KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE
www.cdt.org
CENTER FOR DEMOCRACY & TECHNOLOGY

Statement of Chris Calabrese
Vice President for Policy
Center for Democracy & Technology

Hearing on "Unmanned Aerial Vehicles: Commercial Applications and Public Policy Implications" before the U.S. House of Representatives Committee on the Judiciary's Subcommittee on Courts, Intellectual Property, and the Internet.

September 10, 2015

Chairman Issa, Ranking Member Nadler, and members of the Subcommittee:

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 Subcommittee 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 consistent 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 develops and adopts 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 more. CDT wants to see UAS utilized for science, commerce, disaster relief, journalism, education, and recreation. However, despite these clearly beneficial uses, we should not ignore 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, facial recognition cameras[1], license plate scanners[2], thermal imaging cameras[3], open WiFi sniffers[4], and other[5] sensors can make the surveillance all the more intrusive.

As UAS proliferate, many Americans are now facing the significant likelihood of aerial surveillance in public and private property where currently little or no physical surveillance takes place. For example, most public areas in the US are not under constant law enforcement surveillance, but UAS could underpin a network of sensors capable of identifying and tracking individuals and vehicles on a pervasive basis for generalized public safety purposes. Another example: Most Americans do not expect to be recorded while on fenced-in private property, but commercial UAS platforms could take footage of virtually anyone who steps out of her home, even if the individual remains on private property. These may seem like unlikely examples to some. However, few existing laws would stand in the way, and the public does not trust the discretion of government or the UAS industry to prevent such disagreeable 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.[6] The flying range of the aircraft reportedly covered most of

---

[1] *See* 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.

[2] *See* 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.

[3] *See, e.g.,* Draganflyer X6, Draganfly.com, http://www.draganfly.com/uav-helicopter/draganflyer-x6/features/flir-camera.php.

[4] *See* 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.

[5] 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.

[6] 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. The Dept. of Justice has since announced that the Department will obtain a warrant before using cell tower emulators. *Justice Department Anounces Enhanced Policy for Use of Cell-Site Simulators*, Dept. of Justice Office of Public Affairs, Sep. 3, 2015, http://www.justice.gov/opa/pr/justice-department-announces-enhanced-policy-use-cell-site-simulators.

the U.S. population, with each flight 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 planes for surveillance related to ongoing investigations, usually without court approval.[7] 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.[8] 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. 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.[9] The Supreme Court even held, in *Florida v. Riley* (1989), that the Fourth Amendment is not violated by warrantless police helicopter surveillance from 400ft of the interior of a private building through a hole in the ceiling.[10]

Courts have slowly begun to express skepticism for 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 Court ultimately ruled on grounds that attaching a tracking device to a car was a physical trespass.[11] The *Jones* opinion is not a clear signal that the pubic has meaningful privacy protection from aerial surveillance.[12] More recently, the Eastern District of Washington held, in *United States v. Vargas*, that the government violated the Fourth Amendment through secret video surveillance of the front yard of a suspect's rural home continuously for more than

---

[7] 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.

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

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

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

[11] *U.S. v. Jones*, 132 S.Ct. 945 (2012).

[12] "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).

six weeks.[13] An important, unanswered question is whether any objective reasonable expectation of privacy on outdoor private property will 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.[14] 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 transparency or privacy protections. 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.[15]

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 person.[16] 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.[17] 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,

[13] 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 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.

[14] 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. .

[15] 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.

[16] "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).

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

even when the observed individual is on private property. These and other[18] civil laws 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.[19] Some state UAS-specific laws may run afoul of First Amendment protection for photography by private individuals. For example, North Carolina broadly forbids any person from using UAS to capture an image of any individual, or of private property for the purpose of disseminating or publishing the image, unless the image is newsworthy.[20] Texas law forbids capturing an image of an individual or private property "with intent to conduct surveillance."[21] 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 private UAS would necessarily 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 private UAS-based photography and sound recording while restraining others on privacy grounds.[22]

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.[23] 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. Pursuant to President Obama's Feb. 2015 Memorandum on domestic use of unmanned aircraft, the National Telecommunications and Information Administration (NTIA) recently held its first of a series of multi-stakeholder meetings with industry, academics, public interest groups and

---

[18] 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."

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

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

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

[22] 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.

