UAS Privacy Best Practices – Discussion Draft

Center for Democracy & Technology
DRAFT 09/24/15

This goal of this draft is to advance constructive discussion on UAS privacy best practices. This straw man does not presume to propose the final framework or a consensus position, but hopefully provides a reasonable start that other stakeholders may build upon and edit.

In General:

- This document is an attempt by all stakeholders—industry, privacy advocates, government and academia—to craft voluntary Best Practices around privacy, transparency and accountability principles for the private and commercial use of unmanned aircraft systems (UAS). UAS operators may implement these Best Practices in a variety of ways, depending on their circumstances, technology uses, and evolving privacy expectations. The Best Practices are not meant to create a de-facto standard of care by which the activities of any particular UAS operator should be judged.

- The benefits of commercial and private 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. UAS integration is estimated to 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, mapping large areas, 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, are the same characteristics that may raise privacy issues. The purpose of this document is to outline and describe voluntary measures that UAS operators could take to advance UAS privacy, transparency and accountability in this growing and dynamic industry.

- Privacy and transparency best practices for UAS are focused on data collected via UAS.[1] The Best Practices are not intended to apply to data collected through other means – so, for example, a company need not apply these Best Practices to data collected via the company's website.

- UAS operators should comply with all applicable laws and regulations. Best practices are intended to complement legal compliance.

- These UAS Best Practices are informed by the Fair Information Practice Principles (FIPPs). The FIPPs are incorporated in several privacy laws and standards in the US and throughout the world, such as the Privacy Act, the European Union's Data Protection Directive, and FAA requirements for UAS test sites. The FIPPs are[2]
  1) Transparency,
  2) Purpose Specification,
  3) Data Minimization,
  4) Use Limitation,
  5) Individual Participation,
  6) Security,
  7) Accountability and Auditing,
  8) Data Quality and Integrity.

- These UAS Best Practices are not meant to apply to activities protected by the First Amendment to the United States Constitution.

- Nothing in these Best Practices should be construed to impede the use of UAS for purposes of emergency response, including safety and rescue responses.

- Nothing in these Best Practices should take precedent over the safe operation of a UAS.

Definitions:

- "*Sensitive data*" means:

[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, https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[2] In 2008, the U.S. Department of Homeland Security adopted a modern formulation of these principles. 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.

Deleted:

Deleted: ¶
09

Deleted: 24

Deleted: unmanned aircraft systems (

Deleted:)

Deleted: best

Deleted: practices

Deleted: best

Deleted: practices

Deleted: encourage positive conduct beyond

Deleted: best

Formatted: Font: Not Italic

Deleted: practices

Deleted: should be

Deleted: These widely accepted principles

Deleted: throughout the world, EU

Comment [AAA1]: The best practices document loses utility when it is not clearly bounded. Consequently, we suggest clarifying the scope of the document by removing the "but are not limited to" language. Also, as discussed below, the examples can be tightened up. For instance, not all travel patterns are privacy invasive – only when linked to an individual.

Deleted: should include, but are not limited to

- ~~Data that, in the judgment of the UAS operator, are potentially sensitive~~,
- 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,
- Vehicle license plate numbers,
- Unique biometric data, and
- Unique device signals information, such as a MAC address.
- ~~Other data that personally identifies individuals~~.

- Where a best practice refers only to "*UAS operators*," the best practice should apply to both commercial and noncommercial private UAS operators.[3] Most of these best practices refer only to commercial UAS operators to avoid unrealistic expectations for UAS hobbyists.

- "*UAS Operator*" means a person who uses UAS to collect sensitive data of data subjects.

- The terms "*reasonable*" and "*reasonable effort*" are used frequently in these Best Practices. What qualifies as "reasonable" should depend largely on the circumstances of the UAS operator, as well as on 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 license plates. The terms are intended to provide flexibility for the unique context of each UAS operation. They also indicate that efforts that are aligned with industry practices of comparable entities with similar UAS operations may be reasonable.

- The term "*data subjects*" refers to the individuals about whom sensitive data is collected or retained.

- "*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 sensitive 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*.

- ~~Best practices should be a living document, updated as appropriate over time.~~

[3] Consistent with the President's Feb. 2015 memorandum, which calls for best practices for "the commercial and private sectors."

Deleted:
Deleted: ¶ 09
Deleted: 24
Deleted: unique
Deleted: ~~y~~
Formatted: No underline
Deleted: best
Deleted: practices
Deleted: resources and
Deleted: high altitude
Deleted: UAS
Deleted: is
Deleted: , but the term also
Deleted: s
Deleted: an
Deleted: is
Deleted: too weak may be un
Deleted: information
Comment [AAA2]: Since there is no mechanism to update this document, suggest removing this bullet point.

