CDT COMMENTS TO NTIA ON "PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY REGARDING COMMERCIAL AND PRIVATE USE OF UNMANNED AIRCRAFT SYSTEMS"

April 20, 2015

The Center for Democracy & Technology (CDT) is pleased to submit comments to the National Telecommunications and Information Administration (NTIA) request for public comment on "Privacy, Transparency and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems."

Protecting individuals' privacy and encouraging UAS operators' transparency and accountability requires practical solutions that are grounded in the Fair Information Practice Principles (FIPPs) and that respect free expression values. These solutions must also reflect the technologically unique nature of UAS. UAS are far more than flying cameras: many are enabled with movement, light or temperature sensors, some are Internet-connected, and others carry and deliver supplies. The capabilities of UAS are broad and continue to grow. Designing best practices in this rapidly evolving industry must take into account the increasing capabilities of these devices and the breadth of data that can be collected through these capabilities.

With this in mind, CDT recommends that the NTIA multistakeholder process develops best practices for commercial and private use of UAS centered around four FIPPs: notice, choice, data minimization, and use restrictions. Specifically, we propose that the multistakeholder process consider the following as best practices for adoption: (1) limits on UAS collection and analysis of data; (2) limits on UAS retention of data; (3) standardized methods to disclose data collection practices by non-hobbyist, UAS operators, and technical capacity to identify those operators; and (4) methods to honor requests to opt-out certain areas entirely or partially from UAS data collection.

It is also important to note at the outset that while we applaud the NTIA for focusing on UAS privacy, self-regulation cannot be the sole method for protecting individual privacy. We have long called for the creation of an overarching data protection law to regulate commercial data. Such a law, as long as it is narrowly tailored and appropriately addresses the First Amendment concerns raised by the regulation of publicly accessible information, would also be critical in protecting privacy in this context. Finally self-regulation cannot regulate use of UAS technology by law enforcement, an area CDT believes requires Congressional action.[1]

I. Reasonable limits should be placed on UAS collection of data – particularly UAS surveillance and use of identification technologies

[1] Harley Geiger, The Drones are Coming, CENTER FOR DEMOCRACY & TECHNOLOGY BLOG (Dec. 21, 2011), https://cdt.org/blog/the-drones-are-coming/.

The UAS best practices should include placing reasonable limits on UAS collection of data – particularly as it relates to surveillance and use of identification technologies. This is in line with the Privacy principle outlined in the Request for Comment.

A. Limits on surveillance conducted by UAS

Surveillance equipment installed on UAS is a commonly identified privacy risk.[2] UAS are capable of going places manned aircraft cannot (such as between narrow buildings) and operating in environments that humans cannot (such as during high-g tactical maneuvers, high altitudes, and long times aloft). UAS, like manned aircraft, have unique vantage points allowing for levels of surveillance that ground-based individuals may not expect. Moreover, UAS are becoming more affordable — a simple "drones for sale" Google search produces advertisements for first-person view ("FPV") UAS priced as low as 100 dollars.

UAS surveillance may be appropriate in many contexts but these technologies should not lead to limitless snooping into individuals' private lives. Self-regulation of UAS should set boundaries for surveillance equipment use: It should not, for example, be acceptable for UAS to peer into the windows of people's homes. There should likely be standards advising against UAS surveillance of areas immediately outside of the home or outdoor spaces on private lands protected from observation by a passerby. While it would not be practical to limit UAS surveillance from public airspace of all private property, some private lands may be sufficiently unobservable by ordinary means that UAS surveillance would be contrary to reasonable expectations of privacy. For example, a person may not expect a UAS to surveil under an outdoor canopy or gazebo.

CDT recommends that the NTIA use the multistakeholder process to develop guidance delineating the areas where individuals would reasonably expect to be shielded from public surveillance — certainly within their home, but potentially for other privately held property where a data subject would have a reasonable expectation of privacy. This guidance should be informed by existing state and local laws including Peeping Tom laws, privacy tort and state laws on UAS use. We also encourage the NTIA multistakeholder process to explore and solicit ongoing public input on what reasonable guidelines might be to determine where such an expectation exists.

