# UAS Privacy Best Practices – Discussion Draft v 2

Center for Democracy & Technology
DRAFT 1109/2416/15

~~*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:

- 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. UAS integration is estimated to have significant positive economic impact on the U.S. 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. 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 some of 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 for private and commercial use of UAS. UAS operators may implement these Best Practices in a variety of ways, depending on their circumstances, technology uses, and evolving privacy expectations.

- These Privacy Best Practices for unmanned aircraft systems (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.

- These Best Practices are not intended to create a legal standard of care by which the activities of any particular UAS operator should be judged. These Best Practices are also not intended to serve as a template for future statutory or

[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.

regulatory obligations, in part because doing so would raise First Amendment issues.

- UAS operators should comply with all applicable laws and regulations. These Best Practices do not replace or take precedence over any local, state, federal, or Constitutional law or regulation. Best Practices are intended to encourage positive conduct that complements legal compliance.

- Nothing in these Best Practices should take precedence over the contractual obligations of a UAS operator or the representations of entities contracting UAS operators. However, entities contracting UAS operators should consider these Best Practices when setting the terms of a contract for UAS use, and UAS operators should consider these Best Practices when choosing to accept a contact for UAS use.

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

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

- UAS Privacy Best Practices should be generally informed by the Consumer Privacy Bill of Rights (CPBR) principles~~Fair Information Practice Principles (FIPPs)~~. The CPBR was endorsed by the White House, and the Federal Trade Commission (FTC) noted that the CPBR principles are consistent with the FTC's own privacy framework.~~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~~[2] The principles of the CPBR are
  1) Transparency,
  2) ~~Purpose Specification,~~Respect for Context,
  ~~3)~~ Focused Collection~~Data Minimization,~~
  ~~4)~~3) ~~Use Limitation~~,
  ~~5)~~4) Individual ~~Participation~~Control,
  ~~6)~~5) Security,
  6) Accountability,
  ~~7)~~ Access and Accuracy ~~and Auditing,~~
  ~~8)~~7) ~~Data Quality and Integrity~~.

[2] The White House, *Consumer Data Privacy In A Networked World,* Feb. 2012, https://www.whitehouse.gov/sites/default/files/privacy-final.pdf. The CPBR is based on the Fair Information Practice Principles, see 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

[2] The Federal Trade Commission, *Protecting Consumer Privacy In An Era Of Rapid Change*, Mar. 2012, pg. 38, https://www.ftc.gov/sites/default/files/documents/reports/federal-trade-commission-report-protecting-consumer-privacy-era-rapid-change-recommendations/120326privacyreport.pdf#page=54.

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

## Definitions

- "*Personal data*" should include, but are not limited to:
  a) Data that, in the context in which the data are collected, and in the judgment of the UAS operator, are ~~potentially~~ sensitive,
  b) Unique biometric data, such as i~~I~~magery of an individual's face and voice recordings, that are linked or easily linkable to an identifiable person,
  ~~c) Voice recordings,~~
  ~~d)~~c) An individual's unique travel or location patterns that are linked or easily linkable to an identifiable person,
  ~~e)~~d) Vehicle license plate numbers,
  ~~f) Unique biometric data,~~
  e) Unique device ~~signals~~ information, such as a telephone number or MAC address,
  ~~g)~~f) Other unique identifiers of individuals, such as Social Security, credit card, or other financial account numbers.

- "*Personal data*" does NOT include data that a UAS operator – or the operator's agent – alters such that there is a reasonable basis for expecting that the data could not be linked to a specific individual or device, such as by blurring imagery of an otherwise identifiable individual's face.

- 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.

- 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 resources and circumstances of the UAS operator, ~~as well as on~~ the sensitivity of data collected, and ~~degree of privacy risk~~ the context 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 terms are intended to provide flexibility for the unique ~~context~~ privacy risks of each UAS operation, and indicate that efforts aligned with practices of comparable entities with similar UAS operations may be reasonable; ~~but~~ however, the terms also indicate that an effort that is too weak may be unreasonable.

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

- 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*.~~

| PRINCIPLE 1 | APPLICATION | NOTES |
|---|---|---|
| *TRANSPARENCY* – Exercising reasonable efforts to provide transparency for the collection and use of data. | (1)(a) Where practicable, 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~~ that could allow a close-by observer to determine whom to contact about the UAS.<br><br>(1)(b) Where 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~~ personal data.<br><br>(1)(c) If a commercial UAS operator anticipates that UAS use may result in incidental or intentional collection of ~~sensitive~~ personal 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~~include, as practicable: (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~~Information regarding data retention and de-identification practices ~~deleted or de-identified~~; (4) The types of entities w~~W~~ith whom data collected via UAS will be shared; (5) A mechanism or point of contact for complaints or concerns. The UAS data collection policy should be made publicly available online, or – where online publication | (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?~~This signage should not replace or interfere with any signage required by law or regulation. The signage suggested by this Best Practice do not necessarily need to enable visual identification from afar (though that would be even better), but the signage should at minimum enable identification from an observer that physically handles the UAS (such as by picking up the UAS and looking at the signage). To the extent that signage required by regulation accomplishes this goal, no additional signage is necessary.<br><br>(1)(b) What qualifies as practicable and a 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 notify nearby individuals of UAS flight in the vicinity verbally or with a sign.<br><br>(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~~personal data." This category may include, for example, delivery UAS, but exclude other commercial |

