## **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:

- <u>o</u> 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 defacto 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.

DRAFT	<u>10/20/</u> 15 Deleted:
<ul> <li>Privacy and transparency best practices for 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 are not provide the set Pra</li></ul>	
to data collected via the company's website.	Deleted: 24
	Deleted: unmanned aircraft systems (
<ul> <li>UAS operators should comply with all applicable laws and regulations. Best practices are intended to <u>complement</u> legislations.</li> </ul>	egal Deleted: )
compliance.	Deleted: best
<ul> <li>These UAS Best Practices are informed by the Fair Information Practice Principles (FIPPs). The FIPPs are incorpor</li> </ul>	Deleted: practices
<ul> <li><u>I hese</u> UAS <u>Best Practices are</u> informed by the Fair Information Practice Principles (FIPPs). <u>The FIPPs</u> are incorpor several privacy laws and standards in the US and <u>throughout the world</u>, such as the Privacy Act, the European Unic</li> </ul>	
Data Protection Directive, and FAA requirements for UAS test sites. The FIPPs are <sup>2</sup>	Deleted: practices
<ol> <li>Transparency,</li> <li>Purpose Specification,</li> </ol>	Deleted: encourage positive conduct beyond
3) Data Minimization,	Deleted: best
4) Use Limitation,	Formatted: Font: Not Italic
5) Individual Participation,	Deleted: practices
6) Security,	Deleted: should be
<ul><li>7) Accountability and Auditing,</li><li>8) Data Quality and Integrity.</li></ul>	Deleted: These widely accepted principles
<ul> <li>These UAS Best Practices are not meant to apply to activities protected by the First Amendment to the United State Constitution.</li> </ul>	Deleted: throughout the world, EU
<ul> <li>Nothing in these Best Practices should be construed to impede the use of UAS for purposes of emergency response including safety and rescue responses.</li> </ul>	<u>e.</u>
<ul> <li>Nothing in these Best Practices should take precedent over the safe operation of a UAS.</li> </ul>	
Definitions:	<b>Comment [AAA1]:</b> The best practices document loses utility when it is not clearly

"Sensitive data" means:

<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.

Center for Democracy & Technology

2

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

linked to an individual.

limited to

patterns are privacy invasive - only when

**Deleted:** should include, but are not

DRAFT,	15	Deleted:
<ul> <li>Data that, in the judgment of the UAS operator, are potentially sensitive,</li> </ul>	$\sim$	Deleted: ¶
<ul> <li>Imagery of an individual's face that is linked or easily linkable to an identifiable person,</li> </ul>		09
<ul> <li>Voice recordings that are linked or easily linkable to an identifiable person,</li> </ul>		Deleted: 24
<ul> <li>An individual's travel or location patterns that are linked or easily linkable to an identifiable person,</li> </ul>		Deleted: unique
Vehicle license plate numbers,		
Unique biometric data, and		
<ul> <li>Unique device signals information, such as a MAC address.</li> </ul>		
Other data that personally identifies, individuals.		Deleted: <del>y</del>
<ul> <li>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.</li> </ul>		
<ul> <li><u>"UAS Operator" means a person who uses UAS to collect sensitive data of data subjects.</u></li> </ul>		Formatted: No underline
• The terms "reasonable" and "reasonable effort" are used frequently in these Best Practices. What qualifies as "reasonable		Deleted: best
should depend largely on the circumstances of the UAS operator, as well as on the sensitivity of data collected and degree		Deleted: practices
of privacy risk associated with a particular UAS operation. For example, mapping of sparsely populated areas likely has le		Deleted: resources and
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	*	Deleted: high altitude
entities with similar UAS operations may be reasonable.	/	Deleted: UAS
		Deleted: is
<ul> <li>The term "data subjects" refers to the individuals about whom sensitive data is collected or retained.</li> </ul>		Deleted: , but the term also
		Deleted: s
<ul> <li>"Incidental collection" refers to data collection that is not intentional but which may occur as a byproduct of UAS operation.</li> </ul>	$\langle \rangle \rangle$	Deleted: an
For example, UAS portrait photography would be <i>intentional</i> collection of sensitive data, whereas a UAS used for	$\langle \rangle$	Deleted: is
architectural <u>or agricultural</u> inspection that happens to capture footage of the face of a passerby would be <i>incidental</i> collection.	\	Deleted: too weak may be un
		Deleted: information
<u> → Best practices should be a living document, updated as appropriate over time. </u>		<b>Comment [AAA2]:</b> Since there is no mechanism to update this document, suggest removing this bullet point.
<sup>3</sup> Consistent with the President's Feb. 2015 memorandum, which calls for best practices for "the commercial and private sectors."		removing this bullet point.