PRINCIPLE 1	APPLICATION	NOTES
TRANSPARENCY – Exercising reasonable efforts to provide transparency for the collection and use of data.	(1)(a) When practicable, UAS operators should make a reasonable effort to place call numbers or other identification on UAS that would allow a person to determine whom to contact about the UAS. (1)(b) When practicable, UAS operators should make a reasonable effort to provide prior notice to individuals of the general timeframe that they may anticipate a UAS intentionally collecting sensitive data. (1)(c) If a commercial UAS operator anticipates that UAS use may result in incidental or intentional collection of sensitive 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 include, as practicable: (1) the purposes for which UAS will collect data; (2) the kinds of data UAS will collect; (3) information regarding data retention and de-identification practices; (4) examples of the types of entities with whom data collected via UAS will be shared; (5) a mechanism for complaints or concerns. The UAS data collection policy should be made publicly available online or made available upon request. 1(d) The Transparency Principle shall not apply to a UAS operator that collects data about a	(1)(a) When the technology is cost effective, should operators enable long-range identification of UAS, such as through a beacon, MAC address, or LED signage? (1)(b) What qualifies as a reasonable effort to provide prior notice will depend on operators' circumstances. 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 notify nearby individuals of UAS flight in the vicinity. (1)(c) Two distinctions made here in referring to UAS operators. *First*: the term "commercial operator" excludes noncommercial and hobbyist operators, even if they later turn commercial. *Second*: "Operator that anticipates incidental or intentional collection of sensitive data." This category may include, for example, delivery UAS, but exclude other commercial UAS uses, such as agriculture. It depends on the operator's circumstances. (1)(c) A UAS data collection policy and a company's general privacy policy need not be independent documents or systems.

Deleted:

Deleted: ¶
09

Deleted: 24

Comment [AAA3]: We have not commented on the "Notes" section.

Comment [AAA4]: Deleted the reference to a UAS crash, which needlessly raises fears about the performance of UAS.

Deleted: For example, if a UAS crashes on private property, the property owners should be capable of determining whom to contact about the UAS.

Comment [AAA5]: This addition clarifies that UAS operators should not have to provide prior notice of the incidental collection of data, which will be difficult to predict.

Deleted: specify

Deleted: The

Deleted: T

Comment [AAA6]: Removed the specificity in the previous language. Data retention and de-identification practices are fluid. The previous language could have been construed as requiring specific timelines for data deletion practices.

Deleted: When data collected via UAS will be

Deleted: deleted

Deleted: or

Deleted: ed

Deleted: W

Comment [AAA7]: The disclosure should be about the types of entities, not specific parties.

Deleted: A

Deleted: point of contact

	businesses' employees when the business 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. 1(e) The Transparency Principle does apply to a UAS operator that assigns transparency responsibilities to a third-party by contract or other agreement.	

Deleted:

Deleted: ¶
09

Deleted: 24

PRINCIPLE 2	APPLICATION	NOTES
PURPOSE SPECIFICATION – Specifying how collected data will be used no later than at the time of collection.	(2)(a) Commercial operators that anticipate intentional collection of sensitive data should make a reasonable effort to specify the purposes for which the UAS is collecting sensitive data in the UAS data collection policy no later than at the time of collection. 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. (2)(b) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant to a contract, UAS operators should avoid using UAS for the specific purpose of intentionally collecting sensitive data where the operator has actual knowledge that the data subject has an expectation of privacy.[4] (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant to a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data about specific individuals,	(2)(a) The purposes of data collection and use will vary based on operator goals. The point is that commercial operators should spell out those purposes. Note that noncommercial operators are exempt from this best practice. (2)(b) Note that this best practice excludes (1) Missions that involve intentional collection of sensitive data in public places; (2) Missions that are not specifically aimed at collecting sensitive data where there is a reasonable expectation of privacy, but under which incidental collection of sensitive data is anticipated; and (3) Missions to collect sensitive data where there is a reasonable expectation of privacy plus a compelling need or consent. (2)(c) This is intended to discourage intentional use of UAS for harassment of a single individual as well as for widespread, pervasive monitoring of many individuals.

[4] See, e.g., Mid-Atlantic Aviation Partnership, *UAS Test Site Privacy Policy*, Virginia Tech, http://www.maap.ictas.vt.edu/privacy-2 (last accessed Sep. 21, 2015). "No MAAP UAS Test Site operation will have as its mission intentionally collecting the personal information of individuals in the general public where they have an expectation of privacy to include imagery, phone, wireless or other electronic emissions that might contain personal information."