| | | |
|---|---|---|
| | is impracticable – made available upon request. | UAS uses, such as precision agriculture. It depends on the operator's circumstances.<br><br>(1)(c) A UAS data collection policy and a company's general privacy policy need not be independent documents or systems. UAS operators may modify a broader existing data collection policy to cover data collected via UAS. |

| PRINCIPLE 2 | APPLICATION | NOTES |
|---|---|---|
| ~~*PURPOSE SPECIFICATION*~~ *RESPECT FOR CONTEXT* – Specifying how collected data will be used no later than at the time of collection and in ways that are consistent with the context in which the data is collected. | (2)(a) Commercial operators that anticipate incidental or intentional collection of ~~sensitive~~ personal 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.<br><br>(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~~ personal data<br>(i) Where the operator knows the~~re~~ data subject ha~~i~~s a reasonable expectation of privacy,[4]<br>(ii) For eligibility for employment, credit, or health care treatment.<br><br>(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~~ personal ~~information~~ data about individuals.<br><br>(2~~3~~)(~~a~~d) 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 | (2)(a) The purposes of data collection and use will vary based on operator goals and context. The point is that commercial operators should spell out those purposes. Those purposes may include collecting data with the anticipation of future business uses that are unknown to the operator at the time of collection due to evolving business practices. Note that noncommercial operators are exempt from this Best Practice.<br><br>(2)(b) Note that this B~~b~~est P~~p~~ractice ~~excludes~~ does not explicitly forbid (1) Missions that involve intentional collection of ~~sensitive~~ personal data in public places; (2) Missions that are not specifically aimed at collecting ~~sensitive~~ personal data where there is a reasonable expectation of privacy, but under which incidental collection of ~~sensitive~~ personal data is anticipated; and (3) Missions to intentionally collect ~~sensitive~~ personal data where there is a reasonable expectation of privacy plus a compelling need or consent. However, consistent with (1)(c), the operator should be transparent that the UAS will be used for these purposes.<br><br>(2)(c) This is intended to discourage intentional use of UAS for harassment of a single individual as well as for pervasive monitoring of many individuals without consent or compelling need. |

[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."

| | | |
|---|---|---|
| | or appropriate authority.<br><br>(32)(be) Where practicable, and where it will not impede the purpose for which the UAS is used, UAS operators should make a reasonable effort to minimize UAS operations in public airspace over private property without informed prior consent of the property owner or appropriate authority. | (23)(ad) Note that "private property or airspace" is undefined. This Best Practice still contemplates flights over private property in public airspace. This is consistent withBest Practice does not expand on current law – one owns an undefined but reasonable amount of airspace above private property – and. tThis 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 sincebecause unauthorized physical intrusion on private property is a privacy risk.<br><br>(23)(be) This Best Practice suggests that if a flight path over private property and a flight path over public property are both equally practicable, the UAS operator should make a reasonable effort to fly over public property. As a general matter, it may not practicable for a high altitude UAS to obtain prior consentmake a distinction between private and public property. |

| PRINCIPLE 3 | APPLICATION | NOTES |
|---|---|---|
| ~~*DATA MINIMIZATION*~~ *FOCUSED COLLECTION* – Limiting collection and retention of sensitive data to that which is needed to achieve ~~specified~~ purposes specified under the *Respect For Context* principle. | (3)(a~~c~~) Where practicable, UAS operators should make a reasonable effort to avoid incidental or intentional collection or retention of ~~sensitive~~personal data that are ~~not necessary to fulfill~~unrelated to the purposes for which UAS is used~~ unless the data subjects provide informed prior consent~~.<br><br>(3)(b~~d~~) If a UAS operator knowingly collects or retains ~~sensitive~~personal data that are ~~unnecessary to fulfill~~unrelated to the purpose for which the UAS is used, the operator should make a reasonable effort to destroy, obfuscate, or de-identify such ~~sensitive~~personal data as expeditiously as reasonably possible.<br><br>(3)(c~~e~~) UAS operators should make a reasonable effort to avoid knowingly retaining ~~sensitive~~personal data longer than reasonably necessary to fulfill the purpose for which the ~~UAS was used~~data were collected. With the informed consent of the data subject, or in exceptional circumstances (such as legal disputes or safety incidents), such data may be held for a longer period.<br><br>(3~~4~~)(a~~d~~) Commercial UAS operators should make a reasonable effort to avoid intentionally using or sharing ~~sensitive~~personal data collected via UAS for any purpose that is not specified in the UAS data collection policy.<br><br>(3~~4~~)(b~~e~~) If publicly disclosing ~~sensitive~~personal 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 | (3)(a~~c~~) Note this Best Practice still allows for intentional collection of ~~sensitive~~personal data if that is the purpose of UAS use. However, note also that under the Best Practice in (2)(b), operators should generally not use UAS for the specific purpose of collecting personal data where the data subject has a reasonable expectation of privacy.<br><br>(3)(b~~d~~) Note that the phrase “knowingly collects or retains” does not obligate operators to proactively review collected data in search of ~~sensitive~~personal data. This Best Practice applies only when the UAS operator knows that unrelated personal data were collected.<br><br>~~(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.~~<br><br>(3)(d) Note that in the notes to (2)(a), those purposes can include collection for future business purposes that are unforeseen at the time of collection.<br><br>(3~~4~~)(b~~e~~) Google Street View is a good example of this in practice – the images |

