**Introduction**

Rather than solely picking out specific use cases, we identified buckets into which use cases may fall based on the likelihood that they will impact privacy interests. In is important to note that this document recognizes that collection may serve valid purposes, and this is not an attempt to create “good” and “bad” buckets of drone usage. In meetings, we emphasized that there are incredibly positive uses of drones in each bucket.

**Personal Information**

One approach would be to use personally identifiable information. Another is to generally consider the broader range of sensitive data. Generally, collection of data is not considered bad, but we want to encourage operators to first consider what implications a flight may have. As such, the broader approach may raise questions and address more potential intrusions than the more narrow approach.

In determining if any use would have an impact on privacy, we imagine that information that implicates privacy would include (but is not limited to):

* Imagery of an individual’s face or private property (the latter could be sensitive but not personally identifiable),
* Voice recordings,
* An individual's travel patterns or location information (3 or more data points makes it personally identifiable),
* Vehicle license plate identifier,
* Unique biometric data,
* Unique device signals information, such as a MAC address,
* Identification numbers,
* Other data that, in isolation or in aggregate, can identify an individual.

**Fair Information Practices**

We discussed that Fair Information Practices could apply for each use case bucket, with different degrees of application based on what bucket a use falls into. For example, less transparency would be required for a use with no privacy implications than for a use with intentional privacy implications. There was not an agreement that this should be a basis. However, for reference, the Practices as they appear in the NSTIC document (and alterations in the Consumer Privacy Bill of Rights):

* Transparency
* Individual Participation (Individual Control)
* Purpose Specification (Respect for Context)
* Data Minimization (Focused Collection)
* Use Limitation (Responsible Use)
* Data Quality and Integrity (Access and Accuracy)
* Security
* Accountability and Auditing

**Use Case Buckets**

The bucket of a drone operation could change depending on what it is used for, including during a single drone flight. Examples listed refer to what the group members considered general practice, but not necessarily indicative of the bucket that use would always fall in.

* No collection
	+ Flight with relevant sensors turned off
	+ Controlled environment flights
* Limited collection
	+ Agriculture
	+ Forest health monitoring
	+ Fire fighting (structure and wildland)
	+ Land and environmental survey
	+ Weather monitoring
	+ Traffic monitoring (for pattern monitoring or studies, not ticketing or tracking)
	+ Wilderness studies and exploration
	+ Wildlife surveys
	+ Geological surveys and science
	+ Structural inspections (pipelines, electrical wiring, bridges, dams, roads, trails)
	+ Search and Rescue (incidental for others not the subject of the SAR, intentional for the subject)
	+ Aerial capture, eradication, and tagging of animals (ACETA) - future UAS mission.
	+ Avalanche risk mitigation (future UAS mission).
* Incidental collection (collection that is not intentional, but which may occur as a byproduct of UAS operation)
	+ Delivery
	+ Real Estate
	+ Mapping (dependent on location)
	+ Insurance
	+ Disaster Response
* Intentional Collection
	+ Private border monitoring
	+ Facility security operations
	+ Traffic tracking
	+ Public or private photography or filmography (including news gathering)
	+ Delivery (if recipient verification)
	+ Internet delivery vehicles
	+ Insurance appraisal
* Special circumstances regarding heightened needs or risks from collection
	+ In protest vicinity
	+ In an emergency (eg: disaster relief)
	+ When litigation is involved
	+ Near medical, educational, or religious facilities
	+ Where individuals have a reasonable expectation of privacy

**Further Considerations**

Special Press/First Amendment Considerations

* Not a complete removal of the considerations, but could be grounds to deviate from expressed standards at each level (at each of the three levels the individual’s privacy interest should be seen as greater than the prior level)

Case Studies - Specific Scenarios

* Drone travels to scene of car wreck for insurance purposes. How is the following PII data treated?
	+ PII collected in transit for navigation purposes
	+ PII of individuals involved with the collision
	+ PII of potential witnesses

Additional Issues Raised for Future Consideration:

* Specific language for private drone usage versus commercial drone usage?
	+ Each bucket should have a sliding scale that reflects the scope and sensitivity of the collected data (for example, a travel history may be more sensitive than a blurry photograph of an individual’s face)
* Addressing the issue of “stolen PII.” Many current UAS don’t possess secure and “hack-resistant” control and payload communications links. This presents two distinct vulnerabilities for privacy violations. In the first, a UAS control system could be “hacked” and flown where it would violate privacy statutes/regulations. In the second case, an unsecured payload communications link could be exploited to “steal” and possibly misuse incidental or intentional obtained PII (e.g. car wreck scenario above, stolen video posted online). A related issue is related to the security of UAS obtained data once it has been downloaded. Data has been collected from manned aircraft for decades across most of the use cases discussed above for decades, but there has been little consideration for securing this data (which likely contains the same incidental or intentional PII as UAS will capture). Protecting the anticipated huge increases in and high quality of data that UAS will provide requires a cultural change from how we have traditionally treated similar data collected from manned aircraft.