Comments Regarding

FAA NPRM on Remote Identification of Unmanned Aerial Systems

Docket No.: FAA-2019-1100

I understand the need for remote identification and support reasonable measures to implement remote identification of small UAS. Remote ID can be implemented simply; however, the FAA has proposed a Rube Goldberg-like solution that is complex, costly and delivers an illusion of safety without stopping bad actors intent on causing mayhem.

The proposed rulemaking goes beyond what Congress authorized, appears to conflict with Federal and State laws, eliminates most indoor flights of small UAS, specifies an inappropriate (but fixable) use of FCC Part 15 communications, specifies a mostly infeasible use of Wi-Fi, has unrealistic views on Internet availability, and sets up a framework for a drone-based aerial surveillance network that creates a threat to national security. The proposal largely ends the R/C model aviation hobby, stifles innovation and U.S. competitiveness and imposes cost increases– while yielding little improvement in public safety.

My comments identify problems and propose solutions. Because this NPRM is large, with thousands of pages of supporting documents, and a short time frame to analyze and make comments, I address only some of the issues. Due to the volume of material and short comment period it is possible I have made errors of interpretation, of course.

Author's Background

I have a B.S. in computer science (senior thesis on air traffic control automation), a Master of Science in Software Engineering (thesis on Android smart phone power management) and an M.B.A. degree. I hold two U.S. patents (one in aviation and one in wireless communications), have written about a dozen books on tech subjects, and have had a career in the tech industry working in both software and wireless technology.

I am a model aviation hobbyist, an FAA Private Pilot Certificate holder (currently inactive), member of the Experimental Aircraft Association, member of the Academy of Model Aeronautics and the Field of Dreams RC Club.

Summary of Key Points and Recommendations

The NPRM eliminates most indoor flights of small UAS

The NPRM envisions that only Remote ID compliant craft will be sold. Remote ID compliant craft are unable to take off if they cannot receive a GPS signal. As a GPS signal is not receivable in most indoor locations, this de facto eliminates indoor flight of small UAS and implies the FAA is regulating the indoor airspace, over which it has no jurisdiction. This indoor flight restriction violates PL 115-254 Sec. 354. *Or maybe not* – comments on Page 8 and 22 of the NPRM suggest anyone can sell non-compliant drones by adding a “For indoor use only” sticker since the FAA cannot regulate indoor airspace nor the products on the shelf at Walmart. Which makes much of this NPRM moot.

FAA's Proposed Use of FCC Part 15 Spectrum Will Cause Interference and Crashes

The FAA proposes to use 47 CFR Part 15 of the FCC rules and regulations for transmission of Remote ID broadcast beacon signals and requires that transmitters "**must be designed to maximize the range at which the broadcast can be received**". The requirement to "maximize the range" mandates that small UAS transmit at the 4 w ERP level (1 watt spread spectrum, 6 db gain antenna) – from aircraft potentially located hundreds of feet in the air. This is not how Part 15 bands are intended to be used, will cause interference to residential consumer devices and licensed services, and may lead to receiver desense and loss of flight control signals, causing SUAS to crash, when multiple SUAS are flown in close proximity to each other. This problem is fixable.

The FAA Envisions Using Wi-Fi in a way that is Not Technically Feasible

The NPRM proposes using Wi-Fi, if available, to log flights with the Remote ID USS, particularly with a presumably lower cost Limited Remote ID system. Small UAS that use a flight control app on the smart phone are communicating with the SUAS craft using Wi-Fi. Currently existing small UAS implement a Wi-Fi Access Point (AP) on the aircraft and the phone and flight control app connect to this AP. The phone cannot simultaneously connect to a second AP that has Internet access; the phone can connect to only one AP at a time. *Thus, Wi-Fi cannot be used to provide a Remote ID USS connection*. The flight control app would have to log the flight over a smart phone Mobile Data connection. This means the concept of a low cost Limited Remote ID small UAS is unobtainable. The Limited Remote ID should be dropped and replaced with a broadcast beacon Remote ID for Visual Line of Sight (VLOS) and Internet-based Remote ID USS retained only for Beyond Visual Line of Sight operations (BVLOS). Related: Based on my own tests, the addition of a Remote ID USS data logging app, transmitting once per second, may reduce smart phone battery capacity by 10%. When combined with a smart phone-based flight control app, this may drain 40-50% of the battery in 30 minutes of flying.

