KEEPING THE INTERNET
OPEN • INNOVATIVE • FREE

www.cdt.org

CENTER FOR DEMOCRACY
& TECHNOLOGY

1634 I Street, NW
Suite 1100
Washington, DC 20006

DATE	**10 October 2014**
TO	**House of Lords European Union Committee**
FROM	**Center for Democracy & Technology**
# PAGES	**5**

10 October 2014

House of Lords European Union Committee
EU Sub-Committee B (Internal Market, Infrastructure and Employment)
Committee Office, House of Lords
SW1A 0PW
Tel: +44 (0) 20 7219

RE: Evidence for the House of Lords European Union Committee regarding the civil use of RPAS in the EU.

The Center for Democracy & Technology (CDT) is pleased to submit evidence in response to the Internal Market, Infrastructure and Employment Sub-Committee's call for evidence on its inquiry into the civil use in the EU of RPAS.

The inquiry's objective is commendable: striking the right balance between fostering innovation and protecting citizens' privacy and security has proven challenging for legislators both within the EU, the United States and abroad. CDT hopes our submission will help the Committee identify the appropriate middle ground.

The following submission will respond to Question 6: *Are there existing data protection, liability and insurance regimes at EU and Member State levels sufficient to address the concerns raised by the potential greater use of RPAS, or are changes required?*

Protecting citizens' right to privacy as it relates to civil use of RPAS will not require an entirely new legal framework — the EU Data Protection Directive's principles are applicable to RPAS use. However, as indicated in our 2011 comments to the European Commission, more specificity is needed within the Directive and EU member states' regulatory regimes to respond to privacy concerns presented by emerging technologies.[1] Any changes to the Directive or

[1] Comments of the Center for Democracy & Technology to the European Commission in the Matter of Consultation on the Commission's Comprehensive Approach on Personal

other legal acts or guidance should include (1) reasonable limits on RPAS surveillance, data retention and image identification technologies, as well as (2) the creation of publicly available standardized information on RPAS owners and operators.

1. Reasonable limits should be placed on RPAS surveillance, data retention and image identification technologies.

Data protection authorities should focus on providing clear guidance on the applicability of the Directive and their state's regulations to RPAS use, and robust enforcement against bad actors who do not comply with these rules. EU member states' implementation and enforcement of the Directive's principles should include placing reasonable limits on RPAS surveillance, data retention and image identification technologies.

Limits on surveillance conducted by RPAS.

As the European Commission's April 2014 Communication noted, surveillance equipment installed on RPAS is the most commonly identified privacy risk.[2] RPAS 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). RPAS, like manned aircraft, have unique vantage points allowing for levels of surveillance that ground-based individuals may not expect. Moreover, RPAS are becoming more affordable — a simple search for "drone with camera" on popular online shopping websites shows the availability of RPAs equipped with video cameras for well under 100 American dollars.[3]

RPAS surveillance may be appropriate in many contexts, however these technologies should not lead to limitless snooping into individuals' private lives. Regulations on RPAS should set boundaries for surveillance equipment use: RPAS should not, for example, be allowed to peer into windows of people's homes. Some abusive uses of private RPAs should be clearly covered by existing harassment and stalking laws. There should also be reasonable rules limiting RPAS surveillance of areas immediately outside of the home or outdoor spaces on private lands that are enclosed or protected from observation by a passerby on the ground. While it would not be practical to prohibit RPAS surveillance from public airspace of all private property, some private lands may be sufficiently unobservable by ordinary means that RPAS surveillance would be contrary to reasonable privacy expectations.

Data Protection in the European Union, January 15, 2011, https://cdt.org/files/pdfs/CDT_DPD_Comments.pdf.

[2] Communication from the Commission to the European Parliament and the Council, *A new era for aviation: Opening the aviation market to the civil use of remotely piloted aircraft systems in a safe and sustainable manner*, April 8, 2014, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A52014DC0207.

[3] Amazon, Search for "drone with camera," October 10, 2014, http://www.amazon.com/s/ref=nav_search_go?url=search-alias%3Daps&field-keywords=drone+with+camera&rh=i%3Aaps%2Ck%3Adrone+with+camera.

