COMMENTS OF ACCESS

to

THE NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION

on

"Privacy, Transparency, and Accountability Regarding Commercial and Private Use of Unmanned Aircraft Systems"

Docket 150224183-5183-01

UASrfc2015@ntia.doc.gov

By notice published on March 5, 2015, the National Telecommunications and Information Administration ("NTIA") requested "comment[s] on privacy, transparency, and accountability issues regarding commercial and private use of unmanned aircraft systems (UAS)."[1] The notice follows from a presidential memorandum issued by President Barack Obama in February addressing the increased development and use of drones within the United States.[2] Among other things, the memorandum called for the present multistakeholder process for the creation of non-binding rules governing commercial drone use.[3] In its notice, the NTIA asked for respondents to focus on 16 specific questions, including general questions about drone policy, as well as questions focused on privacy, transparency, and accountability.

Access is an international human rights organization premised on the belief that political participation and the realization of human rights in the 21st century is increasingly dependent on access to the internet and other forms of technology.[4] Access seeks to defend and extend the digital rights of users at risk around the world. Today, Access urges the NTIA to adequately address threats to privacy and free expression posed by the public use of drone technology, particularly the unique challenges of drones as mobile internet service platforms.

These comments primarily respond to the following questions:

---

[1] Request for public comment, 80 Fed. Reg. 11978 (Mar. 5, 2015), *available at* http://www.ntia.doc.gov/files/ntia/publications/rfc_uas_privacy_03052015.pdf. For purpose of this comment, we refer to the so-called "UAS" as drones throughout, and encourage NTIA to do the same throughout its rulemaking process. In order to adequately involve the public as a stakeholder, it is important to use terms that the public understands and finds accessible. Nondescript acronyms will undermine public involvement and bias respondents toward government, companies, and a small number of civil society groups who understand the issue.

[2] Presidential Memorandum on Promoting Economic Competitiveness While Safeguarding Privacy, Civil Rights, and Civil Liberties in Domestic Use of Unmanned Aircraft Systems (Feb. 15, 2015), *available at* https://www.accessnow.org/page/-/2015uas%2Bmem2%2Brel.pdf.

[3] "Taming the skies: Obama memo looks at commercial drones, restricts government use," Access (Feb. 15, 2015) https://www.accessnow.org/blog/2015/02/15/taming-the-skies-obama-memo-looks-at-commercial-drones-restricts-government.

[4] About Access, Access, www.accessnow.org/about.

- "Do some [drone]-enabled commercial services raise unique or heightened privacy issues as compared to non-[drone] platforms that provide the same services?
- "Does [drone]-based Internet service raise unique or heightened privacy issues compared to wireline or ground-based wireless Internet service?
- "What values can be supported by transparency of commercial and privacy [drone] operation?"[5]

Drones provide great capacity to benefit both users and industry. However, drone technology is still new, and it will likely be utilized in ways we cannot imagine today. Access hopes that the process initiated by the Obama Administration will provide clear, lasting rules for drone use. This is particularly important for drones used as internet service platforms, both in a pseudo-permanent and temporary capacity, and the rules that these providers must abide by, including issues of network neutrality. By addressing hard questions now, we can provide for a path forward that allows for innovation without sacrificing user rights.

Using drones to provide internet service removes the biggest impediment to commercial involvement in the internet service provider market: investment in infrastructure. As such, drones (and other aerial vehicles) are sure to raise new and unique legal, technical, and practical issues. Questions of zero-rated services (which were not covered by the FCC's recent Open Internet Rules),[6] permanence of service, licensing, and interconnection should be addressed prior to the launch of drones to provide internet service. Additionally, never before has an internet service provider been able to connect the provision of service to a device that could also be used to conduct persistent and invasive physical surveillance using cameras and other sensors. It will be important to draw lines between how drones can be used in fair and open ways as to not unfairly impact users or infringe upon their rights.

Other issues raised by drones are not new, but will be amplified by the high number of unserved and underserved users who will relatively cheaply and easily accessible by drones. For example, questions of traffic monitoring by providers may be relevant in the wake of revelations that wireless telecommunications companies were using "supercookies" to track users across different websites and services.[7] The security of the technology deployed on drones to transit private user traffic also should be considered, as should law enforcement access to this data. Federal agencies, like the Federal Bureau of Investigation, as well as state and local police have continually demonstrated that they believe that sensitive

[5] *See*, request for public comment, *supra* fn 1.
[6] "Net Neutrality rules ban fast and slow lanes, but leave zero rating in place," Access (Mar. 12, 2015) https://www.accessnow.org/blog/2015/03/12/net-neutrality-rules-ban-fast-and-slow-lanes-but-leave-zero-rating-in-place.
[7] "Users Rally to Challenge Mobile Tracking," Access (Nov. 13, 2014) available at https://www.accessnow.org/blog/2014/11/13/users-rally-to-challenge-mobile-tracking-verizon

information, like location data, can be accessed with minimal legal protections.[8] These interpretations hurt users in a way that will be exacerbated by drones.

Finally, the use of drones to provide internet service in disaster relief and emergency response situations raises significant questions about the appropriate regulatory framework to apply to such providers. Such questions include whether to apply common carriage obligations per the recently-passed Open Internet Rules, which would require providers to provide non-discriminatory access to the open internet.

As drones are used to deliver internet access, transparency about operators, payloads, and service areas will help to mitigate negative repercussions for users.

Access thanks you for this opportunity to provide feedback. If you have any questions, you can contact Amie Stepanovich (amie@accessnow.org) or Drew Mitnick (drew@accessnow.org).[9] We look forward on continuing to engage throughout this process

Respectfully Submitted,

Amie Stepanovich
Access U.S. Policy Manager

Drew Mitnick
Access Policy Counsel

[8] *See, e.g.,* Baltimore Police say Stingray phone tracking use exceeds 25,000 instances (Apr. 20, 2015) http://www.baltimoresun.com/news/maryland/crime/blog/bs-md-ci-stingray-new-disclosures-20150420-story.html.

[9] Research by former Access interns Mohammad Alhinnawi and Brandon Moss contributed to the drafting of this comment.