Center for Democracy & Technology

חר	A 1	_
DR	At	- 1

<u>10/20</u>/15 Deleted: **Deleted: ¶** 09 ence to ars shes ners hom to ifies provide of ecificity on and e strued JAS will ould be 4

				$\langle \rangle$	09
	PRINCIPLE 1	APPLICATION	NOTES		Deleted: 24
	TRANSPARENCY	(1)(a) When practicable, UAS operators should make a reasonable effort to place call numbers	(1)(a) When the technology is cost effective, should operators enable long-range identification of UAS,		<b>Comment [AAA3]:</b> We have not commented on the "Notes" section.
	reasonable efforts to provide transparency for	or other identification on UAS that would allow a person to determine whom to contact about the UAS.	such as through a beacon, MAC address, or LED signage?		<b>Comment [AAA4]:</b> Deleted the referent a UAS crash, which needlessly raises fears about the performance of UAS.
_	the collection and use of data.	(1)(b) When practicable, UAS operators should make a reasonable effort to provide prior notice to individuals of the general timeframe that they	<ul> <li>(1)(b) What qualifies as a reasonable effort to provide prior notice will depend on operators' circumstances.</li> <li>For example, delivery UAS operators may provide customers with an estimated time of delivery. Realtor</li> </ul>		<b>Deleted:</b> For example, if a UAS crash on private property, the property owne should be capable of determining who contact about the UAS.
ļ		may anticipate a UAS <u>intentionally</u> collecting sensitive data.	UAS operators may provide a home seller (and possibly immediate neighbors) with prior notice of the estimated date of UAS photography of the property.		<b>Comment [AAA5]:</b> This addition clarifie that UAS operators should not have to pr prior notice of the incidental collection of data, which will be difficult to predict.
		(1)(c) If a commercial UAS operator anticipates that UAS use may result in incidental or	Hobbyist UAS operators may notify nearby individuals of UAS flight in the vicinity.		Deleted: specify
		intentional collection of sensitive data, the	or OAS hight in the vicinity.	/	Deleted: The
		operator should create a UAS data collection	(1)(c) Two distinctions made here in referring to UAS		Deleted: T
		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	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		<b>Comment [AAA6]:</b> Removed the specifi in the previous language. Data retention de-identification practices are fluid. The previous language could have been const as requiring specific timelines for data deletion practices.
		data UAS will collect; (3) information regarding data retention and de-identification practices;	example, delivery UAS, but exclude other commercial UAS uses, such as agriculture. It depends on the		Deleted: When data collected via UAS be
		(4) examples of the types of entities with whom	operator's circumstances.		Deleted: deleted
		data collected via UAS will be shared; (5) a		_///	Deleted: or
		mechanism for complaints or concerns. The	(1)(c) A UAS data collection policy and a company's	$///_{r}$	Deleted: ed
I		UAS data collection policy should be made	general privacy policy need not be independent	$\langle     \rangle$	Deleted: W
		publicly available online <u>or made available</u> <u>upon request</u> .	documents or systems.		<b>Comment [AAA7]:</b> The disclosure shou about the types of entities, not specific parties.
		1(d) The Transparency Principle shall not apply to a UAS operator that collects data about a		$\setminus$	Deleted: A
I	l				Deleted: point of contact
					· · · · · · · · · · · · · · · · · · ·

Center for Democracy & Technology

DRAFT		<u>10/20</u> /15	Ļ	Deleted:
	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.			Deleted: ¶ 09 Deleted: 24
	<u>1(e) The Transparency Principle does apply to</u> <u>a UAS operator that assigns transparency</u> <u>responsibilities to a third-party by contract or</u> <u>other agreement.</u>			