The NPRM violates the Children's Online Privacy Protection Act (COPPA)

COPPA specifies protections regarding the collection of data related to children, including geolocation data and data from "toys and Internet of Things". An age restriction or permission from a parent or guardian to collect data does not resolve the problem. If a child flew a quad with or without permission, the parent or guardian is legally entitled to contact the data collector and ask to review, delete or suspend future data collection. The NPRM, however requires logged data be retained for at least six months – but COPPA applies to the Federal government and there is no exemption for the FAA. This is a problem for use of the Internet to log consumer product operator information to a Remote ID USS.

The NPRM violates the 4th Amendment

In the event a small UAS (SUAS) can receive a GPS signal indoors, when that SUAS is flown inside a home, it is required to log its activity in the Remote ID USS. The FAA is mandating the installation of a surveillance device inside a home, which lawyers tell me is not permitted by the 4th Amendment to the U.S. Constitution. Others suggest there may conflicts with the 5th Amendment, and the Foreign Intelligence Surveillance Act prohibition on collecting electronic signals of Americans.

The NPRM has an unrealistic view of Internet availability

The NPRM assumes most users have readily available Internet access via cellular service (or Wi-Fi, which is not feasible if low cost is a priority). In many areas of the U.S., cellular service is limited; about half of my state's land mass has no coverage from my cellular service provider. The NPRM appears to define "Internet is available" in a way that if another provider covers an area that my provider does not cover, then I am required to purchase service from that other provider. Taken to an extreme, one could require contracts with multiple service providers to meet the implied wording of the NPRM, or even mandate the use of expensive satellite-based Internet access. This implied requirement is spurious considering the FAA defines a Standard Remote ID capability to fly with a broadcast beacon Remote ID when no Internet is available, which is an additional argument for a broadcast beacon Remote ID only (for non BVLOS flights).

The NPRM Defines an Aerial Surveillance Network Using Remote ID USS

The NPRM says data sent to and collected by a Remote ID USS is not restricted to the basic message elements of operator and craft identification and location. The FAA specifically suggests a Remote ID USS could also collect **"a camera feed or telemetry data".** Some future Remote ID USS vendors have suggested a "free" business model; when the service is "free", private information is usually for sale. In effect, the NPRM is establishing a baseline for a national, real-time, aerial surveillance network having significant implications for personal privacy, safety, and violations of COPPA.

The NPRM Threatens National Security

In January 2020, the U.S. Department of the Interior grounded all of its foreign made drones over concerns that such drones could hypothetically conduct surveillance and transmit intelligence data over the Internet[1]. The US Army grounded its Chinese-made drones in 2017 over fears of their use for espionage[2]. While the left hand is citing threats to national security of Chinese-made drones, the right hand is simultaneously mandating all drones be connected to the Internet in real time, most of which will be made in China, and logging all kinds of data into Remote ID USS and other databases, for potential espionage use.

Is Privatization of Air Traffic Management Services Permitted?

Remote ID identifies a small UAS and also delivers air traffic management (air traffic control) services. If a Remote ID USS is not operating properly, the small UAS is not authorized to take off. If the Remote ID USS malfunctions during flight, the small UAS shall be landed as soon as possible. This is an air traffic control function. Additionally, the NPRM specifies that Remote ID USS location information collected will be used for air traffic control purposes. The FAA has defined small UAS as identical to "aircraft". Thus, a function of Remote ID USS is air traffic control. In 2017, Congress considered a law to establish a privatized, third-party run, fee-for-service air traffic control system but did not approve of this concept. If Congress said no to privatizing ATC, under what authority does the FAA set up a privatized ATC for UAS?

[1] https://dronedj.com/2020/01/29/interior-department-grounds-drone-fleet-with-new-order-issued-today/
[2] https://www.defenseone.com/technology/2017/08/us-army-just-ordered-soldiers-stop-using-drones-chinas-dji/139999/

Amateur Built Regulations Stifle Innovation

I have met EAA members who built newly designed aircraft, but test flew their designs as scale R/C models. There are several Youtube channels where hobbyists are creating innovative flying craft (for example, check out youtube.com/BPS.space and his "Sprite" electric ducted fan craft, currently test flown in his driveway). This NPRM would isolate testing at remote FRIAs, and eventually ban home designed and constructed aircraft. This NPRM is a threat to U.S. innovation.

Restrictions on Custom Built Model Aircraft Stifle Non-Aeronautical Research and Business

The restrictions imposed by this NPRM end the custom development of small UAS used in non-aeronautical research, such as agriculture, wildlife biology, forestry, geology and other areas. Including filmmaking. Custom built craft would be limited to FRIA sites – which is not the location where field research is undertaken. These small UAS will never be manufactured products - and very few can afford to meet the strict requirements – and time delays for approval - for manufacturing one-off products.

