

## 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:**

- Privacy and transparency best practices for unmanned aircraft systems (UAS) are focused on data collected via UAS.<sup>1</sup> 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 encourage positive conduct beyond legal compliance.
- UAS best practices should be informed by the Fair Information Practice Principles (FIPPs). These widely accepted principles are incorporated in several privacy laws and standards in the US and EU, such as the Privacy Act, the European Union’s Data Protection Directive, and FAA requirements for UAS test sites. The FIPPs are<sup>2</sup>
  - 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.

---

<sup>1</sup> 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>.

<sup>2</sup> 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](http://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf).

- “*Sensitive data*” 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,
  - Voice recordings,
  - An individual's unique travel or location patterns,
  - Vehicle license plate numbers,
  - Unique biometric data,
  - Unique device signals information, such as a MAC address,
  - Other data that personally identify individuals.
  
- Where a best practice refers only to “*UAS operators*,” the best practice should apply to both commercial and noncommercial private UAS operators.<sup>3</sup> Most of these best practices refer only to commercial UAS operators to avoid unrealistic expectations for UAS hobbyists.
  
- The terms “*reasonable*” and “*reasonable effort*” are used frequently in these best practices. What qualifies as “reasonable” should depend largely on the resources and 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, high altitude mapping UAS likely has less impact on privacy than low altitude UAS scanning license plates. The term is intended to provide flexibility for the unique context of each UAS operation, but the term also indicates that an effort that is too weak may be unreasonable.
  
- The term “*data subjects*” refers to the individuals about whom information 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 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.

---

<sup>3</sup> Consistent with the President’s Feb. 2015 memorandum, which calls for best practices for “the commercial and private sectors.”

PRINCIPLE 1	APPLICATION	NOTES
<p><i>TRANSPARENCY</i> – Exercising reasonable efforts to provide transparency for the collection and use of data.</p>	<p>(1)(a) UAS operators should make a reasonable effort to place call numbers or other identification on UAS. For example, if a UAS crashes on private property, the property owners should be capable of determining whom to contact about the UAS.</p> <p>(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 collecting sensitive data.</p> <p>(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 specify: (1) The purposes for which UAS will collect data; (2) The kinds of data UAS will collect; (3) When data collected via UAS will be deleted or de-identified; (4) With whom data collected via UAS will be shared; (5) A point of contact for complaints or concerns. The UAS data collection policy should be made publicly available online.</p>	<p>(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?</p> <p>(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.</p> <p>(1)(c) Two distinctions made here in referring to UAS operators. <i>First:</i> the term “commercial operator” excludes noncommercial and hobbyist operators, even if they later turn commercial. <i>Second:</i> “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.</p> <p>(1)(c) A UAS data collection policy and a company’s general privacy policy need not be independent documents or systems.</p>

PRINCIPLE 2	APPLICATION	NOTES
<p><i>PURPOSE SPECIFICATION</i> – Specifying how collected data will be used no later than at the time of collection.</p>	<p>(2)(a) Commercial operators that anticipate incidental or intentional collection of sensitive data should make a reasonable effort to specify the purposes for which the UAS is collecting data no later than at the time of collection. These purposes should be specified in the UAS data collection policy.</p> <p>(2)(b) In the absence of a compelling need to do otherwise, or informed consent of the data subjects, UAS operators should avoid using UAS for the specific purpose of intentionally collecting sensitive data where the operator knows there is a reasonable expectation of privacy.<sup>4</sup></p> <p>(2)(c) In the absence of a compelling need to do otherwise, or informed consent of the data subjects, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive information about individuals.</p>	<p>(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.</p> <p>(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.</p> <p>(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.</p>

<sup>4</sup> 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.”

PRINCIPLE 3	APPLICATION	NOTES
<p><i>DATA MINIMIZATION</i> – Limiting collection and retention of sensitive data to that which is needed to achieve specified purposes.</p>	<p>(3)(a) Barring exceptional circumstances, such as a safety incident or equipment malfunction, UAS operators should make a reasonable effort to prevent UAS from entering private property or airspace without informed prior consent of the property owner or appropriate authority.</p> <p>(3)(b) Where practicable, UAS operators should make a reasonable effort to minimize operations in public airspace over private property without informed prior consent of the property owner or appropriate authority.</p> <p>(3)(c) 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.</p> <p>(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.</p> <p>(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.</p>	<p>(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.</p> <p>(3)(b) As a general matter, it may not be practicable for a high altitude UAS to obtain prior consent.</p> <p>(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.</p> <p>(3)(d) Note that the phrase “knowingly collects or retains” does not obligate operators to affirmatively review data in search of sensitive data.</p> <p>(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.</p>

PRINCIPLE 4	APPLICATION	NOTES
<p><i>USE LIMITATION</i> – Not using or sharing sensitive data for certain purposes.</p>	<p>(4)(a) Commercial UAS operators 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.</p> <p>(4)(b) 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.</p> <p>(4)(c) Commercial UAS operators should make a reasonable effort to avoid using or sharing sensitive data for marketing purposes, unless the data subjects provide informed prior consent.</p> <p>(4)(d) UAS operators should generally avoid voluntarily sharing sensitive data with law enforcement entities, except 1) in response to valid judicial or administrative 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.<sup>5</sup></p>	<p>(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.<sup>6</sup> Some agriculture UAS companies use geofencing to “trim” imagery from outside the geofence, thereby focusing data collection on a particular piece of property.</p> <p>(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.</p>

<sup>5</sup> This list was drawn in part from 18 USC 2702(b).

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

PRINCIPLE 5	APPLICATION	NOTES
<p><i>INDIVIDUAL PARTICIPATION</i> – Facilitating informed and reasonable choices to data subjects regarding the collection, use, and retention of sensitive data.</p>	<p>(5)(a) 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.</p> <p>(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.</p>	

PRINCIPLE 6	APPLICATION	NOTES
<p><i>SECURITY</i> – Exercising reasonable efforts to secure collected and retained data.</p>	<p>(6)(a) Commercial UAS operators should 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.<sup>7</sup></p> <p>(6)(b) Commercial UAS operators should make a reasonable effort to regularly monitor systems for breach and data security risks.</p> <p>(6)(c) Commercial UAS operators should make a reasonable effort to provide security training to employees with access to sensitive data collected via UAS.</p> <p>(6)(d) Commercial UAS operators should make a reasonable effort to permit only authorized individuals to access sensitive data collected via delivery UAS.</p> <p>(6)(e) Commercial UAS operators should make a reasonable effort to encrypt or hash retained sensitive data that have not been publicly disclosed.</p>	<p>(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.</p> <p>Should best practices include cybersecurity of the UAS itself – such as defense against unauthorized operation of the UAS by third parties?</p>

<sup>7</sup> 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/bankinfo/reg/interagencyguidelines.htm>).



PRINCIPLE 7	APPLICATION	NOTES
<p><i>ACCOUNTABILITY</i> – Establishing internal accountability controls to ensure compliance with privacy policies and laws.</p>	<p>(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.</p> <p>(7)(b) Commercial UAS operators should identify individuals to oversee compliance with applicable laws and UAS privacy and security policies.</p> <p>(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.</p>	<p>(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.</p> <p>(7)(c) Larger and more complex UAS operators may want to consider external review.</p>

END