PRINCIPLE 2       APPLICATION       NOTES         PURPOSE SPECIFICATION – Specifying how collected data will be used no later than at the time of       (2)(a) Commercial operators that anticipate (2)(a) Commercial operators that anticipate 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.       (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.       Deleted: 10 Deleted: 10 De	DRAFT.		_10/20/15	5	Deleted:
PRINCIPLE 2     APPLICATION     NOTES       PURPOSE SPECIFICATION     (2)(a) Commercial operators that anticipate intentional collection of sensitive data should make a - Specifying how collected and the UAS is collecting sensitive data in the UAS data collection policy no later than at the time of collection.     (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.     Deleted: Incidental or       Deleted: Incidental collection.     Collection policy no later than at the time of collection.     Collection policy no later than at the time of collection.     Collection policy no later than at the time of collection.     Collection policy no later than at the time of collection are not be able to predict all future uses of data collection.     Collection policy no later than at the time of collection or privacy, but under which incidental collection of sensitive data in public places; (2) Missions that may result in desirable economic or societal benefits.     Deleted: compelling       (2)(b) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant is a contract.     Collect the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant is a contract.     Collect and able to expectation of privacy.       (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant is a contract.     Collect sensitive data single individual swell as for massment of a single individual swell as for widespread, pervasive monitoring of many individuals.     Commert [AAAB]: suggest adding this contract exeption, au UAS					
PURPOSE SPECIFICATION = Specifying how collected data will be used no later than at the time of collection. = Specifying how collection policy no later than at the time of collection later than at the time of collection. = Specifying how collection policy no later than at the time of collection later than at the time of collection. = Specifying how collection policy no later than at the time of collection later than at the time of collection. = Specifying how collection. = Specifying how collection policy no later than at the time of collection has been be origicated in the UAS data collection policy no later than at the time of collection collection. = Specified in the UAS data collection policy no later than at the time of collection collection. = Specified in the UAS data collection policy no later than at the time of collection collection. = Specified in the UAS operators may not be able to predict all future uses of data. = Specified in the data subjects br 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. <sup>4</sup> = (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subject has an expectation of privacy. <sup>4</sup> = (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subject has an expectation of privacy. <sup>4</sup> = (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects programant to a contract, UAS operators should avoid using UAS for the specific purpose of intervise or consent of the data subjects programant to a contract, UAS operators should avoid using UAS for the specific purpose of nersistent and continuous collection of sensitive data, about specific individuals, consent tervise, or consent of the data subjects programant to a contract. = Specific individuals, = Specified individuals, = Specified in the UAS operators should be allowed		ΔΡΡΙ ΙΩΔΤΙΩΝ	NOTES		"
SPECIFICATION       intentional collection of sensitive data should make a reasonable effort to specify the purposes for which collected at will be used no later than at the time of collection.       vary based on operator goals. The point is that reasonable effort to specify the purposes for which due to Xs is collecting <u>sensitive</u> data in the UAS data collection policy no later than at the time of collection.       Deleted: incidental or         Item tan 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) Note that this best practice excludes (1) Missions that involve intentional collection of sensitive data in public places; (2) Missions to to a contract. UAS operator should avoid using UAS for the specific purpose of intentionally collecting sensitive data subjects or pursuant knowledge that the data subjects or pursuant to a contract. UAS operator he data subjects or pursuant knowledge that the data subjects or pursuant is a difficult prove that an an expectation of privacy. <sup>4</sup> Deleted: incidental or         (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant knowledge that the data subjects or pursuant is a difficult prove that an individual set of widespread, pervasive monitoring of many individuals.       Deleted: informed consent.       Deleted: informed consent.         (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant knowledge that the data subjects or pursuant to a contract. UAS operators should avoid using UAS for the specific purpose of persistent and continuous			NOTES		Deleted: 24
SPECIFICATION       intentional collection of sensitive data should make a reasonable effort to specify the purposes for which collected at will be used no later than at the time of collection.       vary based on operator goals. The point is that reasonable effort to specify the purposes for which due to Xs is collecting <u>sensitive</u> data in the UAS data collection policy no later than at the time of collection.       Deleted: incidental or         Item tan 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) Note that this best practice excludes (1) Missions that involve intentional collection of sensitive data in public places; (2) Missions to to a contract. UAS operator should avoid using UAS for the specific purpose of intentionally collecting sensitive data subjects or pursuant knowledge that the data subjects or pursuant to a contract. UAS operator he data subjects or pursuant knowledge that the data subjects or pursuant is a difficult prove that an an expectation of privacy. <sup>4</sup> Deleted: incidental or         (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant knowledge that the data subjects or pursuant is a difficult prove that an individual set of widespread, pervasive monitoring of many individuals.       Deleted: informed consent.       Deleted: informed consent.         (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant knowledge that the data subjects or pursuant to a contract. UAS operators should avoid using UAS for the specific purpose of persistent and continuous	PURPOSE	(2)(a) Commercial operators that anticipate	(2)(a) The purposes of data collection and use will		
- Specifying how collected data with the UAS is collecting sensitive data in the UAS data collection policy no later than at the time of collection. These Best Practices do not intend to discourage unplanned or innovative data uses that may result in desirable economic or societal benefits. These purposes 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 intendinally collecting of privacy. 4 (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant knowledge that the data subjects or pursuant is of a contract. UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, the	SPECIFICATION			_	Deleted: incidental or
