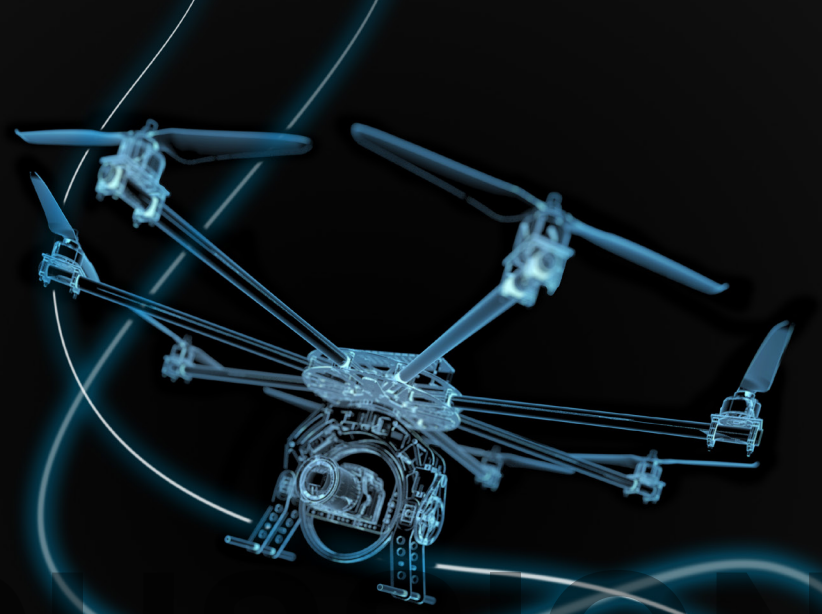


Privacy, Transparency, and Accountability.

Voluntary Best Practices for Commercial and Private Use of Unmanned Aircraft Systems

Introduction.

The benefits of commercial and private unmanned aircraft systems (UAS) are substantial. Technology has moved forward rapidly, and what used to be considered toys are quickly becoming powerful commercial tools that provide enormous benefits in terms of safety and efficiency. Estimates project UAS integration will have an $82 billion economic impact on the U.S. over the next 10 years—with 100,000 new jobs created. Whether UAS are performing search and rescue missions, helping farmers grow better crops in a more sustainable manner, inspecting power lines and cell towers, gathering news and enhancing the public's access to information, performing aerial photography to sell real estate, surveying and mapping areas for stewardship decisions and public policy, delivering medicine to rural locations, providing wireless internet, enhancing construction site safety, or more—society is only just beginning to realize the full potential of UAS. Indeed, the demand for UAS for business purposes has been far-reaching and continues to grow. UAS technology is already bringing substantial benefits to people's daily lives, including cheaper goods, innovative services, safer infrastructure, and greater economic activity. Inevitably, creative minds will devise many more UAS uses that will save lives, save money and make our society more productive.

The very characteristics that make UAS so promising for commercial uses, including their small size, maneuverability and capacity to carry various kinds of recording or sensory devices, also may raise privacy issues. This document is an attempt by all stakeholders—industry, privacy advocates, government and academia—to craft voluntary Best Practices around privacy, transparency and accountability for the private and commercial use of UAS.[1] UAS operators may implement these Best Practices in a variety of ways, depending on their circumstances and technology uses, and based on evolving privacy expectations. The Best Practices do not—and are not meant to—create a de-facto standard of care by which the activities of any particular UAS operator should be judged.

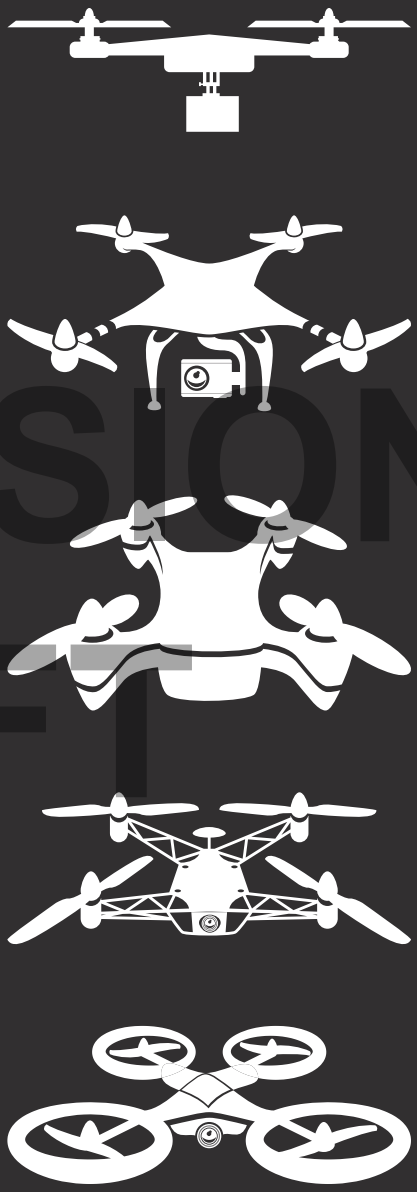
[1] *This effort to draft best practices originated with the President's Feb. 2015 memorandum on UAS. Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems, The White House, Section 2, Feb. 15, 2015.*

