April 20, 2015

National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Avenue NW, Room 4725
Washington, DC 20230

Re: UAS RFC 2015

Dear Mr. Verdi:

The Future of Privacy Forum (FPF) is a think tank seeking to advance responsible data practices and is supported by leaders in business, academia and consumer advocacy.[1] FPF thanks the National Telecommunications and Information Administration (NTIA) for providing this opportunity to comment on its process for developing best practices around commercial and private use of unmanned aircraft systems (UAS).

FPF supports NTIA's continued efforts to facilitate the development and advancement of responsible data practices through multistakeholder processes (MSP). The domestic use of drones has been the subject of considerable public debate,[2] and the development of best practices around unmanned aerial vehicles (UAV) and emerging UAS technologies may help to alleviate concerns about the privacy implications of these systems and the technologies drones can carry.[3]

[1] The views herein do not necessarily reflect those of the Advisory Board or supporters of the Future of Privacy Forum.
[2] *E.g.*, Associated Press, *Americans Remain Skeptical of Drones, New Poll Finds* (Dec. 19, 2014), http://www.theguardian.com/world/2014/dec/19/poll-america-drones;
Aaron Smith, *U.S. Views of Technology and the Future*, Pew Research Center (Apr. 17, 2014), http://www.pewinternet.org/2014/04/17/us-views-of-technology-and-the-future/.
[3] Sandy Johnson, *Balancing Privacy, Jobs in the Domestic Drone Debate*, USA Today (Apr. 11, 2014), http://www.usatoday.com/story/news/nation/2014/04/11/stateline-privacy-jobs-drones/7590409/.

We are excited by efforts from industry to proactively work to protect consumers' privacy, and we look forward to participating in the NTIA MSP.

I. General

First, we urge the NTIA to set a clear timetable for developing UAS best practices as part of the MSP, and FPF recommends that this timetable be accelerated in order for best practices to be most effective in guiding both the future development of UAS technologies and their ultimate use. As the Federal Aviation Administration's (FAA) Notice of Proposed Rulemaking states, UAS technologies are rapidly evolving at this very moment,[4] and establishing best practices for industry will provide an important foundation for protecting consumer privacy. Recognizing that this process will need to move quickly, FPF has the following suggestions for how the MSP should be structured and guided.

The NTIA's effort on the subject of drones is designed to be different than the previous multistakeholder processes on mobile apps and facial recognition. While those processes were designed to produce binding codes of conduct, this effort is aimed at developing best practices for an emerging technology that also is largely restricted by the FAA at present.[5] Participants will need to focus on high-level general principles that can guide current and future technological development. As a result, the MSP must be careful not to become overly focused on different UAS technologies, and instead, should remain focused on the broader policy issues raised by these technologies. We also believe the process should be mindful and thoughtful of developing approaches to UAS privacy issues around the globe, and that the NTIA should develop best practices that can promote the global interoperability of UAS technologies.

It will be important for the NTIA to establish clear expectations and goals for the MSP at the outset. Prior multistakeholders efforts have often been bogged down by lengthy debates over appropriate process and procedures,[6] leaving participants unclear as to how the group intends to resolve disputes and reach consensus. Additional clarity around the rules of engagement and the method in place for considering and resolving open issues would be welcome.[7] The NITA may also wish to develop a mechanism by which proposed and consensus positions of participants can be made public to facilitate a more transparent exchange of views among

---

[4] Fed. Aviation Administration, Notice of Proposed Rulemaking: Operation and Certification of Small Unmanned Aircraft Systems 36 (Feb. 15, 2015), http://www.faa.gov/regulations_policies/rulemaking/recently_published/media/2120-AJ60_NPRM_2-15-2015_joint_signature.pdf [hereinafter NPRM].

[5] Civil Operations (Non-Governmental) of UAS, Fed. Aviation Administration, https://www.faa.gov/uas/civil_operations/ (last updated Mar. 17, 2015).

[6] Robert Gellman, Three Bad Ideas in the Consumer Privacy Bill of Rights 1-2 (Mar. 5, 2015), http://bobgellman.com/rg-docs/rg-CPBR-1-4.pdf.

[7] *See* Omer Tene & J. Trevor Hughes, *The Promise and Shortcomings of Privacy Multistakeholder Policymaking: A Case Study*, 66 Maine L. Rev. 438 (2014) (describing challenges facing participants in the W3C's "Do Not Track" effort), http://mainelaw.maine.edu/wp-content/uploads/2014/05/Tene-Hughes.pdf.

participants. Further, the NTIA should clarify that the development of consensus best practices must not be understood to require unanimity among all participants.