will be used no later than at the time of collection.       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.       exempt from this best practice.       Deleted: These purposes should be specified in the UAS data collection policy (2)(b) Note that this best practice excludes (1) Missions that involve intentional collection of sensitive data in public places; (2) Missions to are not specifically aimed at collection of privacy, but under which incidental collection of sensitive data where there is a reasonable expectation of privacy plus a compelling need or consent.       Deleted: compelling         Comment [AAAB]: suggest removing sensitive data where the operator has actual knowledge that the data subjects br pursuant to a contract.       Collect sensitive data where the operator has an expectation of privacy. <sup>4</sup> Collect sensitive data subject do do consent.         (2)(c) This is intended to discourage intentional use of UAS operators should avoid using UAS for the specific purpose of a legitimate need to do otherwise, or consent of the data subjects br pursuant to a contract.       Contract (UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data about specific individuals,       many individuals.       Deleted: informed as well as for widespread, pervasive monitoring of many individuals.         Deleted: three is Deleted: three is Deleted: three is       Deleted: individual be allowed to rely on contractual promises and representations.	<ul> <li>Specifying how</li> </ul>	reasonable effort to specify the purposes for which			
will be used no later than at the time of collection.       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.       exempt from this best practice.       Deleted: These purposes should be specified in the UAS data collection policy (2)(b) Note that this best practice excludes (1) Missions that involve intentional collection of sensitive data in public places; (2) Missions to are not specifically aimed at collection of privacy, but under which incidental collection of sensitive data where there is a reasonable expectation of privacy plus a compelling need or consent.       Deleted: compelling         Comment [AAAB]: suggest removing sensitive data where the operator has actual knowledge that the data subjects br pursuant to a contract.       Collect sensitive data where the operator has an expectation of privacy. <sup>4</sup> Collect sensitive data subject do do consent.         (2)(c) This is intended to discourage intentional use of UAS operators should avoid using UAS for the specific purpose of a legitimate need to do otherwise, or consent of the data subjects br pursuant to a contract.       Contract (UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data about specific individuals,       many individuals.       Deleted: informed as well as for widespread, pervasive monitoring of many individuals.         Deleted: three is Deleted: three is Deleted: three is       Deleted: individual be allowed to rely on contractual promises and representations.	collected data	the UAS is collecting sensitive data in the UAS data	purposes. Note that noncommercial operators are		
time of collection.       may not be able to predict all future uses of data.       (2)(b) Note that this best practice excludes (1)       specified in the UAS data collection policy         Accordingly, the <i>Best Practices</i> do not intend to discourage unplanned or innovative data uses that may result in desirable economic or societal benefits.       (2)(b) Note that this best practice excludes (1)       Image: Specified in the UAS data collection policy         (2)(b) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant for the specific purpose of intentionally collecting sensitive data where the operator <u>has actual</u> (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 to a contract, UAS operators should avoid using UAS       Deleted: informed         (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       (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.       Deleted: informed         Deleted: inows       Deleted: inows         Deleted: inows       Deleted: inows         Deleted: inows       Deleted: inows	will be used no	<u>collection policy</u> no later than at the time of collection.	exempt from this best practice.		
<ul> <li>Intra individual solution prediction in the predictin the prediction in</li></ul>	later than at the	These Best Practices recognize that UAS operators			
discourage unplanned or innovative data uses that may result in desirable economic or societal benefits.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 ofDeleted: compelling(2)(b) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant for the specific purpose of intentionally collecting sensitive data where the operator has actual knowledge that the data subject has an expectation of privacy.4collect sensitive data where there is a reasonable expectation of privacy plus a compelling need or consent.Deleted: compelling(2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant knowledge that 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,collect sensitive data in public places; (2) Missions that are not specific purpose of persistent and continuous collection of sensitive data subjects or pursuantdiscourage unplanned or innovative data uses that to a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data, about specific individuals,sensitive data in public places; (2) Missions that are not specific individuals,discourage unplanned or innovative data, about specific individuals,sensitive data is not persistent and continuous collection of sensitive data, about specific individuals,collect sensitive data in public places; (2) Missions to collection of sensitive data subjects or pursuant to a contract, UAS operato	time of				specified in the UAS data collection policy.
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 for the specific purpose of intentionally collecting sensitive data where the operator has actual knowledge that the data subject has an expectation of privacy. <sup>4</sup> Deleted: compelling(2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant (2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant (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,are not specifically aimed at collecting sensitive data where there is a reasonable expectation of privacy, but under which incidental collection of sensitive data where there is a reasonable expectation of privacy plus a compelling need or consent.Deleted: compelling(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)(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.Deleted: normed Comment [AAA9]: Suggest adding this contract exception, as UAS operators should be allowed to rely on contractual promises and representations.Deleted: there is Deleted: there is Deleted: there is Deleted: reasonable Deleted: compellingDeleted: reasona	collection.				
(2)(b) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant for the specific purpose of intentionally 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. Knowledge that the data subject has an expectation of privacy.4Deleted: compelling(2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant to a contract.(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.Deleted: compelling(2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant to a contract.(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.Deleted: informed(2)(c) In the specific purpose of persistent and continuous collection of sensitive data about specific individuals,Deleted: there is Deleted: there is Deleted: there is Deleted: there is Deleted: there is Deleted: there is Deleted: compelling					
