KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY & TECHNOLOGY

Statement of Harley Geiger
Senior Counsel and Advocacy Director
Center for Democracy & Technology

Hearing before the U.S. House of Representatives Committee on Oversight and Government Reform on "Drones: The Next Generation of Commerce?"

June 17, 2015

Chairman Chaffetz, Ranking Member Cummings, and members of the Committee:

Thank you for the opportunity to testify on behalf of the Center for Democracy & Technology (CDT). CDT is a nonpartisan, nonprofit technology policy advocacy organization dedicated to protecting civil liberties and human rights, including privacy, free speech and access to information. We applaud the Committee for holding a hearing that covers the challenges of regulating unmanned aircraft systems (UAS) – "drones" – in a manner that preserves both innovation and privacy.

CDT supports the many beneficial applications of UAS, but also acknowledges the potential for UAS to erode civil liberties. Federal and constitutional law do not provide individuals with clear and meaningful privacy protection from government UAS. Common law provides limited privacy protection from private UAS, though any direct privacy regulation of private UAS must be harmonized with the First Amendment. Public distrust, rooted in a perceived lack of privacy protection, hampers the domestic UAS industry and the growth of the technology. To reap the full benefits of UAS, Congress and the industry should take steps to address the public's legitimate privacy concerns. CDT recommends Congress pass federal legislation to enact privacy and transparency standards for UAS – especially law enforcement use. CDT also recommends that the UAS industry adopt a strong and accountable code of conduct.

I. UAS Privacy Issues

CDT readily recognizes that UAS is a valuable technology with many positive uses that pose little threat to privacy. We agree that unmanned aircraft can save lives, promote research, fight fires, make it easier to farm, track wildlife, relay WiFi signals to remote areas, deliver packages, reduce hardship for the many who work in hazardous conditions, and much more. CDT wants to see UAS utilized for science, commerce, disaster relief, journalism, education, and recreation. However, despite these clearly beneficial uses, we must not dismiss the strong potential for some unmanned aircraft applications to enable pervasive surveillance that degrades civil liberties.

Some have argued that UAS do not raise new privacy issues beyond those posed by manned aircraft, CCTV, or red light cameras. We disagree – because UAS operate from vantage points other systems do not reach, UAS can far exceed the privacy impact of those older technologies. Unlike helicopters, high grade UAS can quietly monitor a wide area for extended periods of time without refueling. CCTV and red light cameras are limited in their coverage: turn the corner, leave the intersection, or enter your fenced-in yard, and these systems can no longer observe you – but UAS can. It can be very difficult to avoid the gaze of high-flying UAS once an individual is outside. Because UAS are relatively inexpensive, they are likely to be used more frequently by more parties than most other aerial surveillance systems (like a helicopter). Combining UAS with cell tower emulators[1], facial recognition cameras[2], license plate scanners[3], thermal imaging cameras[4], open WiFi sniffers[5], and other sensors[6] can make the surveillance all the more intrusive.

Here is a nightmare scenario for civil liberties: A network of law enforcement UAS with sensors capable of identifying and tracking individuals monitors populated outdoor areas on a constant, pervasive basis for generalized public safety purposes. At the same time, commercial UAS platforms record footage of virtually anyone who steps out of her home, even if the individual remains on private property. This may seem an unlikely future to some. However, few existing laws would stand in the way, and the public does not yet trust the discretion of government or the UAS industry to prevent such scenarios from approaching reality.

In the past year, two incidents demonstrated the potential for large-scale federal law enforcement aerial surveillance. In 2014, it was revealed that Justice Department agencies used aircraft equipped with cell tower emulators to scan the identification numbers of the cell phones over which the aircraft flew.[7] The flying range of the aircraft reportedly covered most of the U.S. population, with each flight potentially scanning cell phone data from tens of thousands of individuals with no connection to crime. In 2015, it was revealed that the Federal Bureau of Investigation operated scores of aircraft for surveillance related to ongoing

---

[1] *See, e.g.,* Erica Fink, *This drone can steal what's on your phone*, CNN Money, Mar. 20, 2014, http://money.cnn.com/2014/03/20/technology/security/drone-phone/

[2] *See, e.g.,* Noah Shachtman, *Army Tracking Plan: Drones that Never Forget a Face*, Wired, Sept. 28, 2011, http://www.wired.com/dangerroom/2011/09/drones-never-forget-a-face.