[23] 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.

others to develop privacy best practices for private UAS.[24] Though it is early in the process, CDT is optimistic that the goal of meaningful and effective best practices is achievable – particularly since private UAS operators have significant incentives to seek public acceptance of the technology.

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.[25] A 2013 poll from Monmouth University found that three-fourths of surveyed Americans say the government should get a warrant to use UAS.[26] Other polls of residents in specific states show even greater discomfort with UAS surveillance and higher levels of support for a warrant requirement.[27] This lack of trust has prompted the patchwork of state laws and hampered public acceptance of UAS.

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.[28] Most of the state laws are focused on law enforcement use, though other states – such as North Carolina and Louisiana – restrict private UAS.[29] Although state UAS

[24] 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. See also, 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.

[25] 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.

[26] 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.

[27] 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.

[28] 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.

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

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.

This negative sentiment can also manifest in more extreme ways – such as shooting down or disabling UAS in mid-flight. Earlier this summer, 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.[30] A New Jersey man shot down a UAS last fall.[31] A 2013 Reason-Rupe poll found that nearly half of surveyed Americans believe they should have the right to shoot down UAS over their property.[32] 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.[33] Such examples demonstrate the degree to which many Americans feel UAS intrude on their peace and privacy.

To foster broader public acceptance of the UAS industry, 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 public UAS, such as scientific research and other uses with a low impact on civil liberties, but legislation should establish transparency requirements for all government

---

[30] 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.

[31] 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.

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

[33] 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.

("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.[34]
- Requires law enforcement agencies to have a warrant for UAS surveillance of individuals or private property.[35] 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. Crime scene photography should be permitted as well. The main goal is to prevent warrantless use of UAS over private property, and warrantless use of UAS for long-term monitoring of public spaces.
- Bans lethal weapons – "firearms" as defined by 18 USC 921 – from public, private, and hobbyist UAS. Exceptions could include testing, training, and military UAS taking off and landing in the US.
- Does not regulate private UAS in a way that violates the First Amendment right to photography in public places. This can be done by mirroring language in existing privacy torts – such as intrusion upon seclusion – banning private UAS use that is "highly offensive to a reasonable person" in circumstances where the person has a "reasonable expectation of privacy." This would be a weak restriction, which is why a code of conduct is important.

Many of these recommendations are articulated in active 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 "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. 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

[34] FAA Registry, Aircraft Inquiry, Federal Aviation Administration, http://registry.faa.gov/aircraftinquiry (last accessed Jun. 12, 2015).
[35] If law enforcement already has a warrant to search property, a separate warrant to use UAS is unnecessary.
[36] "Preserving American Privacy Act," H.R. 1385, 114th Cong. (2015). "Protecting Individuals From Mass Aerial Surveillance Act of 2015," S. 1595, 114th Cong. (2015).

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 NTIA's effort to develop voluntary best practices 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

- Is based on the Fair Information Practice Principles.[38]
- Establishes reasonable limits on UAS collection, use, and analysis of sensitive or personally identifying information.
- Establishes reasonable limits on the retention and sharing 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 and retention 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.
- Requires operators to make reasonable efforts to communicate these privacy and transparency policies to external audiences, such as through a privacy policy on a website.
- Provides for a means of reporting nuisances and other complaints related to UAS.
- Requires that UAS operators secure sensitive data collected via UAS.
- Establishes cybersecurity standards to prevent hijacking or unauthorized damage to UAS systems.[39]

---

[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.

[38] Department of Homeland Security, The Fair Information Practice Principles: Framework for Privacy Policy at the Department of Homeland Security (Dec. 2008), http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf.

[39] Center for Democracy, CDT Comments To NTIA On "Privacy, Transparency, And Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems," Apr. 20, 2015,

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.[40] 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.[41]

Another technical measure CDT recommends the industry explore is a protocol to allow individuals to communicate privacy preferences to UAS and other devices collecting data in physical space. For example, a 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.[42] 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.[43]

Conclusion

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

---

https://d1ovv0c9tw0h0c.cloudfront.net/files/2015/04/CDT-Submission-to-NTIA-on-Commercial-and-Private-Use-of-UAS.pdf.

[40] See, e.g., NoFlyZone, About, https://www.noflyzone.org/about (last accessed Jun. 12, 2015).

[41] Joseph Hall, 'License Plates' for Drones?, Center for Democracy & Technology, Mar. 2013, https://cdt.org/blog/license-plates-for-drones.

[42] 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).

[43] 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.