<ul> <li>(2)(b) In the absence of a <u>legitimate need to do</u> 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 <u>has actual</u> knowledge that the data subject has an expectation of privacy.<sup>4</sup></li> <li>(2)(c) In the absence of a <u>legitimate need to do</u> otherwise, or consent of the data subjects <u>or pursuant</u> to a contract. UAS operators should avoid using UAS for the specific purpose of intentionally collecting sensitive data where the operator <u>has actual</u> knowledge that the data subject has an expectation of privacy.<sup>4</sup></li> <li>(2)(c) In the absence of a <u>legitimate need to do</u> otherwise, or consent of the data subjects <u>or pursuant</u> to a contract. UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive <u>data</u> about <u>specific</u> individuals,</li> <li>Deleted: compelling</li> <li>Deleted: compelling</li> <li>Deleted: compelling</li> <li>Deleted: informed</li> <li>Comment [AAAB]: Suggest adding this consent.</li> <li>Deleted: informed</li> <li>Comment [AAA9]: Suggest adding this contract exception, as UAS operators should as well as for widespread, pervasive monitoring of many individuals.</li> <li>Deleted: knows</li> <li>Deleted: knows</li> <li>Deleted: there is</li> <li>Deleted: reasonable</li> <li>Deleted: compelling</li> </ul>		may result in desirable economic or societal benefits.			
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.4Comment [AAA8]: suggest removing "informed" as it is difficult to prove that an individual was fully informed. Consent (whic may be implicit or explicit) should be sufficient.(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 (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)(c) This is intended to discourage intentional use of UAS for harassment of a single individual many individuals.Deleted: informedDeleted: informed to a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data, about specific individuals,many individuals.Deleted: there is Deleted: there is Deleted: reasonable Deleted: reasonable					
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.4collect sensitive data where there is a reasonable expectation of privacy plus a compelling need or consent."informed" as it is difficult to prove that an individual was fully informed. Consent (whic may be implicit operator has actual sufficient.knowledge that the data subject has an expectation of privacy.4(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.Deleted: informed(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,many individuals.Deleted: knowsDeleted: there is Deleted: there is Deleted: compellingDeleted: there is Deleted: compellingDeleted: compelling		(2)(b) In the absence of a <u>legitimate</u> need to do			Deleted: compelling
for the specific purpose of intentionally collecting sensitive data where the operator <u>has actual</u> knowledge that the data subject has an expectation of privacy. <sup>4</sup> (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 otherwise, or consent of the data subjects <u>or pursuant</u> to a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive <u>data</u> about <u>specific</u> individuals.		otherwise, or consent of the data subjects or pursuant			
<ul> <li>It the special purpose of intertionally concerning the expectation of privacy plus a competining need of consent.</li> <li>It is special purpose of intertional state and expectation of privacy plus a competining need of consent.</li> <li>It is special purpose of intertional state and expectation of privacy plus a competining need of consent.</li> <li>It is special purpose of intertional state and expectation of privacy plus a competining need of consent.</li> <li>It is special purpose of intertional state and expectation of privacy plus a competining need of consent.</li> <li>It is special purpose of privacy.<sup>4</sup></li> <li>(2)(c) In the absence of a legitimate need to do otherwise, or consent of the data subjects or pursuant many individuals.</li> <li>It is a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data about specific individuals,</li> <li>It is a contract, use of use of the data about specific individuals,</li> <li>It is a contract, use of use of the data about specific individuals,</li> <li>It is a contract, use of use of the data about specific individuals,</li> <li>It is a contract, use of the data about specific individuals,</li> <li>It is a contract, use of the data about specific individuals,</li> <li>It is a contract, use of the data about specific individuals,</li> <li>It is a contract, use of the data about specific individuals,</li> <li>It is a contract, use of the data about specific individuals,</li> <li>It is a contract, use of the data about specific individuals,</li> <li>It is a contract, use of the data about specific individuals,</li> <li>It is a contract, use of the data about specific individuals,</li> <li>It is a contract about the privacy of the data about specific individuals,</li> <li>It is a contract about the privacy of the</li></ul>					
knowledge that the data subject has an expectation of privacy. <sup>4</sup> (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.       Deleted: informed         (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)(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.       Deleted: informed         Deleted: there is       Deleted: there is         Deleted: reasonable       Deleted: reasonable					, , ,
of privacy. <sup>4</sup> (2)(c) In the absence of a <u>legitimate</u> need to do otherwise, or consent of the data subjects <u>or pursuant</u> to a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive <u>data</u> about <u>specific</u> individuals, (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. 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			consent.	- //	sufficient.
(2)(c) In the absence of a <u>legitimate</u> need to do otherwise, or consent of the data subjects <u>or pursuant</u> to a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive <u>data</u> about <u>specific</u> individuals. <b>Comment [AA9]</b> : suggest adding this contract exception, as UAS operators should be allowed to rely on contractual promises and representations. <b>Deleted:</b> there is <b>Deleted:</b> there is <b>Deleted:</b> reasonable <b>Deleted:</b> compelling			(2)(a) This is intended to discourage intentional		Deleted: informed
(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,       as well as for widespread, pervasive monitoring of many individuals.       Contract exception, as UAS operators should be allowed to rely on contractual promises and representations.         Deleted: knows       Deleted: knows         Deleted: there is       Deleted: reasonable         Deleted: compelling		or privacy.			Comment [AAA9]: Suggest adding this
otherwise, or consent of the data subjects or pursuant many individuals. to a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, Deleted: there is Deleted: reasonable Deleted: reasonable Deleted: compelling		(2)(c) In the absence of a legitimate need to do			
to a contract, UAS operators should avoid using UAS for the specific purpose of persistent and continuous collection of sensitive data, about specific individuals, Deleted: knows Deleted: there is Deleted: reasonable Deleted: compelling				-\    \	
for the specific purpose of persistent and continuous collection of sensitive data about specific individuals, Deleted: reasonable Deleted: compelling Deleted: compelling					
collection of sensitive <u>data</u> about <u>specific</u> individual <u>s</u> , Deleted: mere is Deleted: reasonable Deleted: compelling				-\\\ /	
Deleted: reasonable Deleted: compelling					
				<u> </u>	
Deleted: informed				I/	Deleted: compelling
				/ /	Deleted: informed