[3] *See, e.g.,* Kris Gutierrez, *Drone Gives Texas Law Enforcement Bird's Eye View on Crime*, Fox News, Nov. 16, 2011,http://www.foxnews.com/us/2011/11/16/drone-gives-texas-law-enforcement-birds-eye-view-on-crime.

[4] *See, e.g.,* Draganflyer X6, Draganfly.com, http://www.draganfly.com/uav-helicopter/draganflyer-x6/features/flir-camera.php (last accessed Jun. 15, 2015).

[5] *See, e.g.,* Gary Mortimer, *Wi-Fi Aerial Surveillance Platform, WASP Drone*, sUAS News, Aug. 15, 2010, http://www.suasnews.com/2010/08/587/wi-fi-aerial-surveillance-platform-wasp.

[6] *See, e.g.,* Ryan Calo, *Drones, Dogs and the Future of Privacy* Wired, Mar. 8, 2012, http://www.wired.com/threatlevel/2012/03/opinion-calo-drones-dogs-privacy.

[7] Devlin Barrett, *Americans' Cellphones Targeted in Secret U.S. Spy Program*, Wall Street Journal, Nov. 13, 2014, http://www.wsj.com/articles/americans-cellphones-targeted-in-secret-u-s-spy-program-1415917533.

investigations, usually without court approval.[8] The government used manned flights in these examples, but UAS can make such surveillance more widespread, cheaper, and intrusive.

II. Privacy Laws and Law Enforcement UAS

At present, there are few clear nationwide restrictions on law enforcement use of UAS to monitor Americans outside their homes. There is no federal statutory protection. The FAA Modernization and Reform Act of 2012, which establishes a regulatory roadmap for integrating UAS into US airspace, does not mention privacy or transparency at all.[9] No other federal statute provides privacy protection or prescribes a due process standard for government use of UAS for physical surveillance.

CDT believes prolonged physical surveillance of individuals violates Fourth Amendment principles.[10] However, the federal courts have not provided consistent privacy protection from aerial surveillance. In a series of decisions in the late 1980s, the Supreme Court repeatedly found that individuals have no "reasonable expectation of privacy" – and therefore no Fourth Amendment protection – from warrantless government surveillance conducted from publicly navigable airspace.[11] The Supreme Court even held, in *Florida v. Riley* (1989), that the Fourth Amendment is not violated by warrantless police helicopter surveillance of the interior of a private building through a hole in the ceiling.[12]

Courts have slowly begun to express skepticism of the maxim that there is no reasonable expectation of privacy from warrantless government surveillance out of the home. In *United States v. Jones* (2012), the Supreme Court rejected the government's argument that there is never a reasonable expectation of privacy from warrantless government surveillance out of the home, but the *Jones* opinion is not a clear signal that the pubic has meaningful Fourth Amendment protection from aerial surveillance.[13] More recently, the Eastern District of Washington held, in *United States v. Vargas*, that the government violated the Fourth Amendment through secret surveillance of the front yard of a suspect's rural home continuously for more than six weeks from a pole camera.[14] An important, unanswered

---

[8] Jack Gillum, Eileen Sullivan, and Eric Tucker, *FBI behind mysterious surveillance aircraft over US cities*, Associated Press, Jun. 2, 2015, http://bigstory.ap.org/article/4b3f220e33b64123a3909c60845da045/fbi-behind-mysterious-surveillance-aircraft-over-us-cities.

[9] FAA Modernization and Reform Act of 2012, Pub. L. No. 112-05, 126 Stat. 11.

[10] *See*, Amicus Brief of CDT, EFF, et al in U.S. v Jones GPS Vehicle Tracking Case, Center for Democracy & Technology, Oct. 03, 2011, https://cdt.org/insight/amicus-brief-of-cdt-eff-et-al-in-u-s-v-jones-gps-vehicle-tracking-case.

[11] *California v. Ciraolo*, 476 U.S. 207, 222 (1986); *Dow Chem. Co. v. United States,* 476 U.S. 227, 239 (1986).