B. Limits on use of identification technologies

CDT believes UAS operators should place limits on the types of UAS-collected images

---

[2] The use of thermal imaging on drones could possibly sidestep Kyllo v. United States. *See* David Alan Coia, US Domestic Drones Use Sidesteps Warrants for Thermal Imaging, NEWSMAX BLOG (Aug. 11, 2013, 7:51 AM), http://www.newsmax.com/US/drones-warrants-thermal-imaging/2013/08/11/id/519767/. Also, recall the Google Street View wireless sniffing incident. *See* David Kravets, An Intentional Mistake: The Anatomy of Google's Wi-Fi Sniffing Debacle (May 2, 2012, 7:18 PM), WIRED BLOG, http://www.wired.com/2012/05/google-wifi-fcc-investigation/. Drones could similarly collect data on the wire, or even *just* engage in "wardriving" to log which wireless devices are broadcasting at given addresses. They would not need to enter the property to pick up these signals. *See Wardriving,* WIKIPEDIA.ORG, https://en.wikipedia.org/wiki/Wardriving (last visited Apr. 20, 2015).

that are subject to facial recognition technologies or other automated identification. Commercial use of UAS will potentially produce numerous images of people who may not be recognizable without the assistance of identification technologies. Biometric scanning, automated license plate scanners, and other tools designed to identify a person based on unique identifiers or their unique physical or behavioral characteristics, could allow for identification of much of the public captured by a commercial UAS.

We do not believe that universal recognition of everyone in public spaces is necessary, reasonable, or proportional. It might be permissible to ephemerally scan attributes such as faces or license plates for *specific known images*, such as a missing child, a stolen car, or a wanted fugitive, although this is more applicable in the context of law enforcement use of UAS. (However, the biometric identifiers associated with non-suspected individuals should not be logged or maintained.) These potential exceptions to a general limitation on the use of identification technologies would be a useful topic for multistakeholder discussion.

We believe this rule could benefit both the public and industry. By limiting identification, many of the privacy harms from UAS use could be mitigated allowing for broader public acceptance. This is especially true since many uses of UAS – from agriculture to package delivery – require the collection of little or no personal information.

II. Limits should be placed on retention of UAS-collected data

In addition to limiting UAS surveillance and use of identification technology, operators should be cognizant of limiting how long data collected through UAS is retained. This is in line with the Privacy principle outlined in the Request for Comment, as well as the Federal Trade Commission's recommendations in its January 2015 "Internet of Things" report.[3] The report noted that data retention limits are key for two reasons: one, data thieves are more attracted to large data sets, increasing the chances of theft; and secondly, there is an increased risk that data retained for longer than necessary will be involved in a data breach and/or used in ways that do not meet consumers' reasonable expectations.

Data minimization is one of the most important FIPPs and deserves particular attention from UAS operators. Given UAS' ability to collect data on an individual without his or her knowledge or consent, placing limits on how long this data is kept will reinforce individuals' fundamental privacy rights and reduce the likelihood of data breaches that may result from lengthy retention. UAS operators should not hold on to all data points in identifiable form on the off-hand chance that they could prove interesting one day in the future. Purposeful, strategic data collection and retention is not only good for consumers' privacy – it is good for business[4]. UAS operators that implement thoughtful processes on the front-end for determining what data to collect and how long to keep it are arguably

[3] Alex Bradshaw, FTC Says Privacy Still Matters on "Internet of Things", CENTER FOR DEMOCRACY & TECHNOLOGY BLOG (Jan. 20, 2015), https://cdt.org/blog/ftc-says-privacy-still-matters-on-internet-of-things/.
[4] David Hoffman, Privacy is a Business Opportunity, HARVARD BUSINESS REVIEW (Apr. 18, 2014), https://hbr.org/2014/04/privacy-is-a-business-opportunity/.

less susceptible to data breaches and the reputational damage and loss of consumer trust that accompany a breach.

CDT recommends UAS operators distinguish between "identifiable" information that personally identifies someone (such as a name, picture, or biometric reading) and "unidentifiable" or anonymous data points when determining data retention limits. Identifiable information should only be retained for specified purposes and should be permanently deleted within a given period of time – CDT has previously argued for deletion or de-identification of these data types within ninety days of collection absent a compelling reason to retain longer or for journalist purposes.[5] Unidentifiable information or data that has been "de-identified" to remove all identifying features, may be retained for longer periods as long as it is used for limited purposes. De-identification processes may include (but are not limited to) removing names, birth dates and phone numbers, or blurring personal aspects of a data subject. We note, however, that de-identification alone will not provide robust data protection. Given reports of the risks of re-identification[6] it is increasingly clear that de-identifying data should not relieve UAS operators of the responsibility to implement additional safeguards. These safeguards should include, among others, minimizing collection and retention of data.

III. Standardized identifying information on non-hobbyist UAS owners and operators should be publicly available

CDT supports the development of a license plate-type identification system for non-hobbyist (commercial) UAS operators and an accompanying UAS registry. This supports the Transparency and Accountability principles outlined in the Request for Comment. Ideally, all commercial UAS operators would mark their UAS with a consistent identifier that is used to track and report the UAS' movements. However, traditional license plate identifiers likely will not be detectable from the ground given UAS' small size and ability to fly at high altitudes. A more practical solution would be to require that all commercial UAS are configured to emit a standardized signal identifying the UAS. These "identification signals" would be detectable using basic frequency radio receivers.