Center for Democracy & Technology

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

and representations.

Deleted: s

Deleted: information

<sup>&</sup>lt;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."

to that which is needed to achieve specified purposes. (3)(b) Where practicable, UAS operators should make a reasonable effort to minimize <u>UAS</u> operations <u>involving the</u> 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) <u>UAS</u> operators may inform data subjects of their sensitive data collection 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 operations of the proves of UAS use.					
PRINCIPLE 3         APPLICATION         NOTES         09           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 rom entering private property or airspace without prior consent of the property or appropriate authority. If the uAS operation will substantially interfere with the use and enjoyment of the property.         (3)(a) Where practicable, UAS operators should make a enjoyment of the property.         (3)(b) Where practicable, UAS operators should make a reasonable effort to minimize UAS operators may inform data subjects or pursuant to a contract without informed prior consent of the data subjects or pursuant to a contract without informed prior consent of the preporty owner or appropriate authority.         (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)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.         (3)(c) Note this best practice still allows for intentional collection of sens	DRAFT,		<u>10/20</u> /15	-	Deleted:
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 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 enjowment of the property.       (3)(a) Note that "private property or airspace" is undefined. 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.       Deleted: 24         Deleted: barring exceptional droumstances, such as a safety indefer consent of the property.       Comment [AAA11]: fi this draft is going airspace above private property. This best practice does not create a new right or boundary for private airspace.       Deleted: 24         Deleted: informed       Comment [AAA11]: fi this draft is going airspace above private property. This best practice does not create a new right or boundary for private airspace.       Deleted: 24         Deleted: informed       Comment [AAA11]: fi this draft is going include references on collection of sensitive data 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.       Comment [AAA12]: This suggestion mor doal a retention practices including in the previously referenced data collection oplicy. If it is not practicable to provide an exact retention period, because, for example, the retention period depends on legal hold requirements				$\backslash$	
DATA MINIMIZATION - Limiting collection and retention of sensitive data to that which is needed to achieve specified purposes.       (3)(a) Where practicable, LJAS operators should make a (3)(a) Where practicable, LJAS operators should make a (3)(a) Note that "private property or data from entering private property or airspace without prior sensitive data to that which is needed to achieve specified purposes.       (3)(a) Where practicable, LJAS operators should make a (3)(a) Where practicable, UAS operators should make a (3)(b) Where practicable, UAS operators should make a reasonable effort to minimize UAS operations, involving the collection of sensitive data in public airspace or private purposes.       Deleted: Barring exceptional airspace without prior sonsent of the property owner or appropriate authority, if the UAS operators way inform data subjects of pursuant to a contract without informed prior consent of the data subjects of pursuant to a contract without informed prior consent of the property owner or appropriate authority.       Deleted: Barring exceptional airspace is undefined. This best practice consent of the property owner or appropriste authority.         (3)(b) Where practicable, UAS operators may inform data subjects of their sensitive data collection policy. If it is not practicable to provide an exact retention priod, because, for example, the retention period depends on legal hold requirements or evolving business operations, the UAS operator may explain that to data subjects       (3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.       (3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.	PRINCIPLE 3	APPLICATION	NOTES		
MINIMIZATION - Limiting collection and retention of sensitive data to that which is needed to achieve specified purposes.       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 enjoyment of the property.       airspace" is undefined. This best practice still contemplates flights over private property in public airspace. This is consent of the property.       circumstances, such as a safety incider or equipment malfunction, enjoyment of the property owner or appropriate authority, if the enjoyment of the property.       dircumstances, such as a safety incider or equipment malfunction, enjoyment of the property owner or appropriate authority, if the enjoyment of the property.       dircumstances, such as a safety incider or equipment malfunction, airspace above private property in public airspace bar property. This best practice does not create a new right or boundary for private airspace.       Deleted:       Comment [AAA11]: If this draft is going include references, we should airspace above private airspace.         purposes.       collection of sensitive data purposes.       in public airspace or pursuant to a contract without informed prior consent of the property owner or appropriate authority.       or boundary for private airspace.       Nonetheless, entering private rispace is since physical intrusion on private property is a privacy risk.         (3)(c) UAS operators may inform data subjects of their sensitive data collection policy. If it is not practicable to provide an exact 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 req					Deleted: 24
Immunity and the endination of the property on airspace without prior       and pace is difficulted. This to ver private         collection and       data from entering private property on airspace without prior       still contemplates flights over private         consent of the property owner or appropriate authority. If the       UAS operation will substantially interfere with the use and       property in public airspace. This is       consistent with current law - one owns an         a data with ch is       undefined but reasonable amount of       more quipment malfunction.       Comment (AAA11): If this draft is going         is the consent of the property.       (3)(b) Where practicable, UAS operators should make a       airspace above private property. This       best practice does not create a new right       or boundary for private airspace is         purposes.       collection of sensitive data subjects or pursuant to a contract       not private property owner or       not just an air traffic management issue       comment (AAA12): This suggestion more         given property in the absence of a legitimate need to do otherwise, or       not just an air traffic management issue       not private       property is a privacy risk.       (3)(b) As a general matter, it may not       property is a privacy risk.       (3)(c) Note this best practice still allows       (3)(c) Note this best practice still allows       (3)(c) Note this best practice still allows       for intention all collection of sensitive data       (3)(c) Note this best practice still allows       (3)(c) Not	DATA	(3)(a) Where practicable, UAS operators should make a	(3)(a) Note that "private property or		
<ul> <li>Limiting collection and retering private property or airspace without prior still contemplates flights over private consent of the property owner or appropriate authority, if the retention of sensitive data to that which is needed to achieve specified purposes.</li> <li>(3) (b) Where practicable, UAS operations involving the consent of the property in public airspace over private areasonable effort to minimize UAS operations involving the consent of the data subjects or pursuant to a contract without informed prior consent of the property owner or appropriate authority.</li> <li>(3) (c) UAS operators may inform data subjects of their sensitive data collection private, for example, the 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</li> </ul>	MINIMIZATION	reasonable effort to prevent UAS that are collecting sensitive	airspace" is undefined. This best practice		