[12] *Florida v. Riley*, 488 U.S. 445 (1989).

[13] The Court ultimately ruled on grounds that attaching a tracking device to a car was a physical trespass. The Court also said: "Thus, even assuming that the concurrence is correct to say that "[t]raditional surveillance" of Jones for a 4-week period "would have required a large team of agents, multiple vehicles, and perhaps aerial assistance," post, at 12, our cases suggest that such visual observation is constitutionally permissible." *U.S. v. Jones*, 132 S.Ct. 945 (2012).

[14] The court declared that Americans have a reasonable expectation of privacy in the activities occurring in and around the front yard of their homes, and that this expectation prohibits "warrantless, continuous, and covert

question is whether any objective reasonable expectation of privacy on outdoor private property will, as a legal matter, survive in a future in which many UAS regularly traverse the skies.

The Dept. of Justice issued guidance on the domestic UAS that provides only limited privacy protection.[15] The Dept. of Justice guidance states that it will only collect and use information obtained from UAS for an authorized purpose, but this is a very light restraint. The guidance also asks agencies to submit annual privacy reviews, and states that the Dept. of Justice will provide the public with brief descriptions of the types and quantity of its UAS missions. While these steps are positive, they do not provide strong privacy or transparency. Similarly, the International Association of Chiefs of Police issued guidelines recommending that agencies secure a search warrant for UAS only if the UAS will intrude upon reasonable expectations of privacy.[16]

Public concern and the lack of clear federal privacy protection have prompted several states to take action. Approximately 16 states have enacted UAS privacy laws since 2014, and these laws vary widely.[17] Most of the state laws are focused on restricting warrantless law enforcement use, though other states – such as North Carolina and Louisiana – restrict private UAS.[18] Although state UAS privacy laws may reduce public concern within those states, a federal law is preferable to apply to both state and federal UAS, to provide coverage to states that do not have a state UAS law, and to provide greater regulatory certainty to public and private UAS operators.

III. Privacy Laws and Private UAS

Common law privacy torts provide Americans with some protection from private sector UAS out of the home. For example, the torts of intrusion upon seclusion and public disclosure of private facts prohibit intrusions and disclosures that would be highly offensive to a reasonable

---

recording." *United States v. Vargas*, No. CR-13-6025-EFS, slip. op. at 2 (E.D. Wash. Dec. 15, 2014), *available at* https://www.eff.org/files/2014/12/15/vargas_order.pdf. The government withdrew its appeal of the ruling.

[15] Department of Justice Policy Guidance, Domestic Use of Unmanned Aircraft Systems (UAS), Dept. of Justice, May 22, 2015, http://www.justice.gov/file/441266/download. The Dept. of Justice's guidance was in response to a Presidential Memorandum. See Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, The White House, Feb. 15, 2015, https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[16] International Association of Chiefs of Police, Aviation Committee, Recommended Guidelines for the use of Unmanned Aircraft, Aug. 2012, pg. 3, http://www.theiacp.org/portals/0/pdfs/IACP_UAGuidelines.pdf.

[17] Current Unmanned Aircraft State Law Landscape, National Conference of State Legislatures, Jun. 9, 2015, http://www.ncsl.org/research/transportation/current-unmanned-aircraft-state-law-landscape.aspx. See also 2014 State Unmanned Aircraft Systems Legislation, National Conference of State Legislatures, Sep. 16, 2014, http://www.ncsl.org/research/civil-and-criminal-justice/2014-state-unmanned-aircraft-systems-uas-legislation.aspx.

[18] North Carolina General Statutes, Article 16B, Chapter 15A-300.1. Louisiana Revised Statutes, Title 14, Section 337.

person.[19] Many, though not all, states have voyeurism and peeping tom laws that provide additional protections. However, many voyeurism and peeping tom laws apply only to looking within structures or enclosures, require plaintiffs to have a reasonable expectation of privacy, and may include sexual gratification as a component of the perpetrator's intent.[20] Moreover, as camera-equipped UAS proliferate, it may become increasingly difficult to claim that observation from UAS is objectively offensive, or that an individual has a reasonable expectation of privacy, even when the observed individual is on private property. Still, these and other civil laws[21] provide Americans with limited protection from some egregious conduct that UAS can enable.

