Before the
Federal Aviation Administration

The proposed rule requires UASs that are already subject to FAA registration requirements to transmit an identifier along with second-by-second data on the location and altitude of both the drone and the aircraftôs ground controller. The rule provides for two methods by which UASs would be required to identify themselves. The first would be over the Internet through a cellular telephone connection to one of a number of private third-party ñUAS Service Suppliersò (USS), which would collect such data and retain it for six months, to be supplied to the FAA or law enforcement upon request. The second would be by broadcasting such data over short-range public radio frequencies.[2]

In evaluating the consequences of such a tracking infrastructure for privacy, there are two existing paradigms to which we believe it could be fairly compared: automobile license plates, and manned aircraft registration numbers.

First, automobile license plates are a unique identifier, visible to all in the immediate vicinity of a vehicle but generally linkable to that vehicleôs owner only by law enforcement. License plates do not offer the government or others a broad view of vehicular movements across time and space (other than through the relatively new and highly controversial use of automatic license plate reader (ALPR) devices by police in some communities to record and persistently store vehicle location data, an activity that we and many other Americans regard as illegitimate and constitutionally suspect, and which we strenuously oppose[3]).

Second, like cars, manned aircraft are required to be registered with the government and are

1.

a fever pitch; such data is now very valuable and is being mined from every possible source. Without proper protections, it is predictable that aerial photography will become yet another such source.

Americans need the ability to know what ñeyes in the skyò are observing the streets, communities, and cities in which they live. The FAAôs remote ID system should be architected to allow them to do that.

2. **Government and corporate drones should not be exempted from identification requirements**

We do not want a world where individuals cannot launch a drone to carry out their own photography without being minutely monitored by centralized government actors, while government and corporate drones are able to carry out surveillance for their own purposes with their movements and identities shielded from public view. As the Electronic Privacy Information Center has proposed in their comments, individual use of drones should be subject to higher levels of protection (for example, their identities should be available only to the authorities, as with automobile license plates), while government and corporate UASs should be more transparent (for example, the identities of their owners, as well as other information about their operations such as their surveillance capabilities, should be available to ground observers in real time).[8] Itôs possible that corporate drone operators would try to game the system by, for example, hiring individuals to anonymously operate drones on their behalf. In structuring its regulations, the FAA should seek to forestall such possibilities.

Unfortunately, the Remote ID proposal appears to be oriented exclusively around the needs of law enforcement and national security agencies, with no acknowledgment that such a system can help protect the privacy of ordinary people by requring transparency (and thus the possibility of accountability) for privacy invasions accomplished through the use of drones. According to the proposal,

> The FAA believes that the remote identification requirement should be tied to the unmanned aircraft registration requirement because the FAA, national security agencies, and law enforcement agencies have a need to correlate remote identification and registration data.[9]

Private individuals operating UASs should enjoy no less privacy than corporate and government UAS operators ð indeed, because of the potential of drone usage by the government and the need for public oversight of that usage, they should enjoy more. If it becomes clear that there is a compelling need, the FAA could create a mechanism, subject to strict checks and balances, for certain law enforcement operations, narrowly confined in time and space, to be temporarily shielded from such transparency. But that should be the rare exception not the norm.

[8] Comments of the Electronic Privacy Information Center to the Federal Aviation Administration on Remote Identification of Unmanned Systems.
[9] Remote ID NPRM, 72460.

The proposal contemplates offering drone operators the opportunity to have a ñsession IDò (a randomly generated code assigned by the third-party USS) broadcast instead of their droneôs serial number.[10] This removes the serial number as a persistent identifier so that observers canôt track the activities of a particular drone across multiple flight sessions. But since that system will not shield individuals from tracking by the government (which will be able to see through the session IDs and access six monthsô worth of data on a particular operatorôs flights), it may end up doing little more than shielding corporate operators from public scrutiny. The FAA should make session IDs available for individual, but not commercial, operators. The distinction between commercial flights and non-commercial flights is already well-established in FAA regulation of UAS, which for a number of years prohibited commercial but not non-commercial flights without FAA permission.

The proposal states that ñany of the message elements that are broadcast directly from the unmanned aircraft could be received by commonly available consumer cellular phone, tablet, or other wireless device capable of receiving that broadcast.ò[11] That, we have been led to believe, along with the February 2020 publication of an ASTM standard for remote ID of UAS, suggests that the agency envisions allowing individuals to access real-time drone information on a smartphone or other device.[12] That is exactly the kind of transparency that individuals need when it comes that the overhead cameras of various kinds that will be peering down at them as they live their lives. But itôs important that individuals have the right information available to them on those devices.

3. No private parties should have special access to drone flight data

The proposal leaves major questions unanswered about the role that will be played by the USSs that the FAA seeS 7 th pro(b)-20(e)7(p)]TJETQ0.00000912 0 612 792 reW*nBT/F1 12 T -Fm0 gd

ID USS offer services.ò[15] Contractual agreements, of course, are not subject to public rulemaking and can be changed at any time and with uncertain transparency. Itôs also unclear if and how the FAA would ever enforce restrictions on the use of data by USS.

A database of six monthsô worth of every drone flight in the nation ð from children flying toys to big companies making deliveries to photojournalists at work ð is not something that private companies should have privileged access to. If the FAAôs remote ID infrastructure grants information access to any such companies, then it should also provide such access to the public.

Overall, it is damaging to privacy to insert private companies into the middle of a governmental infrastructure for the identification of UASs. If the FAA thinks that a Remote ID system is important for the United S Tm0 g1 0 0 BT/F1 1290000912 0 408.1lrtanc6(iyM.00oN7(s)-7(t)7(e)7( )-20(c)7(o)-

Conclusion