

April 20, 2015

Mr. Lawrence E. Strickling  
Assistant Secretary for Communications and Information  
National Telecommunications and Information Administration  
U.S. Department of Commerce  
1401 Constitution Avenue NW  
Washington, DC 20230

RE: Process for Developing Best Practices for Commercial and Private Use of Unmanned Aircraft Systems

Dear Assistant Secretary Strickling,

The Information Technology & Innovation Foundation (ITIF) is pleased to submit these comments in response to the National Telecommunications and Information Administration's (NTIA's) request for comment (RFC) on the multistakeholder process aimed at developing best privacy, transparency, and accountability practices for the commercial and private use of unmanned aircraft systems (UAS).<sup>1</sup> ITIF is a nonprofit, non-partisan, public policy think tank committed to articulating and advancing a pro-productivity, pro-innovation and pro-technology public policy agenda internationally, in Washington, and in the states. Through its research, policy proposals, and commentary, ITIF is working to advance and support public policies that boost innovation, e-transformation, and productivity.

In early 2015, Barack Obama issued a presidential memorandum tasking NTIA with establishing a multistakeholder engagement process to develop and communicate best practices for accountability, privacy, and transparency regarding the use—both commercial and private—of UAS in the National Airspace System (NAS).<sup>2</sup> The process is timely and important, as commercial UAS are expected to generate \$13.6 billion in

---

<sup>1</sup> "NTIA Seeks Comment on Process for Developing Best Practices for Commercial and Private Use of Unmanned Aircraft Systems," *National Telecommunications and Information Administrations*, March 4, 2015, <http://www.ntia.doc.gov/press-release/2015/ntia-seeks-comment-process-developing-best-practices-commercial-and-private-use-u>.

<sup>2</sup> Barack Obama, "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," *White House*, February 15, 2015, <https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua>.

economic value and 70,000 new jobs within the first three years of their integration into the NAS.<sup>3</sup> Creating a process at the outset to address privacy, transparency, and accountability concerns may help protect consumers and create more public acceptance of this technology. This process should embody a set of community-developed and community-led principles that are technology-neutral, flexible, and designed to promote innovation, transparency, and accountability, and to protect privacy.

While UAS will likely touch many different industries and applications—from farming to insurance to law enforcement—FAA regulations prohibit most commercial uses of the technology.<sup>4</sup> NTIA should recognize that there are inherent limitations to conducting a multistakeholder engagement in regulating a nascent industry since many future industry stakeholders may not yet exist or may be too small to fully participate at this stage. For example, imagine if a similar process about Internet privacy had been initiated in 1998: Now-defunct companies like Netscape Communications and Pets.com would have set policy without the insights of yet-to-be-formed companies such as Facebook and Twitter that have shaped the Internet economy. Similarly, because UAS are an emerging technology and the FAA restricts their commercial uses, many future stakeholders will likely not be part of this initial conversation. As UAS are integrated into the U.S. airspace, it is likely that more interested parties will emerge. Therefore, NTIA should make clear that any policy outcomes created by this process are intended to be provisional and to gradually evolve based on additional community input and industry changes.

ITIF will address many of the questions that NTIA raised in its RFC regarding the general nature of the stakeholder program, as well as privacy, transparency, and accountability issues related to UAS technology.

### **General Questions**

The RFC seeks information on a number of questions related to the general process of the UAS multi-stakeholder work group. ITIF looks forward to participating in the process and submits the following responses to NTIA's general questions.

---

<sup>3</sup> “The Economic Impact of Unmanned Aircraft Systems Integration in the United States,” *Association for Unmanned Vehicle Systems International*, March 2013, [https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New\\_Economic%20Report%202013%20Full.pdf](https://higherlogicdownload.s3.amazonaws.com/AUVSI/958c920a-7f9b-4ad2-9807-f9a4e95d1ef1/UploadedImages/New_Economic%20Report%202013%20Full.pdf).

<sup>4</sup> These prohibitions will remain in place until the FAA creates its commercial UAS rules. “Regulations will facilitate integration of small UAS into U.S. aviation system,” *Federal Aviation Administration*, February 14, 2015, [http://www.faa.gov/news/press\\_releases/news\\_story.cfm?newsId=18295&cid=TW299](http://www.faa.gov/news/press_releases/news_story.cfm?newsId=18295&cid=TW299).

*Would it be helpful to establish three working groups with one focusing on privacy, one on transparency, and one on accountability? Should such groups work in serial or parallel?*

This process should be conducted in a serial manner. If this process were conducted in parallel, NTIA would risk excluding from the process people who do not have the time to engage in multiple working groups.