More sweeping government regulation of private UAS must avoid infringing on Americans' longstanding First Amendment right to take photographs of things visible from public places.[22] Some state UAS-specific laws may run afoul of First Amendment protection for private photography. For example, North Carolina broadly forbids any person from using UAS to capture an image of an individual or private property for the purpose of disseminating or publishing the image, unless the image is newsworthy.[23] Texas law forbids capturing an image of an individual or private property "with intent to conduct surveillance."[24] We believe such laws infringe on free expression due to their overbreadth and are skeptical that they would withstand a First Amendment challenge.

CDT supports comprehensive baseline consumer privacy legislation that is tech-neutral, and therefore includes physical surveillance platforms such as UAS. However, the application of any such legislation to UAS would be somewhat limited in scope to avoid a First Amendment conflict. While UAS must abide by applicable safety laws, and some UAS platforms could be required to disclose data collection practices, it would likely be generally impermissible to authorize some types of UAS-based recording while restraining others on privacy grounds.[25]

---

[19] "One who intentionally intrudes, physically or otherwise, upon the solitude or seclusion of another or his private affairs or concerns, is subject to liability to the other for invasion of his privacy, if the intrusion would be highly offensive to a reasonable person." Restatement (Second) of Torts Sec. 652B (1977). "One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that (a) would be highly offensive to a reasonable person, and (b) is not of legitimate concern to the public." Restatement (Second) of Torts Sec. 652D (1977).

[20] See, Voyeurism Statutes 2009, National District Attorneys Association, Mar. 2009, http://www.ndaa.org/pdf/voyeurism_statutes_mar_09.pdf.

[21] Nuisance and trespass also provide limited privacy protection. However, claims must typically demonstrate a substantial interference with enjoyment of land, and trespass claims likely do not apply to UAS in publicly navigable airspace. Restatement of Torts (Second), Sec. 159(2) (1965), stating that "Flights by aircraft in the airspace above the land of another is a trespass if, but only if, (a) it enters into the immediate reaches of the airspace next to the land, and (b) it interferes substantially with the other's use and enjoyment of the land."

[22] See Know Your Rights: Photographers, American Civil Liberties Union, Jul. 2014, https://www.aclu.org/know-your-rights-photographers.

[23] North Carolina General Statutes, 15A-300.1.

[24] Texas Gov't Code, Sec. 423.003.

[25] See Stephen E. Henderson et al., (2015) "Regulating Drones under the First and Fourth Amendments" *William and Mary Law Review (forthcoming)*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=2574378.

CDT believes a strong and accountable industry code of conduct would be a helpful step towards achieving effective privacy protection from private UAS without infringing on free expression. Unfortunately, the industry code of conduct developed by the Association of Unmanned Vehicle Systems International (AUVSI) does not provide meaningful protection.[26] AUVSI's industry code merely commits to following the law and respecting the privacy of individuals, without further detail. CDT believes more robust and nuanced industry best practices on privacy and transparency are necessary to build public trust in UAS.[27]

IV. Public Trust of UAS

The perceived lack of privacy protection in law has fed widespread public distrust of UAS. A 2014 Pew poll found that nearly two-thirds of surveyed Americans thought the proliferation of personal and commercial UAS would be negative, despite being generally positive about the future benefits of technological advancement.[28] A 2013 poll from Monmouth University found that three-fourths of surveyed Americans say the government should get a warrant to use UAS.[29] Other polls of residents in specific states show even greater discomfort with UAS surveillance and higher levels of support for a warrant requirement.[30] The lack of trust has prompted the patchwork of state laws and hampered public acceptance of UAS.

This negative sentiment can also manifest in more extreme ways – such as shooting down or disabling UAS in mid-flight. Just two weeks prior to this hearing, on June 4th, firefighters in upstate New York repeatedly tried to spray a UAS with their hoses while it filmed them during the aftermath of a house fire.[31] A New Jersey man shot down a UAS last fall.[32] A 2013

---

[26] Unmanned Aircraft System Operations Industry "Code of Conduct," Association for Unmanned Vehicle Systems International, Jul. 2012, pg. 2, http://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedFiles/AUVSI%20UAS%20Operations%20Code%20of%20Conduct%20-%20Final.pdf.

