Before the
Federal Aviation Administration
Washington, D.C. 20590

In the Matter of	)	
	)	
Remote Identification of Unmanned Aircraft Systems	)	Docket No.: FAA-2019-1100; Notice No. 20-01
	)	
	)	

COMMENTS
OF
THE AMERICAN CIVIL LIBERTIES UNION ("ACLU")

Submitted: March 2, 2020

A system for the real-time identification of flights by drones or unmanned aerial systems (UASs), as proposed by the Federal Aviation Administration (FAA), implicates important privacy and free expression interests.[1] The ACLU supports such a system if it is done in a way that properly balances the different interests at stake.

For 100 years, the ACLU has been our nation's guardian of liberty, working in courts, legislatures, and communities to defend and preserve the individual rights and liberties that the Constitution and the laws of the United States guarantee everyone in this country. The ACLU takes up the toughest civil liberties cases and issues to defend all people from government abuse and overreach. With more than a million members, activists, and supporters, the ACLU is a nationwide organization that fights tirelessly in all 50 states, Puerto Rico, and Washington, D.C., for the principle that every individual's rights must be protected equally under the law, regardless of race, religion, gender, sexual orientation, disability, or national origin.

Unmanned Aerial Systems implicate a number of civil liberties interests, including the privacy of people on the ground, the privacy of drone users, and First Amendment interests in public photography. They can serve as both a means for people to carry out public photography, and a platform that allows people to be photographed and surveilled, whether through person-to-person spying, commercial surveillance, or government surveillance of various kinds.

[1] FAA, *Notice of Proposed Rulemaking: Remote Identification of Unmanned Aircraft Systems*, 84 Fed. Reg. at 72471 (Dec. 31, 2019), https://www.govinfo.gov/content/pkg/FR-2019-12-31/pdf/2019-28100.pdf.

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 aircraft's 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 "UAS Service Suppliers" (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 vehicle's 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 assigned a unique identification number ("N-number"). Unlike license plates, however, these ID numbers are communicated through radio transmissions rather than visually, and all such aircraft flying in certain classes of air space can be a) tracked through a nationwide bird's-eye view of the entire airspace and b) linked to their registered owner through a public database, the Civil Aviation Registry. (To protect privacy, the FAA does make it possible for manned aircraft to apply to obtain a temporary address not linked to the aviation registry, but known only to the FAA.[4])

The system proposed by the FAA resembles license plates in that a unique vehicle ID would be available to all, but the identity of the registrant behind that ID visible only to the authorities. It also resembles the manned aircraft registration system, however, in that nationwide location information would be collected in real time on all drone flights.

It is a significant step to impose such a comprehensive identification and tracking system on a technology that may become a routine part of daily life in American communities. We have four main comments on this system.

[2] Remote ID NPRM, 72440-42.
[3] See e.g., Catherine Crump, "You are Being Tracked: How License Plate Readers Are Being Used To Record Americans' Movements," American Civil Liberties Union, July 2013, https://www.aclu.org/files/assets/071613-aclu-alprreport-opt-v05.pdf.
[4] FAA web page, "ADS-B Privacy," https://www.faa.gov/nextgen/equipadsb/privacy/.

1. Remote ID can help protect privacy

We recognize the very real security concerns that drones raise, and understand why our nation's law enforcement and national security agencies as well as the FAA itself want a better method of identifying drones in order to deter certain illegal activity and to identify perpetrators it where it occurs. However, a remote ID system poses a substantial threat to the privacy of drone operators — especially those who rely on the special photographic vantage point that drone flights can provide to monitor law enforcement or other government actors — by removing the possibility of anonymous use.[5] At the same time, a remote ID system can help protect the privacy of those on the ground against aerial surveillance.

In our view, the privacy of the population on the ground is the more compelling interest given the balance of considerations, and a Remote ID system makes sense so long as any invasion of the privacy of drone operators is minimized.

The positive effects on privacy of a Remote ID system have the potential to be substantial, because drones are a very powerful surveillance platform, whether in government or private hands. They can enable intrusive spying by one citizen on another, for example through the windows of residences. They can enable the surveillance of private property, the surveillance of First Amendment protected activities such as protest marches, and even the persistent surveillance of entire cities.

Indeed, we are likely to see a law enforcement push for persistent or other significant aerial surveillance that will increase the importance of a Remote ID system that helps increase transparency over who is flying drones where, and when — including when those drones are controlled by federal, state, or local government actors. The police commissioner in Baltimore, for example, has proposed permanently reviving a formerly secret pilot program in which manned aircraft equipped with high-resolution cameras are deployed to continuously photograph the entire city, enabling the retroactive tracking of every visible vehicle and pedestrian within a 32 square mile area.[6] If this program is permitted to go forward, we can expect similar surveillance to be pushed in many American cities, eventually using drones.[7]

Even without such dramatically Orwellian aerial surveillance systems, it is likely that, if drone flights become commonplace over American communities for purposes such as deliveries, we will see efforts to leverage such flights to collect data about Americans and their lives. We are living in an era when the commercial exploitation of personal data about consumers has reached

[5] See e.g., Jack Gillum, "Ferguson no-fly zone aimed at media," Associated Press, Nov. 2, 2014, at https://apnews.com/674886091e344ffa95e92eb482e02be1/ap-exclusive-ferguson-no-fly-zone-aimed-media; ACLU letter to FAA on Ferguson no-fly zone, Nov. 4, 2014, at https://www.aclu.org/files/assets/aclu_letter_to_faa_11.4.14.pdf; ACLU letter to FAA on Standing Rock no-fly zone, Dec. 16, 2016, at https://www.aclu.org/sites/default/files/field_document/faa_letter_for_standing_rock_12.16.2016.pdf.