Software-based Enforcement Prevents Using U.S.-Sold Drones Outside the U.S.

The FAA believes it can contain alleged risks by using software to automatically control the operation of all small UAS – moving regulation from a trust and enforcement concept (as is done for all other laws) into enforcement by software. Side effects include the elimination of indoor flight, 4th Amendment and COPPA privacy violations, and that drones sold in the U.S., but operated outside the U.S., will likely not be able to fly due to Internet access limitations and that a Remote ID USS may not be available. Travelers from the U.S would have to purchase a drone, at their foreign destination, adding to compliance costs. And of course, they would bring those non-complaint drones back into the U.S.

Environmental Assessment Required

FAA Order 1050.1F, Paragraph 1.8 says "The FAA decision-making process must consider and disclose the potential impacts of a proposed action and its alternatives on the quality of the human environment." This NPRM eventually suspends the use of potentially millions of existing model aircraft, flight control transmitters and batteries, resulting in the likely short-term trashing of millions of pieces of electronics, with corresponding environmental impacts. This NPRM opens the low altitude skies to automated drone delivery fleets that have impacts on noise and quality of life. I was unable to locate an Environmental Assessment of these proposed rules.

The NPRM Bans Large Paper Airplanes Unless 14 CFR 1.1 is Modified

Through a quirk in the definitions of unmanned aircraft, and the requirements of this NPRM, the FAA bans the flight of hand launched paper airplanes and balsa wood airplanes except at FRIA model fields. While it is doubtful the FAA will enforce such a rule, this is a side effect of the proposed rules. This is fixable by a slight modification to the definitions used in 14 CFR 1.1.

Personal Impacts of this NPRM

As my existing fixed and rotor wing model aircraft would be suspended by this NPRM, I may have to trash perhaps $1,500 worth of aircraft and non-reusable accessories and flight controller

transmitters. Because of my long interest in aviation, and because of factors that may limit my access to flying manned aircraft again, I turned to model aviation. But because of uncertainty introduced by this NPRM, I have suspended further investment in R/C model aircraft. Additionally, this NPRM potentially eliminates a popular activity – indoor flight – at our city's annual Aviation Day event designed to interest youth in STEM subjects. This NPRM seems poised to close our nearly three decades old model airfield due to its proximity to an airport and the FAA's undefined "sensitive area" criteria for FRIAs.

General Recommendation

Consistent with privacy laws, threats to national security created by this NPRM, the requirement to allow indoor flights of small UAS, and that the FAA's envisioned use of Wi-Fi for Limited Remote ID is not technically feasible, the FAA should adopt the following instead:

- Use of Internet-based Remote ID USS for BVLOS only; all others optional.
- Use a broadcast-based beacon Remote ID for flights within visual range, based on Part 15 communications such as Wi-Fi and Bluetooth, which are readily receivable by smart phone apps, so that anyone can identify basic information.
- Drop the arbitrary 400-foot range restriction for Limited Remote ID SUAS - or just drop Limited ID concept all together and replace with broadcast beacons for all VLOS flight.
- The FAA must adopt a suitable power level for Part 15 beacons and abandon its mandate to "maximize range". Limit Part 15 Remote ID broadcasts to 100 mw (or +20 dBm) to avoid interference with other Part 15 devices and licensed users, and to avoid causing receiver desense that leads to crashes of SUAS.
- Use LAANC for authorization of R/C model aircraft flight instead of FRIAs.
- Accommodate indoor flight by permitting configuration of small UAS for flight without GPS – but have the SUAS broadcast operator/craft serial number Remote ID beacons..
- Aircraft flying BVLOS – such as automated drone fleets – could receive broadcast Remote ID transmissions from non-Internet connected craft and relay that information into Remote ID USS for the purpose of air traffic management (if desired). If there are no BVLOS drones in the area, this indicates drone traffic is light and that air traffic management services are not needed.
- Enable the addition of a broadcast based Remote ID module to existing small UAS, so that existing model aircraft do not need to be thrown away. This would be far better for the environment. This would support industry and researcher needs for custom made, one-off drones used in agriculture, wildlife and geology research and other areas, as would use of LAANC for authorization of other craft.
- Eliminate the Limited Remote ID Internet-connected concept as its use for low cost small UAS with low-cost Wi-Fi for Remote ID USS logging is infeasible. No one will make Limited Remote ID small UAS and no one will buy them. Replace Limited Remote ID with broadcast-based beacon IDs for VLOS flight.
- This proposal is similar to the European Union rules for small UAS Remote ID and creates a potential for a harmonized, global Remote ID solution. This means potentially lower costs due to greater production volumes, which leads to increased likelihood of compliance.

