The high-resolution camera allows for detailed analysis of the area viewed that goes well beyond what is possible with the naked eye. Even lower-end

---

[9] 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.

[10] *Id*.

[11] 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.

[12] DJI, *Inspire 1*, http://www.dji.com/product/inspire-1/feature (last visited Mar. 14, 2016).

[13] *Id.*

hobbyist drones costing less than $200 can stream live video. The Hubsan X4, a drone that can fit in the palm of your hand, utilizes a front facing camera with 640 x 480 resolution that can stream live video up to 100 meters away and uses a memory card to capture video images.[14]

Although aerial surveillance is not new, drones drastically increase the possibility of aerial surveillance. Drones are cheaper to buy, maintain, and operate than helicopters, or other forms of aerial surveillance.[15] Drone manufacturers have 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]

Because of the unique threat posed by drones, many states have already begun to act in order to implement protections. Oregon has passed a law that provides a good example of how a state may act to properly limit the use of drones by law enforcement while still maintaining its value for police operations.[19]

---

[14] Hubsan, *FPV Hubsan X4*, http://www.hubsan.com/productinfo_11.html (last visited Mar. 14, 2016).

[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; Damon Lavrinc, *Forget the Helicopter: New Drones Cuts Costs of Aerial Video*, Wired (May 17, 2012), 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 around $300 for a drone with the capability to record and transmit HD 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://www.apple.com/shop/product/HE291ZM/A/parrot-ardrone-20-power-edition-quadricopter (last visited Mar. 14, 2016); Office of the Inspector Gen., Dep't Homeland Security, OIG-12-85, *CBPs Use of Unmanned Aircraft Systems in the Nation's Border Security*, 2 (May 2012), *available at* http://www.oig.dhs.gov/assets/Mgmt/2012/OIG_12-85_May12.pdf.

[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] *See* Or. Rev. Stat. Ann. § 837.310 et. seq. (West).

The Oregon law prohibits the use of a drone by law enforcement except for very specific circumstances. Those circumstances include when a warrant is obtained, in exigent circumstances, search and rescue, and reconstruction of a crime scene. The law makes clear that information gathered in violation of the act will not be admissible in court.

Other examples of good state laws include a Florida law, titled the Freedom from Unwarranted Surveillance Act, which prohibits law enforcement's use of drones except for certain circumstances including where a warrant is obtained or in emergency situations.[20] Like the Oregon law, evidence obtained in violation of the Florida law is inadmissible in court.[21] These laws ensure that the police can use new drone technology while providing privacy protections.

Florida's law also prohibits commercial or private individuals from recording people on private property when a reasonable expectation of privacy exists.[22] This is an important provision of the state law, but Florida's law, lack many of the current state laws on drones, do not go far enough to address the full scope of privacy risks posed by government and commercial use of drones, particularly as it relates to surveillance of individuals in public and providing appropriate transparency.

Recommendations

In order to adequately address the privacy risks associated with the domestic use of drones, EPIC recommends incorporating the following recommendations into any future drone legislation in Pennsylvania.

Government Use of Drones

- **Use Restrictions:** Law enforcement drone surveillance should be limited 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;

- **Prohibition on general surveillance:** The government, particularly law enforcement, should be prohibited from using drones to conduct general surveillance of the public;

- **Data Retention Limitations:** Restrictions should be implemented on retaining or sharing surveillance data collected by drones, with emphasis on protecting personally identifiable information;

[20] Fla. Stat. Ann. § 934.50 (West).
[21] *Id.*
[22] *Id.*

- **Transparency and Public Accountability**: Mechanisms like publicly available independent audits should be implemented to provide ongoing transparency and public accountability in the use of drones for surveillance. Transparency and accountability are particularly important for law enforcement's use of exceptions to prevent narrow exceptions from becoming broadly accepted practices; and

- **Published Policy and Procedures:** All state government agencies that use drones should make their policy and procedures with respect to the use of drones publicly available.

Commercial Use of Drones

- **Collection Restrictions:** Companies should be prohibited from collecting personally identifiable information via drone surveillance without informed consent. Additionally, companies should be prohibited from using biometrics to identify individuals whose information has been collected by drones;

- **Use and Data Retention Restrictions:** Data collected via drones should not be used for purposes beyond the original reason for collection or beyond the consented use. Similarly, data should not be retained longer than necessary to fulfill the original purpose of collection; and

- **Transparency Requirements:** Companies using drones should be required to make public the drones they have, their technical capabilities, the information collected by drones, how the information is used, who the information is shared with, and how long it is retained.

Conclusion

The increased use of drones to conduct various forms of surveillance must be accompanied by increased privacy protections. In the absence of strong federal protections, the states should act to safeguard privacy. EPIC supports legislation aimed at limiting drone surveillance and imposing liability on drone operators who fail to comply with the mandated standards of protection.

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