VOLUNTARY BEST PRACTICES
FOR COMMERCIAL AND PRIVATE USE OF
UNMANNED AIRCRAFT SYSTEMS:

PRIVACY, TRANSPARENCY, AND ACCOUNTABILITY

Combined Draft

For discussion purposes only
Last Updated: December 22, 2015

Table of Contents

Section headers in the HL and CDT drafts:

Hogan Lovells	CDT
[Introduction]	[In General]
[Applicability]	No similar section header
(see below for definitions)	[Definitions]
[Voluntary Best Practices for Privacy, Transparency, and Accountability]	[Principles]
1. [Inform Others of Your Use of UAS 2. Minimize Collection of Personal or Private Data 3. Limit the Use and Sharing of Personal or Private Data 4. Secure Personal or Private Data 5. Monitor and Comply with Evolving Federal, State, and Local UAS Laws]	[**1) Transparency – Exercising reasonable efforts to provide transparency for the collection and use of data.** **2) 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.** **3) Focused Collection – Limiting collection and retention of sensitive data to that which is needed to achieve purposes specified under the Respect For Context principle.** **4) Individual Control – Facilitating informed and reasonable choices to data subjects regarding the collection, use, and retention of personal data.** **5) Security – Exercising reasonable efforts to secure collected and retained data.** **6) Accountability – Establishing internal accountability controls to ensure compliance with privacy policies and laws.**]
[Definitions]	(see above for definitions)

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 can provide enormous benefits in terms of safety and efficiency. UAS integration will have a significant positive economic impact in the United States. 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 and provide insurance services, surveying and mapping areas for 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. UAS technology is already bringing substantial benefits to people's daily lives, including cheaper goods, innovative services, safer infrastructure, recreational uses, 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 and non-commercial uses, including their small size, maneuverability and capacity to carry various kinds of recording or sensory devices, also may raise privacy issues. The purpose of this document is to outline and describe voluntary Best Practices that UAS operators could take to advance UAS 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 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.

APPLICABILITY

These voluntary Best Practices for UAS focus on data collected via a UAS operator, which includes both commercial and non-commercial operators. The Best Practices do not apply to data collected by other means – for instance, a company need not apply these Best Practices to data collected via the company's website.

Nothing in these Best Practices shall:

- Be construed to limit or diminish freedoms guaranteed under the Constitution;
- Replace or take precedence over any local, state, or federal or regulation;

[1] This effort to draft best practices originated with the President's February 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.

- Take precedence over contractual obligations or the representations of entities contracting UAS operators[2] ; or

- Impede the safe operation of a UAS.

[**CDT: Many of the Best Practices refer only to commercial UAS operators to avoid unrealistic expectations for UAS hobbyists**]

[The Best Practices do not apply to the use of UAS for purposes of emergency response / **CDT: 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 operators should comply with all applicable laws and regulations. The Best Practices are intended to encourage positive conduct that complements legal compliance.

[**CDT: These Best Practices are also not intended to serve as a template for future statutory or regulatory obligations, in part because doing so would raise First Amendment issues.**]

[**CDT: Best Practices should be a living document, updated as appropriate over time.**]

DEFINITIONS

The term "*commercial UAS operator*" means a UAS operator engaged in or whose UAS activities affect commerce. The term does not include hobbyist UAS operators.

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*" depend largely on the circumstances of the UAS operator, the sensitivity of data collected, and the context associated with a particular UAS operation. For instance, mapping of sparsely populated areas likely has less impact on privacy than low altitude UAS flight. The terms *"where practicable"* and "*reasonable*" are intended to provide flexibility for the unique context of each UAS operation and indicate that practices of comparable entities with similar UAS operations may be reasonable. However, the terms also indicate that an effort that is too weak may be unreasonable.

Breakout of differences between "*personal or private data*" and "personal data" in the HL and CDT drafts:

---

[2] 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 contract for UAS use.