Therefore, CDT recommends formal guidance from privacy regulators delineating the areas where data subjects would reasonably expect to be shielded from public surveillance — certainly within their homes, but potentially for other privately held property where a data subject would have a reasonable expectation of privacy. We encourage data protection authorities to explore and solicit public input on reasonable guidelines to determine where such an expectation exists.

Limits on retention of RPAS collected data.

In addition to RPAS surveillance limitations, reasonable restrictions must be placed on how long data collected through RPAS may be retained. This is in line with the proportionality principle of the Directive: Article 6 requires member states to ensure personal data is "adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed." The Directive further requires that data is kept up to date and not in a form that permits identification for longer than is necessary. Enforcement of these guidelines should thus include limiting retention of RPAS-collected personal data.

Data minimization is one of the most important privacy principles in the RPAS context and deserves particular attention from EU member states. Given RPAS' unique 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 citizens' fundamental privacy rights and reduce the likelihood of data breaches that may result from lengthy retention.

CDT recommends regulatory authorities 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.[4] Unidentifiable information or data that has been "de-identified" to remove all identifying features, may be retained for longer periods. 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.

Limits on use of identification technologies.

CDT believes limits should be placed on the use of facial recognition or other automated identification technologies on RPAS-collected images. Civil use of RPAS will potentially produce numerous images of persons that may not be recognizable without the assistance of identification technologies. Biometric scanning, automated license plate scanners, and other tools designed to identify

[4] 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.

a person based on their unique physical or behavioral characteristics, could allow for identification of every person captured by a commercial RPAS while walking in a public space.

In general, we do not believe that universal recognition of everyone in public (or even private) spaces is necessary, reasonable, or proportional. Certain uses of these technologies to identify general characteristics of individuals may be acceptable — such as biometric characteristic collection that flags someone as falling within a general category like "young woman" or "blond-haired man" — however the categories must be sufficiently large to prevent someone from identifying specific individuals. It may also be permissible to ephemerally scan attributes such as faces or license plates for *specific known images*, like a missing child, a stolen car, or a wanted terrorist. However, the biometric identifiers associated with non-suspect individuals should not be logged or maintained.

2. Standardized information on RPAS owners and operators should be publicly available.

CDT recommends a license plate-type identification system for RPAS and accompanying RPAS registry. Ideally, all RPAS would be marked with a consistent identifier that is used to track and report the RPAS' movements. However traditional license plate identifiers likely will not be detectable from the ground given RPAS' small size and ability to fly at high altitudes. A more practical solution would be to require that all RPAS are configured to emit a standardized signal identifying the drone (such as through a registration number) that is detectable using radio frequency readers, or to provide identification information in response to interrogation by a radio frequency reader.[5]

In addition to identification signals, regulatory authorities could establish a commercial RPAS registry where interested parties may access metadata on the RPAS transmitted through its identification signal — including names of the owner and operator(s) — as well as a link to other information on the RPAS, such as the owner's privacy policy. This registry should be public facing and searchable. (There should be an exception for RPAS such as model aircraft that are designed for personal use.)

This regulatory system should also require detailed statements from the RPAS' owner outlining the RPAS' purpose, planned operations and capabilities. CDT's previous submissions to American regulatory authorities propose requiring RPAS operators in the US to submit a licensing statement, or Data Collection Statement ("DCS"), as a condition of receiving a license to operate.[6] The DCS would be

---

[5] For more information, see Joseph Lorenzo Hall, Center for Democracy & Technology blog, *"License Plates" for Drones?*, March 8, 2013, https://cdt.org/blog/license-plates-for-drones/.

[6] 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.

accessible from the RPAS registry and include information such as:

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

We believe this framework would be equally as effective in the EU. A licensing statement essentially serves as the RPAS owner's privacy policy. Allowing the public access to a detailed overview on the RPAS' past and current operations reinforces the Data Protection Directive's principle of transparency and will empower EU member state citizens to safeguard their right to privacy.

For further information, contact:

Alexandria Bradshaw
Plesser Fellow
Center for Democracy & Technology
alex@cdt.org

Justin Brookman
Director, Consumer Privacy Project
Center for Democracy & Technology
justin@cdt.org