Applicability.

These voluntary Best Practices for UAS focus on data collected via a UAS operator (as defined below). The Best Practices do not apply to:

- UAS activities protected by the First Amendment to the United States Constitution; or
- The use of UAS for purposes of emergency response, including safety and rescue responses.

Nothing in these Best Practices should take precedence over the safe operation of a UAS. Also, the Best Practices do not take precedence over the contractual obligations of a UAS operator or the representations of entities contracting UAS operators.



Voluntary Best Practices.

1. INFORM OTHERS OF YOUR USE OF UAS

1(a) When intentionally collecting personal or private data, and where practicable, UAS operators should make a reasonable effort to provide prior notice to individuals of the general timeframe that they anticipate a UAS intentionally collecting such data.[2]

1(b) When a commercial UAS operator[3] anticipates that UAS use may result in incidental or intentional collection of personal or private data, the operator should create a UAS data collection policy, which may be incorporated into an existing privacy policy that is broader than UAS. The UAS data collection policy should be made publicly available online or made available upon request. The policy should include, as practicable:

(1) the general purposes for which UAS will collect data;
(2) the kinds of data UAS will collect;
(3) information regarding data retention and de-identification practices, if any; [4]
(4) examples of the types of entities with whom data collected via UAS will be shared, if any; and
(5) information on how to submit complaints or concerns.

[1(c) When practicable, UAS operators should make a reasonable effort to place call numbers or other identification on UAS that would allow a close-by observer to determine whom to contact about the UAS.] [NTD: ensure consistency with FAA requirements]

1(d) Commercial operators that anticipate intentional collection of personal or private data should make a reasonable effort to specify the purposes for which the UAS is collecting personal or private data in the UAS data collection policy no later than at the time of collection. [5]

These principles shall not apply to a UAS operator that assigns transparency responsibilities to a third-party by contract or other agreement. Also, these principles shall not apply to a UAS operator that collects data about employees when the employer has consented to UAS operations or a land or property owner or licensee when it consents on behalf of all persons on the relevant land or property.

2. MINIMIZE COLLECTION OF PERSONAL OR PRIVATE DATA

2(a) Where practicable, UAS operators should make a reasonable effort to prevent UAS that are collecting personal or private data from entering public airspace over private property if the UAS operation will substantially interfere with the use and enjoyment of the property. These Best Practices recognize that there are legitimate reasons for flights over private property that will not constitute an invasion of privacy. Also, UAS operators may have specific consent of the property owner or data subjects, or contractual obligations to uphold.[6]

2(b) UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of personal or private data about specific individuals, in the absence of a legitimate need to do otherwise, consent of the data subjects, or pursuant to a contract.[7]

3. LIMIT THE USE AND SHARING OF PERSONAL OR PRIVATE DATA

3(a) Commercial UAS operators commit to making reasonable and responsible use of personal or private data and may share that information as reasonable for those uses. Reasonable and responsible practices may vary over time as business practices and individual expectations evolve.

3(b) Personal or private data collected without consent and not pursuant to a contract should not be used in an adverse manner for the following purposes: employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility.

3(c) Commercial UAS operators should make a reasonable effort to avoid using or sharing personal or private data for specific use in targeted marketing to that individual where the operator has actual knowledge that the data subject has an expectation of privacy. There is no restriction on the use or sharing of such information as an input (e.g., statistical information) for broader marketing campaigns nor are there restrictions on the use or sharing of reasonably de-identified personal or private data for marketing purposes.

3(d) UAS operators should generally avoid voluntarily sharing personal or private data with law enforcement entities, except 1) in response to valid judicial, administrative or other legal processes, 2) to protect the operator's property, 3) to defend claims against the operator, 4) to provide what the operator believes in good faith to be evidence of loss of life, serious injury, property destruction or theft, or exploitation of minors, or 5) if the data subjects provide informed prior consent.