Consent of the property in problem attraction will substantially interfere with the use and enjoyment of the property.property in public anspace. 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.Comment [AAA11]: if this draft is going include references taw we show include references taw we show include references to trepas law, we show include references to trepas law, we show include references to trepas law, we show include references on trepas law, we show include references on trepas law, we show include references on trepas law, we show include references to trepas law, we show include references to trepas law, we show include references on trepas law, we show include refe	<ul> <li>Limiting</li> </ul>	data from entering private property or airspace without prior	still contemplates flights over private		
<ul> <li>sensitive data to that which is needed to achieve specified purposes.</li> <li>(3)(b) Where practicable, UAS operators should make a 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.</li> <li>(3)(c) UAS operators may inform data subjects of their sensitive 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</li> </ul>	collection and	consent of the property owner or appropriate authority, if the	property in public airspace. This is		Deleted: informed
to that which is needed to achieve specified purposes. (3)(b) Where practicable, UAS operators should make a collection of sensitive data purposes. (3)(b) Where practicable, UAS operators should make a collection of sensitive data purposes. (3)(c) UAS operators may inform data subjects of their sensitive data retention practices including in the previously referenced data collection operator, the UAS operator may explain that to data subjects operations contexplain that to da	retention of	UAS operation will substantially interfere with the use and	consistent with current law - one owns an		
Indict without       (3)(b) Where practicable, UAS operators should make a achieve specified purposes.       (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       best practice does not creater an wright or boundary for private airspace. Nonetheless, entering private airspace is 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.       not just an air traffic management issue       Comment [AAA12]: This suggestion mor closely ties the provision to privacy concert of the 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       (3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.       (3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.	sensitive data	enjoyment of the property.	undefined but reasonable amount of		<b>Comment [AAA11]:</b> If this draft is going to
needed to       (3)(b) Where practicable, UAS operations involving the specified purposes.       best practice does not create a new right or boundary for private airspace.       Restatement (Second) of Torts, § 158.         purposes.       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 concent of the property owner or appropriate authority.       not just an air traffic management issue since physical intrusion on private property is a privacy risk.       Comment [AAA12]: This suggestion mor closely ties the provision to privacy concert by 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       (3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.	to that which is		airspace above private property. This		include references to trespass law, we should
achieve specified purposes.reasonable effort to minimize UAS operations involving the collection of sensitive data in public airspace over privateor boundary for private airspace. Nonetheless, entering private airspace is not just an air traffic management issueComment [AAA12]: This suggestion mor closely ties the provision to privacy concern the consent of the data subjects or pursuant to a contract without informed prior consent of the property owner or appropriate authority.or boundary for private airspace. Nonetheless, entering private airspace is not just an air traffic management issueComment [AAA12]: This suggestion mor closely ties the provison to privacy concern Deleted:(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(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.	needed to	(3)(b) Where practicable, UAS operators should make a			
purposes.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.not just an air traffic management issueclosely ties the provision to privacy concern Deleted:(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(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.	achieve		or boundary for private airspace.		Restatement (Second) of Toris, § 158.
the consent of the data subjects or pursuant to a contract without informed prior consent of the property owner or appropriate authority.since physical intrusion on private property is a privacy risk.Deleted:(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 subjectssince physical intrusion on private property is a privacy risk.Deleted:	specified	collection of sensitive data in public airspace over private	Nonetheless, entering private airspace is		Comment [AAA12]: This suggestion more
without informed prior consent of the property owner or appropriate authority.property is a privacy risk.(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 subjectsproperty is a privacy risk.(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.	purposes.	property in the absence of a legitimate need to do otherwise, or	not just an air traffic management issue		closely ties the provision to privacy concerns.
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       (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)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.			since physical intrusion on private		Deleted:
<ul> <li>(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</li> <li>(3)(b) As a general matter, it may not practicable for a high altitude UAS to obtain prior consent.</li> <li>(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.</li> </ul>		without informed prior consent of the property owner or	property is a privacy risk.		
<ul> <li>(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</li> <li>(3)(c) UAS operators may inform data subjects of their sensitive data if that is the purpose of UAS use.</li> </ul>		appropriate authority.			
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 subjectsobtain 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)(b) As a general matter, it may not		
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       (3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.			practicable for a high altitude UAS to		
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(3)(c) Note this best practice still allows for intentional collection of sensitive data if that is the purpose of UAS use.			obtain prior consent.		
depends on legal hold requirements or evolving business operations, the UAS operator may explain that to data subjectsfor intentional collection of sensitive dataif that is the purpose of UAS use.					
operations, the UAS operator may explain that to data subjects if that is the purpose of UAS use.					
		depends on legal hold requirements or evolving business	for intentional collection of sensitive data		
when disclosing its retention policies Where practicable UAS			if that is the purpose of UAS use.		
		when disclosing its retention policies. Where practicable, UAS			
operators should make a reasonable effort to avoid incidental or (3)(d) Note that the phrase "knowingly					
intentional collection or retention of sensitive data that are not collects or retains" does not obligate					
necessary to fulfill the purposes for which UAS is used – unless operators to affirmatively review data in					
the data subjects provide informed prior consent. search of sensitive data.		the data subjects provide informed prior consent.	search of sensitive data.		
(3)(d) If a UAS operator knowingly collects or retains sensitive (3)(e) Three years is the statute of					
data that are unnecessary to fulfill the purpose for which the limitations for trespass in CA and NY.					
UAS is used, the operator should make a reasonable effort to This figure is suggested to help operators					
destroy, obfuscate, or de-identify such sensitive data as guard against trespass claims.			guard against trespass claims.		
expeditiously as reasonably possible.		expeditiously as reasonably possible.			
	L		L		