With regards to the scope and structure of the group's work, FPF supports considering all sizes and types of UAS platforms together. The NTIA asks whether it would help to distinguish between micro, small, and large drones, but despite some obvious differences based on size, the major privacy issues around UAS platforms will depend upon functionality, such as a drone's payload or sensor capabilities. Participants should be encouraged to identify specific types of functionality or uses of information that present concerns, and at this early stage, best practices should be developed with an eye toward addressing all types of commercial drone applications, independent of platform size.

The NTIA should explore how existing Fair Information Practice Principles (FIPPs) can apply to an aerial platform that can carry a diverse array of payloads, with different sensor arrays and data-collection capabilities. We specifically support the NTIA's suggestion that the group's work be focused on areas like transparency and accountability, as well as privacy more broadly. This structure helpfully echoes the policies and procedures discussed in the government use of UAS in a recent Executive Order. This Executive Order, otherwise termed a Presidential Memorandum on "Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems," could serve as a model for developing privacy best practices around commercial drone use.[8] The Executive Order directs the federal government to develop and follow certain requirements in the use of data gathered by drones, and we believe these principles should inform the work of the NTIA on this subject.

Taking these issues in turn, we would encourage the NTIA to specifically consider what best practices can promote privacy, transparency, and accountability around the uses of information that can be collected from UAS technologies. We also believe that these particular areas of focus can be tackled collectively by the MSP without the need for separate working groups.

II. Privacy

Developing best practices that support the beneficial uses of drones while addressing privacy concerns will be essential to the ultimate success of the MSP. Even as the public recognizes the value of using UAS for tasks such as inspecting oil platforms and bridges, there remains considerable skepticism among the public about the broad commercial use of drones.[9] One recent study, for example, has cautioned that UAS technology alters public perceptions about

[8] Presidential Memorandum: Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015), https://www.whitehouse.gov/the-press-office/2015/02/15/presidential-memorandum-promoting-economic-competitiveness-while-safegua.

[9] A recent poll by the Associated Press found that 43 percent of those surveyed opposed the commercial use of drones with only 21 percent expressing support. Associated Press, *supra* note 2.

any information collection, lowering support for activities that would otherwise be considered acceptable.[10] Drones have become a flashpoint for public concerns about privacy, even where their use presents limited privacy impact.

Responding to public perceptions about UAS technology has become a top priority for industry.[11] Trade associations such as the Association of Unmanned Vehicle Systems International (AUVSI) have already advanced general codes of conduct which stress the importance of respecting individual privacy,[12] and the Small UAV Coalition has expressed a commitment to proactively working to protect consumer privacy.[13] Several drone companies have also agreed to support a geofencing approach that allows individuals to limit where certain UAS platforms are allowed to fly.[14]

The White House Executive Order specifically addresses the need to consider data collection and use and data retention and dissemination policies. As we have argued previously, the best way to ensure that the economic benefits of drones are realized and the risks to individual privacy minimized will be to focus on how the data collected by UAS technologies are used.[15] The NTIA specifically asks whether UAS-based aerial photography or Internet service present different privacy concerns, but these uses do not capture some of the more novel applications of UAS technologies. The ultimate advantage and benefit of UAS technology will be via the capacity of different payloads to offer a simultaneous array of different audio-visual sensors, broadcasting equipment, and connective functionality. These include not only high-powered zoom lenses on cameras, but also advanced imaging capabilities, including night vision, infrared, ultraviolet, and thermal imaging; radar technologies; video analytics technologies; biometric recognition capabilities; and the ability to work in conjunction with our devices.[16]

---

[10] Visioncritical, Drone Awareness and Perceptions (Feb. 2, 2014), http://odesi1.scholarsportal.info/documentation/drones-survey/2014/Drone_Awareness_and_Perceptions.pdf. It is likely that much of this concern stems from the fact that drones are highly visible and salient to the public. As Professor Ryan Calo has observed, drones act a visual representation of the public's underlying concerns about privacy. Ryan Calo, *The Drone as Privacy Catalyst*, 64 STAN. L. REV. ONLINE 29 (2011), http://www.stanfordlawreview.org/online/drone-privacy-catalyst (Calo further notes that drones can make people "*feel* observed, regardless of how or whether the information was actually used.")