[27] See, e.g., Center for Democracy, CDT Comments To NTIA On "Privacy, Transparency, And Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems," Apr. 20, 2015, https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/04/CDT-Submission-to-NTIA-on-Commercial-and-Private-Use-of-UAS.pdf.

[28] U.S. Views of Technology and the Future, Pew Research Center, Apr. 17, 2014, pg. 3, http://www.pewinternet.org/files/2014/04/US-Views-of-Technology-and-the-Future.pdf.

[29] U.S. Supports Unarmed Domestic Drones, But Public Prefers Requiring Court Orders First, Monmouth University, Aug. 15, 2013, pg. 2, https://www.monmouth.edu/assets/0/32212254770/32212254991/32212254992/32212254994/32212254995/30064771087/409aecfb-3897-4360-8a05-03838ba69e46.pdf.

[30] See, e.g., William Petroski, Iowa Poll: 76% favor requiring warrants for drone surveillance, Des Moines Register, Mar. 11, 2014, http://www.desmoinesregister.com/story/news/politics/2014/03/11/iowa-poll-76-favor-requiring-warrants-for-drone-surveillance/6311137. See also, Sakiyama, et al., Nevada vs. U.S. Residents' Attitudes Toward Surveillance Using Aerial Drones, University of Nevada Las Vegas Center for Crime and Justice Policy, Dec. 2014, http://www.unlv.edu/sites/default/files/page_files/27/NevadaU.S.Residents%27Attitudes.pdf. See also, Poll: 72% of North Carolina Voters Support Warrant Requirement for Drone Surveillance, ACLU of North Carolina, Mar. 2014, http://acluofnc.org/blog/poll-72-of-north-carolina-voters-support-warrant-requirement-for-drone-surveillance.html.

[31] Michael Franco, *Watch firefighters blast drone out of sky with hose*, CNet, Jun. 11, 2015, http://www.cnet.com/au/news/watch-firefighters-blast-drone-out-of-sky-with-hose.

Reason-Rupe poll found that nearly half of surveyed Americans believe they should have the right to shoot down UAS over their property.[33] A bill that would have provided civil immunity to individuals that shoot down UAS over their property passed the Oklahoma Senate Judiciary Committee earlier this spring.[34]

To foster broader public acceptance of UAS, the government and the industry itself should fully address civil liberties issues. We understand that most unmanned aircraft will not be equipped with sophisticated sensors and tracking systems, and it's clear that most businesses want to be good actors. However, the public wants protections from the most troubling capabilities and uses of this technology that we've seen in both theaters of war and domestically. Congress, Executive Branch agencies, and the private sector have important roles to play in providing protections and preserving public trust.

V. Federal UAS Legislation Recommendations

CDT believes Congress should consider legislation regarding UAS to provide privacy where protections are currently weak, to provide regulatory clarity to both businesses and government agencies, and to promote public trust of UAS technology.

The key issue this legislation should address is establishing due process standards for law enforcement use of UAS. While the public has broader concerns with UAS, law enforcement use may be the most acute. The legislation should have a lighter touch for non-law enforcement uses of government ("public") UAS, such as scientific research and other uses with a low impact on civil liberties, but legislation should establish transparency requirements for all public UAS. Any provision regulating private use of UAS should be flexible enough to avoid infringing on free expression and violating the First Amendment.

More specifically, CDT recommends that Congress enact federal legislation that

- Requires public UAS to submit a data collection statement as part of the Federal Aviation Administration's (FAA) UAS certification process. The data collection statement should outline the agency's data collection, retention, and use policies, and provide an individual point of contact.
- Requires the FAA to establish a publicly accessible database indexing public UAS licenses and data collection statements. This could be similar to the FAA's database for private aircraft.[35]

---

[32] Jeff Goldman, *Man arrested after shooting down neighbor's remote control helicopter, cops say*, NJ.com, Sep. 30, 2014, http://www.nj.com/cape-may-county/index.ssf/2014/09/man_faced_with_gun_charges_after_shooting_down_remote_control_helicopter.html.