3(e) Where practicable, commercial UAS operators should offer data subjects reasonable means to review personal or private data and take reasonable measures to maintain the accuracy of such data.

4. SECURE PERSONAL OR PRIVATE DATA

4(a) Commercial UAS operators should employ reasonable administrative, physical and technical safeguards to protect personal or private data.

4(b) UAS operators should establish a process, appropriate to the size and complexity of the operator, for receiving privacy, security, or safety concerns. Commercial operators should make this process easily accessible to the public, such as by placing points of contact on a company website.[8]

5. MONITOR AND COMPLY WITH EVOLVING FEDERAL, STATE, AND LOCAL UAS LAWS

5(a) UAS operators should comply with applicable laws and UAS privacy and security policies.

[2] What qualifies as a practicable and reasonable effort to provide prior notice will depend on operators' circumstances and the context of the UAS operation. For example, delivery UAS operators may provide customers with an estimated time of delivery. Realtor UAS operators may provide a home seller (and possibly immediate neighbors) with prior notice of the estimated date of UAS photography of the property. Hobbyist UAS operators may not need to notify nearby individuals of UAS flight in the vicinity.

[3] The term "commercial operator" excludes noncommercial and hobbyist operators, even if they later turn commercial.

[4] If it is not practicable to provide an exact retention period, because, for example, the retention period depends on legal hold requirements or evolving business operations, the UAS operator may explain that to data subjects when disclosing its retention policies.

[5] These Best Practices recognize that UAS operators may not be able to predict all future uses of data. Accordingly, the Best Practices do not intend to discourage unplanned or innovative data uses that may result in desirable economic or societal benefits.

[6] This best practice still contemplates flights over private property in public airspace and does not create a new right or boundary for private airspace. Occasional overflights do not constitute a substantial interference with the use and enjoyment of the property. As a general matter, it may not practicable for a high altitude UAS to obtain prior consent.

[7] This best practice is intended to discourage intentional use of UAS for harassment of a single individual as well as for widespread, pervasive monitoring of many identifiable persons.

[8] For a hobbyist it may be as basic as talking to an individual who approaches the hobbyist with a concern.

Definitions.

The term "consent" means words or conduct indicating permission. Consent may be express or implied.

The term "data subjects" refers to the individuals about whom personal or private data is collected.

The term "incidental collection" refers to data collection that is not intentional but which may occur as a byproduct of UAS operation. For example, UAS portrait photography would be intentional collection of personal or private data, whereas a UAS used for architectural or agricultural inspection that happens to capture footage of the face of a passerby would be incidental collection.

The terms "where practicable" and "reasonable" and "reasonable effort" are used frequently in these Best Practices. What qualifies as "practicable" or "reasonable" should depend largely on the circumstances of the UAS operator, the sensitivity of data collected, and degree of privacy risk associated with a particular UAS operation. For example, mapping of sparsely populated areas likely has less impact on privacy than low altitude UAS scanning of residential neighborhoods. The terms are intended to provide flexibility for the unique context of each UAS operation and indicate that efforts that are aligned with industry practices of comparable entities with similar UAS operations may be reasonable.

The term "personal or private data" means information that identifies a particular person where the affected person has a reasonable privacy interest in the data. A person's privacy interest in the data depends on the context of the data capture and the future use of the data. If data captured by UAS likely will not be linked to an individual's name or other personally identifiable information, or if the data is altered so that a specific person is not recognizable, a person does not have a reasonable privacy interest in the data. The incidental collection of data on a passerby in a public space, for instance, likely is not personal or private data. However, if such data is publicly displayed in a malicious manner to identify the individual, a person may have a privacy interest in the data.

Examples of personal or private data may include:

- Imagery of an individual's face that is linked or easily linkable to an identifiable person,
- Voice recordings that are linked or easily linkable to an identifiable person,
- An individual's travel or location patterns that are linked or easily linkable to an identifiable person,
- Unique biometric data, and
- Unique device signals information, such as a MAC address.

The term "UAS operator" means a person, partnership, or organization that uses UAS to collect personal or private data of data subjects. Where a best practice refers only to "UAS operators," the best practice should apply to both commercial and noncommercial private UAS operators. A commercial UAS operator is a person, partnership, or organization engaged in or whose UAS activities affect commerce.

DISCUSSION

Draft 11/19/15

Prepared for the National Telecommunications and Information Administration (NTIA) Multi-Stakeholder Meeting on Privacy, Transparency, and Accountability Regarding Commercial and Private UAS

DRAFT