Letter from Privacy Groups to Participants in the NTIA Multi-Stakeholder Process on Unmanned Aircraft Systems

We are writing to comment upon the April 22 "combined draft" of "Voluntary Best Practices for UAS Privacy, Transparency, and Accountability." We recognize that the drafters of this document, which represent a subset of industry, privacy advocates, and other stakeholders, engaged in extensive negotiations to produce the proposed best practices. We thank these stakeholders to their time and effort in reaching consensus on several important points. Nevertheless, we believe that it falls short of representing *best* practices for UAS use.

Companies that want to tout compliance with "best practices" that have been endorsed by not only industry but privacy advocates and other stakeholders as well, need to make certain basic commitments. If they are unwilling to make those basic commitments to avoid practices that are at odds with widely accepted privacy principles, and often seen as unacceptable by the public, then they should not be able to claim the mantle of compliance with best practices.

We ask that the following changes be made to the combined draft to bring it in line with core principles of protecting privacy while operating UAS:

- **Framing.** In the "Introduction," the drafters take great care to detail the important ways in which UAS could positively impact individuals and the economy. However, the privacy impacts of UAS are expressed merely as "concerns." In order to accurately convey the risk to privacy that UAS pose, both in their ability to increase the breadth and depth of the personal information collected about individuals, this section should be made more balanced.
- **Applicability.** Section II should make it clear that these best practices are only intended to apply to commercial and private UAS operators. UAS use by governments, or companies acting pursuant to a contract with a government entity, carry unique privacy and constitutional concerns that are beyond the scope of these best practices.
- **Contracts**. Section II should be modified to require any UAS operator claiming compliance with these best practices to ensure that any subcontractors involved with the operation of UAS on their behalf also comply. Otherwise, the delegation of noncompliant behavior to a subcontractor becomes a gaping loophole in these best practices; requiring subcontractors to merely "consider these Best Practices" is not enough.
- **Meaningful consent.** Section III defines "consent" as encompassing both express and implied consent. While implied consent may make sense in certain circumstances, for most of the consent requirements in this document, only meaningful, written *express* consent should be adequate to permit the practices in question. The document should define consent as consisting of "meaningful, freely given, express permission," and only use "implied consent" in the limited circumstances where that lower standard is appropriate.
- **Covered data.** Section III's definition of "covered data" does not sufficiently protect data that implicates individuals' privacy. Specifically, the criteria should not be whether data is "likely to be linked," but whether it is "likely to be linkable" to an individual's name or other personally identifiable information, because for example that could refer to nothing more than the intentions of the collecting party at the time of collection—

intentions that could easily change. In addition, altered data should only be exempted if it is "permanently" altered.

- **Notice.** Section IV.1(a) allows drone operators to determine whether they should provide notice to data subjects before collecting private data. The initial clause "Where practicable" is redundant and should be struck. This provision already limits its requirement to "a reasonable effort" to provide prior notice.
- **Reasonable expectation of privacy.** Section IV.2(a) allows UAS operators to collect covered, private data without data subjects' consent. Companies wishing to claim compliance with best practices should commit to not using UAS to intentionally collect *any* data from a subject who has a reasonable expectation of privacy without express consent. Item 2(a) should be amended to read: "UAS operators should not use UAS to intentionally collect covered data where the data subject has a reasonable expectation of privacy or is in a private space, absent express, written consent." Further, because the term "reasonable expectation of privacy" has specific legal connotations, the section should include an explanation and some examples. For example: "People reasonably expect their actions will remain private in spaces like their backyards, homes, churches and doctor's offices. People also expect that their communications will not be intercepted by anyone beyond their intended recipients and that they will not be tracked over extended periods of time when they move about in public."
- **Continuous observation.** Section IV.2(b) allows UAS operators to conduct persistent and continuous surveillance of people without their consent—even in traditionally-protected private spaces like their homes. Continuous and persistent surveillance represents one of the most privacy invasive potential uses of UAS, and one that many Americans most fear drones will be used for. A best practices document should categorically reject such data collection absent express consent of each individual. Item 2(b) should be struck in its entirety and replaced with a provision indicating that companies "will not engage in persistent and continuous collection of data on individuals outside of specific special situations where express consent has been granted."
- **Private property.** Section IV.2(c) should begin with "UAS operators should make a reasonable effort," with the earlier portion of that sentence cut. The best practice is to make reasonable efforts to minimize operations over private property without permission. Allowing all such operations as long as they are consistent with any declared purpose would create a loophole that would swallow the rule.
- **Retention.** The words "reasonable effort" should be struck from Section IV.2(d). The best practice is to delete unneeded data. This provision should also be expanded to note that covered data that has been inadvertently collected outside the purposes for which the UAS was operated should also be deleted.
- **Special uses of data.** Section IV.3(a) could be read to allow a drone user to gather information without the consent of a subject and use that data for important life decisions concerning employment, health care and credit. In many cases, federal and state laws prohibit these uses of covered data and prohibit entities from contracting around these uses. Therefore, this section needs to be altered to: "UAS operators should not use covered data for the following purposes: employment eligibility, promotion, or retention; credit eligibility; or health care treatment eligibility other than subject to express consent or when expressly permitted by and subject to the requirements of a sector-specific regulatory framework.

- **Privacy policy.** Section IV.3(b) is unnecessarily weak and would allow UAS operators to violate the express terms of their privacy policies. It should be altered to read, "UAS operators should not use or share covered data for any purpose that is not included in their privacy policies covering UAS data."
- **Marketing.** Section IV.3(d) allows operators to share covered data with third parties for any purpose, including marketing. It should be altered to read, "UAS operators should not use covered data for marketing purposes or share covered data for any purpose without consent." (Provided that the definition of consent is altered as suggested above.)
- **Securing covered data.** Section IV.4 should be modified to require UAS operators engaged in commercial activity to "comply with widely recognized best practices for securing personal data." It should also note that state data breach laws will likely apply to data collected by UAS.
- **Appendix.** The Appendix, "Guidelines for Neighborly Drone Use," as currently drafted, is contrary to the overall purpose of the best practices document and should be eliminated. It contradicts specific best practices by allowing non-commercial UAS operators to violate privacy if they have a "very good reason" or are "polite and reasonable" and to retain "sensitive data on other people" as long as they somehow "secure it against theft." If not eliminated, the Appendix should be edited to be as strong as the best practices document, as amended above. It should also focus on providing additional context to UAS operators about privacy expectations, such as: "People reasonably expect their actions will remain private in spaces like their backyards, homes, churches and doctor's offices. People also expect that their communications will not be intercepted by anyone beyond their intended recipients and that they will not be tracked over extended periods of time when they move about in public."

The ACLU strongly urges this additional change:

- **First Amendment rights**. The provision in Section II stating that constitutional rights will not be diminished by the best practices should be further clarified to protect the First Amendment rights of non-commercial UAS operators. For example, the provision should be edited to say: "Nothing in these best practices shall be construed to limit or diminish freedoms guaranteed under the constitution, including but not limited to the First Amendment rights of non-commercial UAS operators."

We believe that unless these changes are made, this document will not represent "best practices" for the use of UAS. We urge the participants in this process to make these changes.

Signed,

Access Now
American Civil Liberties Union
Electronic Frontier Foundation