Deleted:

Deleted: ¶
09

Deleted: 24

Deleted: incidental or

Deleted: These purposes should be specified in the UAS data collection policy.

Deleted: compelling

Comment [AAA8]: Suggest removing "informed" as it is difficult to prove that an individual was fully informed. Consent (which may be implicit or explicit) should be sufficient.

Deleted: informed

Comment [AAA9]: Suggest adding this contract exception, as UAS operators should be allowed to rely on contractual promises and representations.

Deleted: knows

Deleted: there is

Deleted: reasonable

Deleted: compelling

Deleted: informed

Comment [AAA10]: Suggest adding this contract exception, as UAS operators should be allowed to rely on contractual promises and representations.

Deleted: information

Deleted: s

PRINCIPLE 3	APPLICATION	NOTES
DATA MINIMIZATION – Limiting collection and retention of sensitive data to that which is needed to achieve specified purposes.	(3)(a) Where practicable, UAS operators should make a reasonable effort to prevent UAS that are collecting sensitive data from entering private property or airspace without prior consent of the property owner or appropriate authority, if the UAS operation will substantially interfere with the use and enjoyment of the property. (3)(b) Where practicable, UAS operators should make a reasonable effort to minimize UAS operations involving the collection of sensitive data in public airspace over private property in the absence of a legitimate need to do otherwise, or the consent of the data subjects or pursuant to a contract ~~without informed prior consent of the property owner or appropriate authority.~~ (3)(c) UAS operators may inform data subjects of their sensitive data retention practices including in the previously referenced data collection policy. 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. ~~Where practicable, UAS operators should make a reasonable effort to avoid incidental or intentional collection or retention of sensitive data that are not necessary to fulfill the purposes for which UAS is used – unless the data subjects provide informed prior consent.~~ ~~(3)(d) If a UAS operator knowingly collects or retains sensitive data that are unnecessary to fulfill the purpose for which the UAS is used, the operator should make a reasonable effort to destroy, obfuscate, or de-identify such sensitive data as expeditiously as reasonably possible.~~	(3)(a) Note that "private property or airspace" is undefined. This best practice still contemplates flights over private property in public airspace. This is consistent with current law - one owns an undefined but reasonable amount of airspace above private property. This best practice does not create a new right or boundary for private airspace. Nonetheless, entering private airspace is not just an air traffic management issue since physical intrusion on private property is a privacy risk. (3)(b) As a general matter, it may not practicable for a high altitude UAS to obtain prior consent. (3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use. (3)(d) Note that the phrase "knowingly collects or retains" does not obligate operators to affirmatively review data in search of sensitive data. (3)(e) Three years is the statute of limitations for trespass in CA and NY. This figure is suggested to help operators guard against trespass claims.

Deleted:

Deleted: ¶
09

Deleted: 24

Deleted: Barring exceptional circumstances, such as a safety incident or equipment malfunction,

Deleted: informed

Comment [AAA11]: If this draft is going to include references to trespass law, we should include this element which is found in the Restatement (Second) of Torts, § 158.

Comment [AAA12]: This suggestion more closely ties the provision to privacy concerns.

Deleted:

	~~(3)(e) UAS operators should make a reasonable effort to avoid knowingly retaining sensitive data longer than reasonably necessary to fulfill the purpose for which the UAS was used. With the informed consent of the data subject, or in extraordinary circumstances (such as legal disputes or safety incidents), such data may be held for a longer period. As a rule of thumb, UAS operators should endeavor to avoid knowingly retaining sensitive data for longer than 3 years.~~	

PRINCIPLE 4	APPLICATION	NOTES
USE LIMITATION – Not using or sharing sensitive data for certain purposes.	(4)(a) Commercial UAS operators commit to making reasonable and responsible use of sensitive 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. ~~should make a reasonable effort to avoid intentionally using or sharing sensitive data collected via UAS for any purpose that is not specified in the UAS data collection policy~~. (4)(b) Sensitive 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. ~~If publicly disclosing sensitive data is not necessary to fulfill the purpose for which the UAS is used, commercial UAS operators should avoid knowingly publicly disclosing data collected via UAS until the operator has undertaken a reasonable effort to obfuscate or de-identify sensitive data – unless the data subjects provide informed prior consent to the disclosure.~~ (4)(c) Commercial UAS operators should make a reasonable effort to avoid using or sharing sensitive 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	(4)(b) Google Street View is a good example of this in practice – the images are publicly available but individuals and license plates are blurred.[6] Some agriculture UAS companies use geofencing to "trim" imagery from outside the geofence, thereby focusing data collection on a particular piece of property. (4)(c) A definition of "marketing purposes" – as distinct from public disclosure – may be helpful here. One scenario to which people may object could be using sensitive data collected via UAS to supplement online advertising or junk mail without informed prior consent.