Hogan Lovells	CDT
[“Personal or private data”**]**	**[**“**Personal data**”**]**
[“means information that identifies a particular person where the affected person has a reasonable privacy interest in the data”**]**	No similar provision
[“A person’s privacy interest in the data depends on the context of the data capture and the future use of the data”**]**	No similar provision
[“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”**]**	**[“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”]**
[“The incidental collection of data on a passerby in a public space, for instance, likely is not personal or private data”**]**	No similar provision
[“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”**]**	No similar provision
“Examples of personal or private data **[**may**]** include:”	“Examples of personal or private data **[should]** include:”
	• **[“Data that, in the context in which the data are collected, and in the judgment of the UAS operator, are sensitive”]**
• An individual's travel or location patterns that are linked or easily linkable to an identifiable person;	• Same
• Unique biometric data, **such as imagery of an individual’s face and voice recordings, that are linked or easily linkable to an identifiable person**	• Same concepts
• No similar provision	• **[Vehicle license plate numbers]**
• Unique device information, such as a MAC address	• Same

• No similar provision	• **[telephone number]**
• No similar provision	• **[Other unique identifiers of individuals, such as Social Security, credit card, or other financial account numbers]**

The term "*UAS operator*" **[**means a person, partnership, or organization that uses UAS to collect **[**personal or private data**]** of data subjects - **CDT does not include:]**. Where a best practice refers only to "*UAS operators*," the best practice should apply to both commercial and noncommercial private UAS operators.

Voluntary Best Practices

[NPPA suggests adding: The following constitute voluntary best practices except where explicitly required by law or exempted as First Amendment protected activities.]

[1. INFORM OTHERS OF YOUR USE OF UAS]

1(a) 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 [personal or private data].[3]

1(b) When a commercial UAS operator 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 in place no later than the time of collection and made publicly available online or made available upon request **[CDT: where online publication is impracticable]**. The policy should include, as practicable:

- (1) the **[CDT does not include: general]** purposes for which UAS will collect data;[4]
- (2) the kinds of data UAS will collect;
- (3) information regarding any data retention and de-identification practices;[5]
- (4) examples of the types of any entities with whom data collected via UAS will be shared; and
- (5) information on how to submit complaints or concerns.

---

[3] 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. Real estate professionals using UAS 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.

[4] 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.

[5] 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.

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

[2. MINIMIZE COLLECTION OF PERSONAL OR PRIVATE DATA]

UAS operators should avoid using UAS for the purpose of persistent and continuous collection of personal or private data about specific individuals, in the absence of a **[**legitimate / **CDT: compelling]** need to do otherwise or **[CDT: informed]** consent of the data subject. [6]

Side-by-side of the remaining provisions:

Hogan Lovells	CDT
No similar provision in this section. A similar provision is included in section 1(b) above.	~~**(2)(a) Commercial operators that anticipate incidental or intentional collection of 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.**~~ ~~**"Notes": 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.**~~
No similar provision.	**[(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 personal data (i) Where the operator knows the data subject has a reasonable expectation of privacy…]**
No similar provision. However, the Hogan Lovells draft states that "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:	~~**(2)(b) …(ii) For eligibility for employment, credit, or health care treatment.**~~ ~~**"Notes": Note that the [Best Practice 2(b)] does not**~~

6 ~~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.~~

employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility."	~~explicitly forbid (1) Missions that involve intentional collection of personal data in public places; (2) Missions that are not specifically aimed at collecting personal data where there is a reasonable expectation of privacy, but under which incidental collection of personal data is anticipated; and (3) Missions to intentionally collect 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.~~
[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.**]**	**[(2)(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 or appropriate authority.]** [7] **[(2)(e) 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.]** [8]
[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.**]**	No similar provision

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

Personal or private data collected without **[CDT: informed]** 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.