*Would it be helpful for stakeholders to distinguish between micro, small, and large UAS platforms (e.g., UAS under 4.4 lbs., UAS between 4.4 lbs. and 55 lbs., and UAS over 55 lbs.)? Do smaller or larger platforms raise different issues for privacy, transparency, and accountability?*

Before attempting to differentiate these technologies, the multistakeholder working group should first identify a common set of principles that should apply to all UAS technologies. These principles would then serve as a springboard for addressing specific issues associated with different types of UAS even if the actual implementation of the principle varies. For example, if the working group identifies a need for labeling or other identification, the appropriate specifications for small versus micro-UAS may differ according to the space available for a physical label.

## **Privacy**

New technologies often generate privacy concerns, especially if the public does not commonly use them or understand them.<sup>5</sup> Because UAS are still an emerging technology, privacy fears are likely to be heightened. Privacy is also highly subjective, so concerns will differ from one person to another.<sup>6</sup> More broadly, NTIA should not create rules that try to solve problems that have yet to arise. With this in mind, ITIF submits the following responses to NTIA's questions regarding privacy concerns for UAS.

*UAS can be used for a wide variety of commercial and private purposes, including aerial photography, package delivery, farm management, and the provision of Internet service. Do some UAS-enabled commercial services raise unique or heightened privacy issues as compared to non-UAS platforms that provide the same services? For example, does UAS-based aerial photography raise unique or heightened privacy issues compared to manned aerial photography? Does UAS-based Internet service raise unique or heightened privacy issues compared to wireline or ground-based wireless Internet service?*

---

<sup>5</sup> Adam Thierer, "Technopanics, Threat Inflation, and the Danger of an Information Technology Precautionary Principle," *Mercatus Center*, January 25, 2013, <http://mercatus.org/publication/technopanics-threat-inflation-and-danger-information-technology-precautionary-principle>.

<sup>6</sup> Alan Westin, "Social and Political Dimensions of Privacy," *Journal of Social Issues*, Vol. 59 No. 2, 2003, <http://www.privacysummersymposium.com/reading/westin.pdf>.

Most, if not all of the privacy concerns associated with UAS are not unique to the technology. NTIA should not attempt to create any UAS-specific rules that would put them at a disadvantage compared to other technologies. For example, standards for UAS-based photography should be no different than those for manned aircraft or satellites. By endorsing technology-neutral standards, the NTIA can create a level playing field for innovation.<sup>7</sup>

*Which commercial and private uses of UAS raise the most pressing privacy challenges?*

Many of the privacy implications of UAS technology are already made illegal by laws or rules currently on the books. For example, stalking laws prevent UAS operators from following others around without their permission and to their emotional detriment.<sup>8</sup> NTIA should not have the working group focus on problems already addressed by other legislative or regulatory efforts.

NTIA should also ensure that this conversation does not focus exclusively on commercial use of UAS technology. The goal of this multistakeholder working group should be to develop guidelines that interweave both the commercial and personal use of UAS. Included in this discussion should be a conversation about the extent to which drone operators, especially individuals, should be able to operate anonymously and privately. In addition, this conversation should include a discussion about the conditions, if any, under which law enforcement should be allowed to seize control of UAS remotely.

## **Transparency**

NTIA should approach transparency requirements cautiously because heavy-handed transparency practices could reduce privacy. Indeed, a certain level of transparency is essential to promoting safety, for both commercial applications of UAS technology and personal use. With the right balance, NTIA can use transparency requirements to support safety through information sharing and disclosures of accidents, while supporting the privacy of individual users. To that end, ITIF submits the following responses to NTIA's questions regarding transparency and the use of UAS technology.

---

<sup>7</sup> For additional information on technology neutral rules for UAS technologies, see Robert Atkinson, Daniel Castro, and Alan McQuinn, "ITIF Comments on the FAA's Small Unmanned Aircraft Systems Rulemaking," *Information Technology and Innovation Foundation*, April 20, 2015, <http://www2.itif.org/2015-comments-faa-unmanned-aircraft-systems.pdf>.

<sup>8</sup> Ryan Gallagher, "New Report Warns That Drones Could Be Used for Stalking, Voyeurism," *Slate*, February 1, 2013, [http://www.slate.com/blogs/future\\_tense/2013/02/01/drones\\_could\\_be\\_used\\_for\\_stalking\\_voyeurism\\_says\\_congressional\\_research.html](http://www.slate.com/blogs/future_tense/2013/02/01/drones_could_be_used_for_stalking_voyeurism_says_congressional_research.html).

*Transparent UAS operation can include identifying the entities that operate particular UAS, the purposes of UAS flights, and the data practices associated with UAS operations. Is there other information that UAS operators should make public?*

Transparency for UAS should be similar to transparency for manned flight systems, taking into account differences in the technology. For example, if other small aircraft operators are required to produce specific information, such as their data practices, then UAS operators should do the same. However, where there are differences in technology, NTIA should establish sensible rules that allow similar levels of transparency across all technologies. For example, it obviously does not make sense to require unmanned aircraft to disclose their passenger lists (since there are none).