[33] Reason-Rupe Public Opinion Survey, February 2013 Topline results, Feb. 25, 2013, Pg. 5. http://reason.com/assets/db/13620384648046.pdf.

[34] S.B. 492, 55th Leg., 1st Sess. (Okla. 2015), *available at*, http://www.oklegislature.gov/BillInfo.aspx?Bill=SB492&Session=1500. The bill would not affect liability for discharging a firearm, nor liability for violating FAA rules.

[35] FAA Registry, Aircraft Inquiry, Federal Aviation Administration, http://registry.faa.gov/aircraftinquiry (last accessed Jun. 12, 2015).

- Requires law enforcement agencies to obtain a warrant for UAS surveillance of individuals or private property. Exceptions to this requirement should include exigent circumstances such as destruction of evidence, hot pursuit of a fleeing suspect, and emergency situations involving imminent danger of death or serious injury.
- Bans lethal weapons – "firearms" as defined by 18 USC 921 – from public, private, and hobbyist UAS. Exceptions could include military testing, training, taking off and landing in the US.

Many of these recommendations are articulated in legislation in both the House and Senate. CDT supports the Preserving American Privacy Act of 2015, sponsored by Reps. Poe and Lofgren, as well as Senator Wyden's forthcoming "Protecting Individuals From Mass Aerial Surveillance Act of 2015."[36] We believe both bills would establish meaningful protections from overbroad government UAS surveillance while preserving beneficial uses with less impact on civil liberties, such as government research and disaster relief. Senator Wyden's bill has the added benefit of applying to manned, as well as unmanned, aerial surveillance. The Preserving American Privacy Act does include a light restriction on private UAS, but we believe this restriction – which forbids intentionally using UAS, in a manner that would be highly offensive to a reasonable person, to observe an individual engaging in personal activity in circumstances where the individual has a reasonable expectation of privacy – is generally aligned with privacy torts and does not, on its face, violate the First Amendment. CDT urges Congress to swiftly advance these bills.

VI. Private UAS Recommendations

CDT supports comprehensive baseline consumer privacy legislation that includes UAS, but recognizes that First Amendment principles would constrict privacy regulation of UAS-enabled observation. If broadly adopted and faithfully implemented, an industry code of conduct with meaningful privacy, transparency, and accountability requirements could provide protection and foster public trust. CDT supports the National Telecommunications and Information Administration's (NTIA) effort to develop voluntary guidelines for UAS, as required by Presidential memorandum on domestic UAS.[37] Because such guidelines would be voluntary, they should not raise the same First Amendment issues associated with formal regulation of data collection by private UAS.

CDT recommends that the UAS industry work to develop a code of conduct for private UAS that

- Establishes reasonable limits on UAS collection and analysis of sensitive or personally identifying information.

[36] "Preserving American Privacy Act," H.R. 1385, 114th Cong. (2015). "Protecting Individuals From Mass Aerial Surveillance Act of 2015," 114th Cong. (2015), draft bill on file with author.

[37] Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, The White House, Feb. 15, 2015, https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

- Establishes reasonable limits on the retention of sensitive or personally identifying data collected by UAS.
- Creates a publicly accessible UAS registry that includes a data collection statement detailing the UAS owner's collection, retention, and use practices and providing an individual point of contact.
- Provides for reasonable exceptions to a UAS registry, such as registration by proxy or a full exemption, to protect UAS owners' privacy interests in their identifying information, such as investigative journalists.
- Provides for a means of reporting nuisances and other complaints related to UAS.
- Establishes cybersecurity standards to prevent hijacking or unauthorized damage to UAS systems.[38]

In addition, CDT recommends that the industry explore technical measures to protect individual privacy in physical space. One example is the private sector effort to enable individuals to "geo-fence" their property so that UAS avoids flying over, or avoids retaining data collected over, the delineated area.[39] An example of a technical transparency measure would be to equip UAS with transponders that broadcast a signal identifying the UAS – acting as UAS "license plates" that are easier for individuals to read at a distance than tail markings.[40]

