**NTIA Multistakeholder Process**

**Privacy, Transparency, and Accountability Regarding Commercial and Private Unmanned Aircraft Systems (UAS)**

**Revised September, 2015**

Priorities Identified by Stakeholders: Privacy, Transparency, and Accountability Issues that Could be Addressed by Best Practices for Commercial and Private UAS Operation

**Top Priorities Identified via email after August 3, 2015 Meeting**

* To address a core privacy concern, this process should establish best practices regarding the collection by UAS operators of identifiable images of individuals in places where there is a reasonable expectation of privacy.
* The transparency and accountability best practices developed in this proceeding should:
	+ Address issues regarding the posting of privacy policies on a commercial UAS operator’s website that describe the data collected, shared, and used in the operation of a commercial UAS.
	+ Consider whether analogous practices for private operation exist that would promote transparency and accountability, while acknowledging that this poses challenges.
	+ Leverage existing precedent in aviation and air navigation to promote transparency and accountability.
	+ Try to address the challenge of identifying commercial and private UAS that might be violating privacy, civil rights, and civil liberties.  In addition to being a privacy issue, this is also a security concern.
* Promote security of UAS payload links. Malicious privacy/civil rights/civil liberties violations can occur when UAS being employed in a responsible manner have their payload link “hacked.”  This can result in the UAS collecting data where it was not meant to or having the data stream intercepted and posted where it shouldn't be.
* Make distinctions between visual line of sight operations (when operators can be identified nearby) and operations when operators cannot be identified nearby.
* Consider a tiered structure of best practices.
* Promote training and education for an emerging industry, including educating operators as well as educating the public about the varied and positive uses of UAS, including newsgathering.
* Promote the freedom and ability of the press to gather news via UAS and inform the public.
* Consider how best practices might encourage good hobbyist/amateur behavior.
* Draw lessons from analogous technologies, including best practices for privacy and data security as applied to PII and/or sensitive data collected by UAS.
* Discuss property concerns (existing law/norms)
* Develop best practices that are not overly complex or burdensome.
* Develop best practices that contemplate and address privacy rights, but do not go too far so as to restrict UAS use to the extent that its use would only be permitted in only narrow circumstances.
* Ensure that best practices provide flexibility for UAS use depending on the setting and type of UAS use, and provide room for best practices to adapt to technological UAS advances.

**Priorities Identified at August 3, 2015 Meeting**

* Divide by use?
* Review current law
	+ Impact of Best Practice on law
	+ Impact of technology on law
	+ Focus on commercial/private sector
* Distinguish between spaces with varying expectations of privacy
	+ Caution on question of distinguishing space
* Identify owner of drone
* Outreach?
* Separating hobbyist vs commercial?
* Retention and sharing of information
	+ Rendering information non-identifiable
	+ Platform agnostic?
* Tracking benefits of UAS
* Crossover between public and private
* Property concerns
	+ Existing law/norms
* Training
	+ Commercial use
	+ Hobbyist use
	+ Safety
* FIPPs
* Physical privacy vs. Informational privacy
* Distinguishing private data vs. non-private data
* Privacy of operators
* Notice to participants and nonparticipants
* Identifiable vs. non-identifiable data
* Consumer expectations
* Operators, Manufacturers, other stakeholders/users of UAS
* Further adoption of Best Practices
* Other technologies for non-fliers that are implicated in best practices (geofencing)
* Remote identification of UAS
* Reporting requirements (e.g. in event of a crash)
* Interaction with privacy policies
* Sensor data that may be of particular concern
* Cross-reference to part 107
* First amendment/free speech rights
* Fixed wing vs. copter, practical differences
* Analogous technologies
* Visual line of sight
* Collection vs. use of data
* Effects on innovation of Best Practices
* Tiered structure of Best Practices
* Data security
* Cost benefit analysis
* Awareness of infancy of industry