[11] Aerospace-Industries Association, Unmanned Aircraft Systems: Perceptions & Potential, http://www.aia-aerospace.org/assets/AIA_UAS_Report_small.pdf (last visited Apr. 1, 2015).

[12] Unmanned Aircraft System Operations Industry "Code of Conduct" (2012), *available at* http://www.auvsi.org/conduct.

[13] Press Release, Small UAV Coalition, The Small UAV Coalition Is Ready to Start Working with NTIA on Privacy Issues (Mar. 4, 2015), http://www.smalluavcoalition.org/wp-content/uploads/2015/03/Small-UAV-Coalition-NTIA-press-release-3-4_1095467402.pdf.

[14] No Fly Zone, https://www.noflyzone.org (last visited Apr. 1, 2015).

[15] Christopher Wolf & Jules Polonetsky, An Updated Privacy Paradigm for the Internet of Things (Nov. 19, 2013), *available at* http://www.futureofprivacy.org/wp-content/uploads/Wolf-and-Polonetsky-An-Updated-PrivacyParadigm-for-the-%E2%80%9CInternet-of-Things%E2%80%9D-11-19-2013.pdf.

[16] Office of the Privacy Commissioner of Canada, Drones in Canada (Mar. 2013), https://www.priv.gc.ca/information/research-recherche/2013/drones_201303_e.asp#heading-002-3; see also Thomas

Individually, these sensor capabilities will collect a lot of information, but particular privacy concerns will only arise depending upon sensor combination and use. For example, agricultural drones could collect vast quantities of data yet have minimal impact on consumer's privacy due to the way this information is used. Similarly, even sensors that capture sensitive information may have limited privacy impact if that UAS platform lacks the capability to record, or otherwise share that data. Further, a use-based approach to drone privacy considerations could also encourage industry to evaluate both retention and dissemination policies, which the Executive Order highlights as especially important.

Other countries have already begun to integrate commercial UAS into their national airspace, offering lessons for how industry can advance privacy measures domestically.[17] Several regulators have encouraged drone manufacturers to engage in privacy by design when developing new UAS platforms and technologies.[18] In addition to calling for privacy impact assessments with the use of drones, the European Data Protection Supervisor (EDPS) has also recently recommended that industry could (1) propose different categories of sensors that could be tailored to different commercial objectives, (2) establish data retention capabilities that allow users to schedule the deletion of data captured by a UAS platform, and (3) provide privacy-protecting tools and technologies to users, including the ability to turn on and off sensors in-flight and automatic masking where appropriate.[19] Existing practices abroad should inform the work of the MSP, and guidance from European as well as Canadian drone experts could be sought, as well.

Drones may be best understood as an aerial platform that will offer a wide-variety of different services. As a result, it will be important that these business models are deployed in ways that are not only considerate of privacy but take into account broader ethical concerns, as well. One potential suggestion is to encourage different industries that take advantage of UAS technologies to develop sector-specific policies around the use of data derived from different UAS platforms.[20]

Frey, *192 Future Uses for Flying Drones*, Futurist Speaker (Sep. 2, 2014), http://www.futuristspeaker.com/2014/09/192-future-uses-for-flying-drones/.

[17] For example, the European Aviation Safety Administration has advanced a set of progressive guidelines for UAS operation within the EU, and, moreover, the European Commission has expressed the opinion that the EU's existing regulations are "adequate to address the privacy, data protection, and ethical impacts" of drones.

[18] Opinion of the European Data Protection Supervisor (Nov. 26, 2014), https://secure.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2014/14-11-26_Opinion_RPAS_EN.pdf; Information and Privacy Commissioner, Ontario, Canada, Privacy and Drones: Unmanned Aerial Vehicles (Aug. 2012), https://www.privacybydesign.ca/content/uploads/2012/06/pbd-drones.pdf.

[19] Opinion of the European Data Protection Supervisor, *supra* note 18, at 15.

[20] For example, the Tow Center prepared a detailed report to guide how journalists deploy and use sensor data to uncover news. Sensors and Journalism (Fergus Pitt, ed. 2014), http://towcenter.org/wp-content/uploads/2014/05/Tow-Center-Sensors-and-Journalism.pdf.