In addition to identification signals, operators could contribute to a UAS registry where interested parties may access metadata on the UAS transmitted through its identification signal – including names of the owner and operator(s) – as well as a link to other information on the UAS, such as the owner's privacy policy. This registry should be public-facing and searchable.

The registry should host detailed statements from the UAS' owner outlining the UAS' purpose, planned operations and capabilities. CDT's previous submissions to regulatory authorities propose requiring commercial UAS operators in the US to submit a licensing statement, or Data Collection Statement ("DCS"), as a condition of receiving a license to

[5] Comments of the Center for Democracy & Technology to the Federal Aviation Administration on Unmanned Aircraft System Test Site Program, April 23, 2013, https://www.cdt.org/files/file/CDTComments_FAA-UAS.pdf.
[6] Rebecca Jacobson, Your 'Anonymous' Credit Card Data is Not So Anonymous, Study Finds, PBS THE RUNDOWN BLOG (Jan. 29, 2015), http://www.pbs.org/newshour/rundown/anonymous-credit-card-data-anonymous-study-finds/.

operate.[7] The DCS would be accessible from the UAS registry and include information such as:

- The purpose for which the UAS has been obtained;
- The scope of information that will be collected by the UAS;
- The length of time information collected by the UAS will be retained;
- Parties that will have access to information collected by the UAS;
- How data collection will be minimized or aggregated and a procedure for data deletion;
- The possible impact the UAS will have on individuals' privacy and the methods the operator will employ to mitigate this impact; and
- An individual point of contact for complaints.

A licensing statement essentially serves as the UAS owner's privacy policy. Allowing the public access to a detailed overview on the UAS' past and current operations reinforces the FIPPs of notice and transparency and will enhance data subjects' right to privacy.

It should be noted that some of CDT's recommended best practices will need to work in coordination with existing or future rules created by regulatory authorities like the Federal Aviation Administration or Department of Transportation. The "license plate" and DCS registry proposal is an example of a best practice that would be most successful if it is harmonized with US regulatory regimes.

Furthermore, because the NTIA process is aimed at developing best practices that protect the privacy of individuals whose image or information may be captured by UAS, we think most of the best practices the NTIA process will identify should likely apply to both hobbyist and non-hobbyist operators alike. We also think that the ability for individuals to obtain identifying information about UAS operators is an important accountability measure. However, we recognize that UAS operators, particularly those who employ UAS for personal use, have a privacy interest in their own identifying information. Thus, we recommend that registration of the operator's identifying information be considered a best practice for non-hobbyist UAS, and suggest that the NTIA process discuss the alternatives that should be available to hobbyist operators (including non-registration or registration by proxy).

IV. Operators should honor requests to opt-out certain areas entirely or partially from UAS data collection

Finally, there should be a mechanism by which certain areas can be opted out of UAS data collection entirely or partially, as well as technical features on commercial and private UAS that allow for owners to honor these requests without significantly hindering their UAS operations. This is in line with the FIPPs of choice and use restrictions, as well as the principles of Privacy and Accountability discussed in the Request for Comments.

[7] Comments of the Center for Democracy & Technology to the Federal Aviation Administration on Unmanned Aircraft System Test Site Program, April 23, 2013, https://www.cdt.org/files/file/CDTComments_FAA-UAS.pdf.

NoFlyZone.org[8] is one example of such an effort. After entering an address on the homepage, the site coordinates with participating UAS manufacturers to automatically prevent UAS from flying over the listed property. The database includes civil and military airspace, airports, hospitals and schools, and the UAS manufacturer voluntarily agrees not to fly over the designated area.

This topic would be another fruitful area for discussion among stakeholders. Voluntary collection restrictions that limit the flight patterns of UAS over certain private and public property could provide powerful protections for individual privacy. But, because these restrictions are likely to be built into the UAS by manufacturers, there may be use-cases for these UAS that manufacturers do not anticipate when deciding to limit operators' abilities to collect or interact with information that is otherwise publicly viewable. Journalists, filmmakers, artists, and others make use of sensor-enabled UAS for expressive purposes, and it is important to understand the potential impact on these activities of manufacturer-set limitations on UAS' operations. CDT encourages NTIA to include a discussion of the criteria and implementation options for an opt-out or Do Not Scan (or No Fly Zone) in its agenda for this proceeding.

For further information, contact:

Alex Bradshaw
Ron Plesser Fellow
Center for Democracy & Technology
202.407.8822
alex@cdt.org

[8] *No Fly Zone,* NOFLYZONE.ORG, https://www.noflyzone.org/ (Last visited Apr. 20, 2015).