[6] Justin Fenton and Talia Richman, "Baltimore Police back pilot program for surveillance planes, reviving controversial program," *Baltimore Sun*, Dec. 20, 1919, at https://www.baltimoresun.com/news/crime/bs-md-ci-cr-baltimore-police-support-surveillance-plane-20191220-zfhd5ndtlbdurlj5xfr6xhoe2i-story.html.

[7] Arthur Holland Michel, *Eyes in the Sky: The Secret Rise of Gorgon Stare and How it Will Watch us All*. New York: Houghton Mifflin Harcourt, 2019.

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 "eyes in the sky" are observing the streets, communities, and cities in which they live. The FAA's 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] It's 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 — 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 "session ID" (a randomly generated code assigned by the third-party USS) broadcast instead of their drone's serial number.[10] This removes the serial number as a persistent identifier so that observers can't 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 months' worth of data on a particular operator's 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 "any 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."[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 it's 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 seeks to create. It does state that "The remote identification message elements that operators would be required to transmit to a Remote ID USS under this rule would be considered publicly accessible information."[13] That is promising, but it is unclear what information that USSs will collect that is not available to the general public. We do know that they will hold six months of data on their clients' flights, and that they will know the identity of every aircraft that is obfuscated for the rest of the world via the Session IDs that the USS issues. Would the USSs be permitted to make whatever use of such data that they wish (marketing, profiling, or anti-union activism for example)? Would they be permitted to share that data with whomever they wish (a tabloid reporter, for example)? While the FAA says it "expects" to include privacy protections in its agreements with the USS, the proposal does not contemplate any regulatory restrictions on the USSs other than a requirement that they retain the drone data that operators must send them for six months, and that they must make that data (stored or real-time) available to the FAA.[14] Rather, "the FAA intends to provide oversight of the Remote ID USS through contractual agreements and is therefore not proposing specific rules related to how the Remote

[10] Remote ID NPRM, 72442.
[11] Remote ID NPRM, 72485.
[12] ASTM International, "Standard Specification for Remote ID and Tracking," at https://www.astm.org/Standards/F3411.htm.
[13] Remote ID NPRM, 72485.
[14] Remote ID NPRM, 72484-85

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

A database of six months' worth of every drone flight in the nation — from children flying toys to big companies making deliveries to photojournalists at work — is not something that private companies should have privileged access to. If the FAA's 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 States to build in order to fully exploit the potential benefits of drone technology, then it should ask Congress for the funds to do what is necessary. It should not try to do it by outsourcing essential government functions to private companies that are then positioned to exploit their special nationwide access to data on Americans' use of an important new technology.

4. The network Remote ID infrastructure does not strike the right balance

Requiring every drone operator to buy a data plan with a cellular provider and connect to the Internet before their craft can lift off so that the government can access a nationwide bird's eye view of all active drones does not strike the right balance between the privacy and security purposes of remote UAS identification, and the privacy rights of drone users. The broadcast Remote ID should be sufficient to achieve both the security goal of allowing facilities to identify and deter illegal or hostile drone flights, and the goal of empowering individuals to know what aerial cameras may be recording them.Local, contemporaneous knowledge is enough.

Naturally, law enforcement will always cite scenarios in which having a network infrastructure could be useful, but the question is not whether such a system could ever be useful, it is how significant those benefits are and how they balance against the disadvantages of such a system.

Furthermore, the creation of bi-directional dataflows between drones in the field and a centralized entity (the USS) raises the specter of certain dangers associated with centralized control. It could be possible, for example, for a malicious USS to inject hostile code into any vulnerable client drone, enabling centralized control over those drones. This system of bi-directional data flow also raises the prospect that law enforcment and national security agencies might in the future push for certain lawful abilities to exercise centralized control over the nation's drones. That would represent a dangerous centralization of power that exceeds what any democratic government should be permitted to have. Creating an infrastructure that connects virtually every operating drone in the nation through the Internet to what may be a mere handful of centralized sources is a recipe for trouble.

[15] Remote ID NPRM, 72483.

Conclusion

The FAA has consistently resisted considering privacy a part of its mission.[16] But, by proposing an infrastructure for the identification and tracking of drones, the agency has irrevocably entered the realm of privacy policymaking. It has entered that realm by pursuing a vision in which low-flying drones serving a variety of functions are integrated into American daily life. By going beyond its traditional role in protecting the safety of aircraft to address the concerns of law enforcement — including concerns that, while legitimate, have nothing to do with aircraft crashes or collisions — so must the agency consider the centuries-old flip side of law enforcement power: the protection of privacy. There is no neutral ground on privacy here. In seeking the security benefits of remote ID the FAA can create an architecture that either creates the best privacy balance for individuals, or that creates a one-way mirror in which individual drone use is transparent while government and corporate operators are shielded from transparency as they carry out surveillance on individuals. The agency should do the former.

[16] Petition from EPIC, ACLU et al., to Michael P. Huerta, Acting Administrator, Federal Aviation Administration, Mar. 8, 2012, at https://epic.org/privacy/drones/FAA-553e-Petition-03-08-12.pdf.