Finally, a key issue to address in developing best practices will be to recognize existing rules around aircraft over individuals and their property. The FAA's NPRM attempts to address this, limiting the ability of UAS operators from flying directly over individuals.[21] However, the FAA's recent announcement of a new interim policy that provides blanket authorization for currently authorized commercial UAS operators to fly under 200 feet suggests both the commercial value of low-flying drones and the additional regulatory and administrative challenges that exist at such low heights.[22] Low-flying drones may hold some of the biggest commercial benefits of UAS technologies, but will also likely disrupt existing jurisprudence around individuals' airspace rights.[23]

Proposed solutions to this challenge range from dedicated drone "air highways,"[24] no fly zones,[25] and efforts by individual companies to restrict where drones may fly.[26] As mentioned above, one ambitious industry-led solution would allow individuals to not only limit where certain UAS platforms are allowed to fly but also offer customizable control over a homeowner's localized, immediate airspace.[27] Individual companies may also offer solutions that will aim to protect safety, as well as privacy. For example, DJI recently implemented a more extensive geofencing solution to control where its consumer drones can be used in response to a wayward Phantom drone that crashed onto the White House grounds.[28] Understanding how these technological efforts could interact with emerging best practices will be important.

III. Transparency

As we have argued previously, transparency will be an important element to ensuring public trust in the development of the Internet of Things and expanding uses of personal information.[29] More transparency around commercial uses of UAS will be essential to

---

[21] Fed. Aviation Administration, Overview of Small UAS Notice of Proposed Rulemaking (Feb. 2015), https://www.faa.gov/regulations_policies/rulemaking/media/021515_sUAS_Summary.pdf.

[22] Press Release, FAA Streamlines UAS COAs for Section 333, Fed. Aviation Administration (Mar. 27, 2015), http://www.faa.gov/news/updates/?newsId=82245&omniRss=news_updatesAoc&cid=101_N_U.

[23] Alissa M. Dolan & Richard M. Thompson II, Integration of Drones into Domestic Airspace: Selected Legal Issues, Cong. Research Serv. 6 (Apr. 4, 2013), http://fas.org/sgp/crs/natsec/R42940.pdf.

[24] Jason Koebler, *How NASA Plans to Open 'Air Highways' for Drones*, Motherboard (Sep. 9, 2014), http://motherboard.vice.com/read/how-nasa-plans-to-open-air-highways-for-drones.

[25] No Fly Zone, *supra* note 14.

[26] Frank Bi, Grounded: Drone Manufacturer DJI To Prevent Its Drones From Flying Over Washington D.C., Forbes (Jan. 28, 2015), http://www.forbes.com/sites/frankbi/2015/01/28/grounded-dji-to-prevent-drones-from-flying-in-washington-d-c/.

[27] No Fly Zone, *supra* note 14.

[28] Frank Bi, *supra* note 26.

[29] Wolf & Polonetsky, *supra* note 15; Christopher Wolf, Jules Polonetsky & Kelsey Finch, A Practical Privacy Paradigm for Wearables (Jan. 8, 2015), http://www.futureofprivacy.org/wp-content/uploads/FPF-principles-for-wearables-Jan-2015.pdf.

changing public perceptions about these technologies. The challenge will be determining what type of transparency is appropriate and feasible at present.

Commercial UAS use presents two transparency hurdles. First, in general, commercial users are likely to pursue broad company-specific uses of these technologies. While the NTIA should be cautious about establishing rigid transparency requirements, companies should be encouraged to explain clearly to consumers how personal information about them can be collected through commercial UAS use. Organizations may not be able to predict all of the ways in which this information may be used, but at minimum, they can provide details about the primary and secondary uses of information collected through UAS platforms. Amazon, for example, has been at the forefront of exploring the use of UAS to deliver packages directly to consumers, and the company has already built an online website that provides detail about the project and technology.[30] The NTIA should discuss and encourage other innovative ways to communicate company-specific practices with consumers.

Another component where transparency could alleviate public concerns about UAS use involves information about individual UAS operations. The NTIA should address the viability of identifying specific UAS operators and how this can be communicated with the public. Participants may be able to find common ground as to what sort of public documentation could be made available, which could include UAS flight scheduling and purpose and operator contact information. It could be helpful to see whether the documentation requirements that were required of FAA UAS Test Sites could provide a starting point for discussion.

A larger question that the FAA may need to consider is how to identify individual drones during operations. The FAA NPRM discusses the need for drones to display registration markings, though it recognizes the size of small UAS platforms may make these requirements unfeasible.[31] In the future, it is likely that the FAA will explore the viability real-time tracking tools to facilitate aviation safety, which could subsequently by broadcast to the public through web portals or mobile applications in a form comparable to existing flight tracking monitors.[32] This type of information, particularly if available in real-time, could serve as a robust transparency tool,[33] and the MSP should engage with the FAA to ensure such mechanisms will take privacy and transparency values into account.