| | | |
|---|---|---|
| | undertaken a reasonable effort to obfuscate or de-identify ~~sensitive~~personal data – unless the data subjects provide informed prior consent to the disclosure.<br><br>(34)(~~c~~f) Commercial UAS operators should make a reasonable effort to avoid using or sharing ~~sensitive~~personal data for marketing purposes, until the operator has undertaken a reasonable effort to obfuscate or de-identify personal data – unless the data subjects provide informed prior consent to the disclosure.<br>~~unless the data subjects provide informed prior consent.~~<br><br>(34)(~~d~~i) UAS operators should generally avoid ~~voluntarily~~ sharing ~~sensitive~~personal data with law enforcement entities, except 1) in response to valid judicial, ~~or~~ 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]<br><br>~~As a rule of thumb, UAS operators should endeavor to avoid knowingly retaining sensitive data for longer than 3 years.~~ | 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.<br><br>~~(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.~~ |

[5] This list was drawn in part from 18 USC 2702(b).
[6] Google "Street View: Privacy and Security" http://www.google.com/maps/about/behind-the-scenes/streetview/privacy (last accessed Sep. 21, 2015).

| PRINCIPLE 45 | APPLICATION | NOTES |
|---|---|---|
| *INDIVIDUAL ~~PARTICIPATION~~ CONTROL* – Facilitating informed and reasonable choices to data subjects regarding the collection, use, and retention of ~~sensitive~~personal data. | (45)(a) Where practicable, i~~i~~f an individual requests that a UAS operator correct, destroy, obfuscate, or de-identify ~~sensitive~~personal data about the individual, and retention of the ~~sensitive~~personal 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.<br><br>(45)(b) Opportunities for individuals to participate in data management are described in (2)(b), (2)(c), (2)(d), (2)(e), (3)(c), (3)(e), (3)(f), (3)(i), and (6)(a)~~(2)(b), (3)(a), (3)(b), (3)(c), (4)(b), (4)(c), and (4)(d)~~ of these Best Practices. | (4)(a) This Best Practice does not necessarily require that operators be capable of performing each of these actions (correct, destroy, obfuscate, de-identify). For example, an operator may have the capability to de-identify or destroy, but not correct data. This Best Practice also does not necessarily require that the operator each action if multiple actions are requested; for example, if a data subject that requests both de-identification and destruction, it may be reasonable for the operator to simply destroy the data. |

| PRINCIPLE 56 | APPLICATION | NOTES |
|---|---|---|
| *SECURITY* – Exercising reasonable efforts to secure collected and retained data. | (56)(a) Commercial UAS operators should ~~develop~~ have 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]<br><br>(56)(b) Commercial UAS operators should make a reasonable effort to regularly monitor systems for breach and data security risks.<br><br>(56)(c) Commercial UAS operators should make a reasonable effort to provide security training to employees with access to ~~sensitive~~personal data collected via UAS.<br><br>(56)(d) Commercial UAS operators should make a reasonable effort to permit only authorized individuals to access ~~sensitive~~personal data collected via delivery UAS.<br><br>(56)(e) Commercial UAS operators should make a reasonable effort to encrypt or hash retained ~~sensitive~~personal data that have not been publicly disclosed. | (56)(a) As with the data collection policy referenced in (1)(c), UAS operators may modify a broader existing security policy to incorporate data collected via UAS. 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?~~ |

[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 67 | APPLICATION | NOTES |
|---|---|---|
| *ACCOUNTABILITY* – Establishing internal accountability controls to ensure compliance with privacy policies and laws. | (67)(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.<br><br>(67)(b) Commercial UAS operators should identify individuals to oversee compliance with applicable laws and UAS privacy and security policies.<br><br>(67)(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.~~ | (67)(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.<br><br>(67)(c) Larger and more complex UAS operators may want to consider external review. |

END