[6] Google "Street View: Privacy and Security" http://www.google.com/maps/about/behind-the-scenes/streetview/privacy (last accessed Sep. 21, 2015).

Deleted:

Deleted: ¶
09

Deleted: 24

Formatted: Strikethrough

Comment [AAA13]: Limiting uses to pre-identified purposes could cut off innovation data uses that could produce economic or societal benefits.

Deleted: purposes, unless the data subjects provide informed prior consent.

	broader marketing campaigns nor are there restrictiosn on the use or sharing of reasonably de-identified sensitive data for marketing purposes. (4)(d) UAS operators should generally avoid voluntarily sharing sensitive 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.[5]	

Deleted:

Deleted: ¶
09

Deleted: 24

[5] This list was drawn in part from 18 USC 2702(b).

PRINCIPLE 5	APPLICATION	NOTES
INDIVIDUAL PARTICIPATION – Facilitating informed and reasonable choices to data subjects regarding the collection, use, and retention of sensitive data.	(5)(a) Where practicable, UAS operators should offer data subjects reasonable means to review sensitive data and take reasonable measures to maintain the accuracy of such data. ~~If an individual requests that a UAS operator destroy, obfuscate, or de-identify sensitive data about the individual, and retention of the sensitive data is not necessary to fulfill a purpose for which the UAS is used, the UAS operator should take reasonable steps to honor this request.~~ ~~(5)(b) Opportunities for individuals to participate in data management are described in (2)(b), (3)(a), (3)(b), (3)(c), (4)(b), (4)(c), and (4)(d) of these best practices.~~	

Deleted:

Deleted: ¶
09

Deleted: 24

Formatted: Strikethrough

Formatted: Strikethrough

PRINCIPLE 6	APPLICATION	NOTES
SECURITY – Exercising reasonable efforts to secure collected and retained data.	(6)(a) Commercial UAS operators should employ reasonable administrative, physical and technical safeguards to protect sensitive data. ~~develop a written security policy with respect to the collection, use, storage, and dissemination of data collected via UAS appropriate to the size and complexity of the operator and the sensitivity of the data collected and retained.~~[7] ~~(6)(b) Commercial UAS operators should make a reasonable effort to regularly monitor systems for breach and data security risks.~~ ~~(6)(c) Commercial UAS operators should make a reasonable effort to provide security training to employees with access to sensitive data collected via UAS.~~ ~~(6)(d) Commercial UAS operators should make a reasonable effort to permit only authorized individuals to access sensitive data collected via delivery UAS.~~ ~~(6)(e) Commercial UAS operators should make a reasonable effort to encrypt or hash retained sensitive data that have not been publicly disclosed.~~	(6)(a) A security policy should include, at minimum, such basic steps as keeping software up to date and downloading security patches for known vulnerabilities. Should best practices include cybersecurity of the UAS itself – such as defense against unauthorized operation of the UAS by third parties?

Deleted:

Deleted: ¶
09

Deleted: 24

Formatted: Strikethrough

Formatted: Strikethrough

Formatted: Strikethrough

[7] This "size and complexity" language is mirrored in security guidelines elsewhere, such as the HIPAA Security Standards [45 CFR 164.306(b)(2)], and the Federal Reserve Security Guidelines for financial institutions (see III. Implementing an Information Security Program, available at http://www.federalreserve.gov/bankinforeg/interagencyguidelines.htm).

PRINCIPLE 7	APPLICATION	NOTES
ACCOUNTABILITY – Establishing internal accountability controls to ensure compliance with privacy policies and laws.	(7)(a) 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. (7)(b) Commercial UAS operators should identify individuals to oversee compliance with applicable laws and UAS privacy and security policies. ~~(7)(c) Commercial UAS operators should make a reasonable effort to periodically review compliance with applicable laws and privacy and security policies. As a rule of thumb, commercial operators should aim to conduct reviews no less than biennially.~~	(7)(a) Note that this best practice is silent on what the process should be. For a hobbyist it may be as basic as talking to an individual who approaches the hobbyist with a concern. (7)(c) Larger and more complex UAS operators may want to consider external review.

END

Deleted:

Deleted: ¶
09

Deleted: 24

Formatted: Strikethrough

Comment [AAA14]: 7(c) is covered by 7(b).

Formatted: Strikethrough