In both instances, the NTIA could facilitate discussions about what categories of information should be communicated to consumers, and participants should be encouraged to consider innovative methods of providing transparency to consumers without placing a significant

[30] Amazon Prime Air, http://www.amazon.com/b?node=8037720011 (last visited Apr. 1, 2015).
[31] NPRM, *supra* note 4, at 128-130.
[32] *See, e.g.*, Flight Aware, http://flightaware.com/live/ (last visited Apr. 1, 2015).
[33] Rachel Finn, David Wright, Laura Jacques and Paul De Hert, Privacy, Data Protection and Ethical Risks in Civil RPAS Operations, Final Report for the European Commission 363 (Nov. 7, 2014), http://ec.europa.eu/DocsRoom/documents/7662 [hereinafter Trilateral Report].

burden on individual UAS operators. Drone manufacturers may have additional obligations. At a minimum, UAS manufacturers could incorporate privacy materials through packaging, documentation, or via a web link so UAS users could learn more about how to use drones in a way that respects individual privacy, in addition to basic safety literature.[34]

IV. Accountability

Finally, FPF recognizes the importance that rigorous accountability mechanisms can play in facilitating both responsible and privacy-considerate use of UAS technologies. Many of the organizations seeking to operate drones for commercial purposes have existing privacy programs in place, as well as the capacity and experience to conduct risk assessments, and it is likely that accountability lessons can be drawn from existing practice that could be easily applicable to commercial drone use. In many respects, public disclosures that promote transparency may also foster accountability through existing Section 5 enforcement by the Federal Trade Commission.

At the same time, addressing public concerns may require some dedicated privacy training as it relates to UAS operations. Increasingly, organizational privacy training has become a key component in protecting consumer privacy, and significant staff training in privacy was an important proposal put forward in the recent White House Consumer Privacy Bill of Rights.[35] The MSP should consider whether – and how – privacy training could be done in conjunction with the proposed safety training that the FAA will require of UAS operators.

One challenge will be to ensure that privacy training can be done both effectively and responsibly without imposing unnecessary burdens on operators and companies. It may also be necessary to distinguish between small UAS operations and companies with more extensive UAS programs. Larger organizations may be in a position to only hire operators who have completed both safety training as demonstrated an understanding of potential privacy risks and safeguards,[36] and smaller organizations may simply need guidance that could elaborate upon how privacy considerations should inform an operator's good judgment.[37] Privacy training and awareness could be incorporated into public education campaigns, such as the industry-led and FAA-supported "Know Before You Fly" campaign which aims to educate operators about the safe and responsible use of drones,[38] and the use of educational videos and point-of-sale materials that stress privacy issues and best practices should be encouraged.

Again, the NTIA should solicit input from both the experiences at existing FAA UAS Test Sites and commercial drone operations abroad.

---

[34] *Id.* at 345. At present, the Amazon Drone Store provides information to consumers about how to "learn more about flying responsibly." Similar privacy-oriented materials could also be provided.
[35] White House, Consumer Privacy Bill of Rights Act, Discussion Draft 13-14 (Feb. 2015), https://www.whitehouse.gov/sites/default/files/omb/legislative/letters/cpbr-act-of-2015-discussion-draft.pdf.
[36] Trilateral Report, *supra* note 33, at 345-46.
[37] *See* NPRM, *supra* note 4, at 27-29.
[38] Know Before You Fly, http://knowbeforeyoufly.org/ (last visited April 15, 2015).

Conclusion

There is much work to be done to determine how general privacy principles can be applied to diverse UAS technologies. Consumers, businesses, and policymakers must all have a voice in determining how commercial drones can and should take flight, and we believe the NTIA is well positioned to direct a fruitful dialog to develop best practices that promote privacy, transparency, and accountability. FPF urges the NTIA to move forward with a process that works to address specific uses and practices of concern involving UAS technologies. Many companies have already committed themselves to careful consideration of UAS privacy issues, and the MSP should work in conjunction with these efforts to identify procedures, policies, and potential technological tools to help industry address public concern and deploy UAS in a privacy-friendly manner.

We thank the NTIA for considering these comments.

Respectfully submitted,

Jules Polonetsky
Co-Chair and Director
Future of Privacy Forum

Joseph Jerome
Policy Counsel
Future of Privacy Forum