Another technical measure CDT recommends the industry explore is are protocols to allow individuals to communicate privacy preferences to UAS and other devices collecting data in physical space. For example, UAS equipped with a camera could halt visual observation of individuals who display a particular graphic symbol or color, or who broadcast a "do not track" signal from handheld devices.[41] While such privacy protective measures are available to Internet users in the online context, few comparable measures are available yet to protect privacy in physical space.[42]

Conclusion

Unmanned aircraft have great potential benefit, but also potential for invasion of privacy. For this reason, the public does not trust UAS. Without public trust, the UAS industry will struggle with acceptance, public hostility, and a regulatory patchwork. Current laws do not adequately

[38] Center for Democracy, CDT Comments To NTIA On "Privacy, Transparency, And Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems," Apr. 20, 2015, https://cdt.org/files/2015/04/CDT-Submission-to-NTIA-on-Commercial-and-Private-Use-of-UAS.pdf.
[39] See, e.g., NoFlyZone, About, https://www.noflyzone.org/about (last accessed Jun. 12, 2015).
[40] Joseph Hall, 'License Plates' for Drones?, Center for Democracy & Technology, Mar. 2013, https://cdt.org/blog/license-plates-for-drones.
[41] See, e.g., Jeremy Schiff et al. (2009). Respectful Cameras: Detecting Visual Markers in Real-Time to Address Privacy Concerns. In *Protecting Privacy in Video Surveillance*, Springer, http://goldberg.berkeley.edu/pubs/respectful-cameras-book-chapter-F08.pdf (last accessed Jun. 12, 2015).
[42] A system of this kind would have applications beyond UAS, such as facial recognition and other biometric sensors. See, e.g., Harley Geiger, Seeing Is ID'ing: Facial Recognition & Privacy, Comments to the Federal Trade Commission, Center for Democracy & Technology, pg. 17, https://www.cdt.org/files/pdfs/Facial_Recognition_and_Privacy-Center_for_Democracy_and_Technology-January_2012.pdf.

protect privacy from broad surveillance by unmanned aircraft systems. A combination of federal legislation for government UAS and best practices for private UAS would be good initial steps. The goal should be to meaningfully protect privacy and enhance transparency while preserving essential law enforcement use and maintaining a light regulatory touch on emergency, scientific, and other uses with low impact on civil liberties. We look forward to working with both the government and the UAS industry to preserve privacy, free expression, security, and innovation.

END

Committee on Oversight and Government Reform
Witness Disclosure Requirement – "Truth in Testimony"
Required by House Rule XI, Clause 2(g)(5)

Name: HARLEY GEIGER

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

NONE.

2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

CENTER FOR DEMOCRACY AND TECHNOLOGY.
I AM SENIOR COUNSEL AND ADVOCACY DIRECTOR.

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

NONE.

I certify that the above information is true and correct.
Signature: Harley Geiger Date: 06/15/15

Harley Geiger
Advocacy Director & Senior Counsel

Harley Geiger is Advocacy Director and Senior Counsel at the Center for Democracy & Technology (CDT). He works on issues related to civil liberties and government surveillance, computer crime, and cybersecurity.

From 2012-2014, Harley served as Senior Legislative Counsel for U.S. Representative Zoe Lofgren of California. There he was the lead staffer for technology and Internet issues, and was instrumental in helping develop Rep. Lofgren's Internet freedom agenda, including legislation to reform the Foreign Intelligence Surveillance Act, ECPA, the Computer Fraud and Abuse Act, and copyright laws.

Harley worked at CDT from 2008-2012 as Staff Attorney and Senior Policy Counsel, focusing on surveillance, consumer privacy, health information technology, and data security. Prior to working at CDT, Harley clerked with the Bureau of Consumer Protection at the Federal Trade Commission, where he worked on information security public awareness campaigns. In 2007, Harley clerked with the Electronic Privacy Information Center where he worked on health privacy, telephone network security, employee verification, and human rights issues. In 2006, he clerked with the Minority Leader of the Missouri House of Representatives, where he testified before a Missouri Senate Committee on technology policy.

Harley earned a BA in Journalism, an MA in Journalism, and a JD from the University of Missouri – Columbia. Harley is CIPP/US certified and *Politico* named him one of the Emerging Tech Leaders of 2013.