Center for Democracy & Technology

DRAFT.		_10/20/1	5	Deleted:
	(3)(c) 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.			Deleted: ¶ 09 Deleted: 24
	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	(4)(a) Commercial UAS operators <u>commit to making reasonable and</u> <u>responsible use of sensitive data and may share that information as</u> <u>reasonable for those uses. Reasonable and responsible practices may</u> <u>vary over time as business practices and individual expectations evolve.</u>	(4)(b) Google Street View is a good example of this in practice – the images are publicly available but		
sensitive data or certain	should make a reasonable effort to avoid intentionally using or sharing sensitive data collected via UAS for any purpose that is not specified in	individuals and license plates are blurred. <sup>6</sup> Some agriculture		Formatted: Strikethrough
purposes.	the UAS data collection policy. (4)(b) Sensitive data collected without consent and not pursuant to a	UAS companies use geofencing to "trim" imagery from outside the geofence,		<b>Comment [AAA13]:</b> Limiting uses to pre- identified purposes could cut off innovation data uses that could produce economic or societal benefits.
	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 no necessary to fulfill the purpose for which the UAS is used, commercial	thereby focusing data collection on a particular piece of property.		
	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) A definition of "marketing purposes" – as distinct from public disclosure – may be helpful here. One		
	(4)(c) Commercial UAS operators should make a reasonable effort to avoid using or sharing sensitive data for <u>specific use in targeted</u> marketing	scenario to which people may object could be using sensitive g data collected via UAS to		
	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	supplement online advertising or junk mail without informed prior consent.		Deleted: purposes, unless the data subjects provide informed prior consen

<sup>&</sup>lt;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). Center for Democracy & Technology

DRAFT <mark>,</mark>		<u>,10</u> / <u>20</u> /15		Deleted:
	broader marketing campaigns nor are there restrictiosn on the use or sharing of reasonably de-identified sensitive data for marketing purposes.			Deleted: ¶ 09
				Deleted: 24
	(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. <sup>5</sup>			

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

Center for Democracy & Technology

DRAFT,		<u>,10/20</u> /15		Deleted:
PRINCIPLE 5	APPLICATION	NOTES	$\backslash$	Deleted: ¶ 09
		NOTES		Deleted: 24
INDIVIDUAL	(5)(a) Where practicable, UAS operators should offer data			
PARTICIPATION -	subjects reasonable means to review sensitive data and			
Facilitating informed	take reasonable measures to maintain the accuracy of			
and reasonable	such data. If an individual requests that a UAS operator			Formatted: Strikethrough
choices to data	destroy, obfuscate, or de-identify sensitive data about the			
subjects regarding	individual, and retention of the sensitive data is not			
the collection, use,	necessary to fulfill a purpose for which the UAS is used, the UAS operator should take reasonable steps to honor			
and retention of sensitive data.				
Sensitive data.	this request.			
	(5)(b) Opportunities for individuals to participate in data			Formatted: Strikethrough
	management are described in (2)(b), (3)(a), (3)(b), (3)(c),			
	(4)(b), (4)(c), and (4)(d) of these best practices.			

DRAFT <mark>,</mark>		<mark>,10/20/</mark> 15	-	Deleted:
		NOTEO		Deleted: ¶ 09
PRINCIPLE 6	APPLICATION	NOTES		Deleted: 24
SECURITY – Exercising reasonable efforts to secure collected and	(6)(a) Commercial UAS operators should <u>employ reasonable</u> 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	(6)(a) A security policy should include, at minimum, such basic steps as keeping software up to date and downloading security patches for known		Formatted: Strikethrough
retained data.	data collected and retained. <sup>7</sup>	vulnerabilities.		Formatted: Strikethrough
	<ul> <li>(6)(b) Commercial UAS operators should make a reasonable effort to regularly monitor systems for breach and data security risks.</li> <li>(6)(c) Commercial UAS operators should make a reasonable effort to provide security training to employees with access to sensitive data collected via UAS.</li> <li>(6)(d) Commercial UAS operators should make a reasonable effort to permit only authorized individuals to access sensitive data collected via delivery UAS.</li> <li>(6)(e) Commercial UAS operators should make a reasonable effort to encrypt or hash retained sensitive data that have not been publicly disclosed.</li> </ul>	Should best practices include cybersecurity of the UAS itself – such as defense against unauthorized operation of the UAS by third parties?		Formatted: Strikethrough

<sup>&</sup>lt;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/bankinforeg/interagencyguidelines.htm).

D	RAFT		<mark>,10/20/</mark> 15		Deleted:
I	PRINCIPLE 7	APPLICATION	NOTES	$\overline{\ }$	Deleted: ¶ 09
-	ACCOUNTABILITY – Establishing internal accountability controls to ensure compliance with privacy policies and laws.	<ul> <li>(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.</li> <li>(7)(b) Commercial UAS operators should identify individuals to oversee compliance with applicable laws and UAS privacy and security policies.</li> <li>(7)(c) Commercial UAS operators should make a reasonable effort</li> </ul>	<ul> <li>(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.</li> <li>(7)(c) Larger and more complex UAS operators may want to consider external review.</li> </ul>		Deleted: 24
		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.			Comment [AAA14]: 7(c) is covered by 7(b).
l					Formatted: Strikethrough

END