*What values can be supported by transparency of commercial and private UAS operation? Can transparency enhance privacy, encourage reporting of nuisances caused by UAS flights, or help combat unsafe UAS flying? Can transparency support other values?*

NTIA should approach transparency requirements delicately. To go overboard with transparency or identification requirements could actually intrude upon the privacy of UAS operators. For example, stakeholders may decide that hobbyists should be able to fly their drones anonymously (or pseudo-anonymously). In this case, the working group may still recommend an identification system, but one where the personally identifiable information is only released under certain conditions, such as an accident.

*How can companies and individuals best provide notice to the public regarding where a particular entity or individual operates UAS in the NAS?*

UAS operators should not be required to post “flight plans” in advance of their operations. Posting this information in advance would be cumbersome for both commercial operators and hobbyists. In addition, excessive transparency requirements could result in unintended consequences, such as increased theft. (Imagine the privacy and security considerations if all Ferrari owners had to disclose where they were going to be driving their cars.)

*What mechanisms can facilitate identification of commercial and private UAS by the public? Would standardized physical markings aid in identifying UAS when the aircraft are mobile or stationary? Can UAS be equipped with electronic identifiers or other technology to facilitate identification of UAS by the public?*

NTIA should encourage the development of an interoperable system of electronic identifiers for UAS. Electronic identifiers may facilitate identification in the event of a crash or lost UAS, or help with

identification and avoidance by other aircraft. However, electronic identifiers may expose UAS to automated tracking and decrease privacy for some UAS operators. Again, the working group should consider both first-order and second-order effects of establishing electronic identifiers and design privacy into any system of identifiers from the outset.

*How can companies and individuals best keep the public informed about UAS operations that significantly impact privacy, anti-nuisance, or safety interests? Would routine reporting by large-scale UAS operators provide value to the public? What might such reporting include? How might it be made publicly available?*

NTIA should encourage commercial UAS operators to disclose their data-handling practices, safety ratings of their aircraft, and other pertinent UAS information to consumers as a best practice. Commercial UAS operators should also routinely disclose any government requests for data they have collected. NTIA should encourage individual UAS operators to follow the guidelines established by community organizations to avoid privacy, safety, or nuisance problems.

*What specific best practices would promote transparent UAS operation while supporting innovation?*

In particular, disclosures about safety could support innovation. For example, all operators should disclose if their UAS have crashed, if these aircraft have caused any damage or personal injury, and what caused the crash (e.g., human error, weather, animal strike, etc.). The purpose of these disclosures should be to ensure the cost of accidents is high (e.g., by increasing reputational damage), so that the free market punishes unsafe operators and favors safe ones, and policymakers have good data on which to make policy.

### **Accountability**

NTIA should adopt a self-regulatory framework that encourages the private sector and the hobbyist community to police themselves. ITIF submits the following responses to NTIA's questions regarding accountability for UAS technology.

*UAS operators can employ accountability mechanisms to help ensure that privacy protections and transparency policies are enforced within an organization. How can companies, model aircraft clubs, and UAS training programs ensure that oversight procedures for commercial and private UAS operation comply with relevant policies and best practices? Can audits, assessments, or reporting help promote accountability?*

Self-regulation of privacy practices may be a useful approach to police bad actors within the UAS industry. Businesses often provide the best oversight of their competitors and can refer violations of self-regulatory codes of conduct to regulators. A self-regulatory framework can promote efficiency, reduce information

asymmetry, and provide more flexibility than government regulations, while still protecting consumers and fostering innovation.<sup>9</sup>

### **Conclusions**

The integration of UAS into the national airspace holds the potential to usher in a new wave of innovation, allowing many different stakeholders to increase efficiency in a variety of sectors, including transportation, healthcare, law enforcement, telecommunications, energy, the creative arts, and agriculture. UAS technology could bring incredible benefits to the daily lives of U.S. citizens, including cheaper goods, innovative services, safer infrastructure, and greater economic activity. Furthermore, enthusiasts will be able to enjoy their hobby freely. NTIA will play a role by helping to establish norms and best practices for privacy, transparency, and accountability for the use of this technology. To achieve this future, any framework should be community-led, technology-neutral, and flexible, and it should not create unnecessary rules that stifle innovation.

Sincerely,

Robert D. Atkinson

President and Founder, The Information Technology and Innovation Foundation

Daniel Castro

Vice President, The Information Technology and Innovation Foundation

Alan McQuinn

Research Assistant, The Information Technology and Innovation Foundation

---

<sup>9</sup> Daniel Castro, “Benefits and limitations of Industry Self-Regulation for Online Behavioral Advertising,” *Information Technology and Innovation Foundation*, December 2011, <http://www.itif.org/files/2011-self-regulation-online-behavioral-advertising.pdf>.