Brendan Schulman c/o KLNF 1177 Avenue of the Americas New York, NY 10036 (212) 715-9247

Brendan100@Gmail.com

April 20, 2015

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

Attn: UAS RFC 2015

Via Email: UASrfc2015@ntia.doc.gov

Re:

Request for Comment Concerning National Telecommunications and Information Administration, U.S. Department of Commerce

Privacy, Transparency, and Accountability Regarding Commercial and

Private Use of Unmanned Aircraft Systems

RIN 0660-XC016

Dear Assistant Secretary Strickling,

I am an attorney in the field of civilian unmanned aircraft law, but write this comment in my personal capacity only. For over 20 years I have built and flown remotely-piloted model aircraft, now more commonly referred to as "drones" or unmanned aircraft systems ("UAS"), for recreational purposes. The following is my comment in response to the NTIA's Request for Comment.

Unmanned aircraft systems have the power to save lives, benefit the environment, achieve new economic efficiencies, and make the world a better place -- just as other modern technologies have throughout human history. Unfortunately, due to common misperceptions and misunderstandings, as well as a legacy of terminology used in military contexts, there appears to be great public concern about the impact on privacy of UAS technologies.

First, proper regard should be given to existing state law doctrines that already address many of the privacy-related concerns raised by lawmakers and members of the public. Physical intrusions that capture photography in inappropriate locations or to advance prurient interests are already largely addressed by state laws concerning stalking, unlawful surveillance, intrusion

upon seclusion, trespassing, "peeping," and similar civil and criminal provisions. Importantly, these legal provisions often have as elements of the crime a malicious or nefarious intent. Both the states and the federal government, via the NTIA or another agency, should adopt in the first instance a technology-neutral approach to understanding the issues. An invasion of privacy achieved by use of a tripod and zoom lens is just as offensive as one achieved by use of a drone, and likely already prohibited. Drone technology may not require any separate legislation or regulation, particularly if such legislation would inadvertently prohibit, chill or burden the many beneficial uses of the technology that do not pose privacy issues.

Second, it is important to understand what the actual problem, if any, is posed by UAS technology before devising purported legal or "best practices" solutions to those problems. Aerial imagery is not at all new. Airplanes have been flying for over a century. Satellites in Earth-orbit provide overhead imagery at high resolution that can be accessed publically, such as on Google Maps. Other service providers, like Bing Maps, provide even higher resolution aerial imagery captured by manned aircraft from a "Bird's Eye" view. Our Supreme Court has addressed the reasonable expectations of privacy from aerial photographs, in the context of the Fourth Amendment, finding that a person "could not reasonably have expected that his greenhouse was protected from public or official observation from a helicopter had it been flying within the navigable airspace for fixed-wing aircraft." *Florida v. Riley*, 488 U.S. 445, 450-51 (1989). The question for the multi-stakeholder process is whether and how a UAS operation differs from that of the routine operation of aircraft in the navigable airspace, many of which have long carried powerful cameras and other data-collection technology. Thus the focus should be on what differences, if any, render UAS technology subject to differing standards or use restrictions, based on:

- Operational location of the UAS in places where manned aircraft cannot fly or do not typically fly;
- Operational location of the UAS at altitudes below "navigable airspace" in places that raise actual privacy concerns;
- Operations that involve persistent surveillance as opposed to the more transient nature of manned aircraft operations; and
- Data security issues when the captured data involves personally identifiable information of non-consenting persons.

In many cases, commercial UAS operations simply do not raise any of these issues, because the subject matter of the UAS work is private infrastructure, such as a cellular telephone tower or a farmland, or images are collected from public vantage points. In such contexts, and many others, drones are simply industrial measurement and imaging tools. Their use does not require complicated regulatory or industry practices relating to transparency, accountability or privacy. On the contrary, imposing such elaborate requirements practices would burden innovation without much (if any) measurable benefit relating to privacy.

Many of the questions posed appear to presume that civilian UAS use always raises privacy issues warranting elaborate oversight or practices. For example, one of your questions asks,

"How can companies and individuals best provide notice to the public regarding where a particular entity or individual operates UAS in the NAS?" This presumes that notice to the public is of benefit or utility, as opposed to just a burden upon the operator (as well as a potential threat to competitiveness). In comparison, manned aircraft operators are not required to provide such notice, nor are the operators of other imaging and data-collecting devices.

As the Administration moves forward with the stakeholder process, I urge that we first establish the types of transparency, civil rights, or privacy concerns that are actually posed by this technology, so that the resulting framework is a measured response that does not impede innovation.

Respectfully,

Brendan Schulman