7 **[CDT "Notes": Note that "private property or airspace" is undefined. This Best Practice still contemplates flights over private property in public airspace. This Best Practice does not expand on current law – one owns an undefined but reasonable amount of airspace above private property – and 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 because unauthorized physical intrusion on private property is a privacy risk.]**

8 **[CDT "Notes": 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.]**

Side-by-side of the remaining provisions:

Hogan Lovells	**CDT**
[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(a) Where practicable, UAS operators should make a reasonable effort to avoid incidental or intentional collection or retention of personal data that are unrelated to the purposes for which UAS is used. [9]]** **[3(b) If a UAS operator knowingly collects or retains personal data that are unrelated to the purpose for which the UAS is used, the operator should make a reasonable effort to destroy, obfuscate, or de-identify such personal data as expeditiously as reasonably possible. [10]]** **[3(c) UAS operators should make a reasonable effort to avoid knowingly retaining personal data longer than reasonably necessary to fulfill the purpose for which the 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.]** **[3(d) Commercial UAS operators should make a reasonable effort to avoid intentionally using or sharing personal data collected via UAS for any purpose that is not specified in the UAS data collection policy. [11]]** **[3(e) If publicly disclosing 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 undertaken a reasonable effort to obfuscate or de-identify personal data – unless the**

9 **[CDT "Notes": Note this Best Practice still allows for intentional collection of personal data if that is the purpose of UAS use. However, note also that under the Best Practice in [reference to CDT provision (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.]**

10 **[CDT "Notes": Note that the phrase "knowingly collects or retains" does not obligate operators to proactively review collected data in search of personal data. This Best Practice applies only when the UAS operator knows that unrelated personal data were collected.]**

11 **[CDT "Notes": Note that in the notes to [reference to CDT provision (2)(a)], those purposes can include collection for future business purposes that are unforeseen at the time of collection.]**

	data subjects provide informed prior consent to the disclosure. [12]**]**
[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(f) Commercial UAS operators should make a reasonable effort to avoid using or sharing personal data 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.]**
[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 related to loss of life, serious injury, property destruction or theft, or exploitation of minors, or 5) if the data subjects provide informed prior consent.**]**	Same as CDT section 3(i) except CDT subclause 4 uses "evidence of" rather than "related to"
[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(a) Where practicable, if an individual requests that a UAS operator correct, destroy, obfuscate, or de-identify personal data about the individual, and retention of the 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.]** [13] **[4(b) Opportunities for individuals to participate in data management are described in [listing of various provisions of the CDT document: (2)(b), (2)(c), (2)(d), (2)(e),(3)(c), (3)(e), (3)(f), (3)(i), and (6)(a)].]**

[12] **[CDT "Notes": Google Street View is a good example of this in practice – the images are publicly available but individuals and license plates are blurred. Some agriculture UAS companies use geofencing to "trim" imagery from outside the geofence, thereby focusing data collection on a particular piece of property.]**

[13] **[CDT "Notes": 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.]**

[4. SECURE PERSONAL OR PRIVATE DATA]

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

For example, Commercial UAS operators should consider taking the following actions to secure **[**personal or private data**]**:

- **[CDT: Commercial UAS operators should 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.]** [14]

- **[CDT: Commercial UAS operators should make a reasonable effort to regularly monitor systems for breach and data security risks.]**

- **[CDT: Commercial UAS operators should make a reasonable effort to provide security training to employees with access to personal data collected via UAS.]**

- **[CDT: Commercial UAS operators should make a reasonable effort to permit only authorized individuals to access personal data collected via delivery UAS.]**

- **[CDT: Commercial UAS operators should make a reasonable effort to encrypt or hash retained personal data that have not been publicly disclosed.]**

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. [15]

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

5(a) UAS operators should ensure compliance with evolving applicable laws and regulations and UAS operators' own privacy and security policies through appropriate internal processes.

---

[14] **[CDT "Notes": 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.]**

[15] **[CDT: 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.