This recommendation meets the direction given by Congress, does not eliminate indoor flight, does not require the elimination of the model aviation hobby and the loss of business

opportunities, youth STEM programs and innovation. These methods can be implemented at modest cost, increasing the likelihood of compliance, and reducing the environmental impact of needlessly grounding (and eventually trashing) millions of existing electronic components.

The NPRM Eliminates Most Indoor Flight of Small UAS

The NPRM requires all small UAS to have Remote ID capability, except for recreational small UAS under 0.55 pounds. All small UAS operating under Part 107 rules, regardless of size, are required to have functioning Remote ID although technically, the FAA does not regulate the indoor airspace so that a Part 107 license is not required there.

The FAA's NPRM envisions all commercially sold small UAS will be compliant with the Remote ID rules.

Remote ID, as defined, requires transmission of latitude and longitude of the operator and/or the craft, in real time, during flight. The only known method to obtain reliable latitude and longitude is via GPS satellite signals. If a GPS signal is not available, small UAS with Remote ID are prevented from taking off.

No GPS signal means no flight, and this eliminates flight of small UAS in most indoor locations including most homes, businesses, convention halls, exhibit halls, movie studies, warehouses, manufacturing facilities, mines and caves.

From page 16 of the NPRM:

> "*The FAA envisions that upon full implementation of this rule, no unmanned aircraft weighing more than 0.55 pounds will be commercially available that is not either a standard remote identification UAS or a limited remote identification UAS."*

The FAA expects all commercially made craft > 0.55 pounds[3] to have functioning Remote ID. In effect, no commercially available products may be flown indoors; only home built and craft in existence prior to this rule, could fly indoors. (Or perhaps, using the page 8 definition, craft labeled "Indoor use only" will be sold?)

In email correspondence with the FAA Office of Rulemaking, the FAA concurs with this interpretation.

The FAA defines the remote ID requirements to include (Page 94):

> "These message elements would include: the UAS Identification (either the unmanned aircraft's serial number or session ID); **latitude, longitude**, and barometric pressure altitude **of both the control station and the unmanned aircraf**t; a time mark; and an emergency status code that would broadcast and transmit only when applicable."

[3] The 0.55-pound weight was determined in regard to safety of an SUAS falling out of the sky. The use of the 0.55-pound weight limit in the context of Remote ID appears arbitrary. Other nations have used other criteria, such as 900 grams, 2 kg, and so forth, in terms of registration and other requirements. Congress, in PL 115-254 Section 370 calls out the 2 kg level, referencing UA "under 4.4 pounds". This suggests that Congress envisioned Remote ID for craft under this weight level to be implemented in the simplest way possible. Section 370 also suggests that rules for BVLOS may be different than those for VLOS flight.

The requirements for latitude and longitude for both Standard and Limited remote ID are specified in a table on pages 97-98 of the NPRM. The lat/long is required for the craft and/or the operator's location, depending on type of Remote ID in use. The latitude and longitude are, presumably, from GPS signals (indeed, no one knows of another way to obtain this information such as indoors). **The craft may not be flown if the remote ID and its mandated message elements are not available:**

> "For example, a standard remote identification UAS would automatically transmit and broadcast the message elements and **its design would prevent it from taking off when the remote identification capability is not functioning**." (Page 95)

Thus, a small UAS that is unable to obtain latitude and longitude from GPS is incapable of flight.

Stated another way, this mean no certified and compliant aircraft will be capable of being flown inside most buildings, mines or caves. Specifically, except for a few buildings whose roofing does not act as a Faraday cage to shield RF signals, this prohibits indoor small UAS flight in numerous scenarios.

FAA Office of Rulemaking Agrees that the NPRM Restricts Indoor Flight

On January 8, 2020, I emailed the FAA asking questions to clarify the interpretation of this NPRM vis a vis indoor flight.

The FAA's January 9th, 2020 reply confirms that the NPRM bans the flight of small UAS over 0.55 pounds in weight when GPS is not available (i.e. indoors):

> Mr. Mitchell, Thank you for your questions regarding the proposed rule for UAS remote identification.
>
> 1. UAS that are “standard remote identification UAS” would transmit (through the internet) and broadcast (through an RF signal from the aircraft) the lat/long position of both the unmanned aircraft (UA) and the control station (CS). UAS that are “limited remote identification UAS” would transmit (through the internet) the lat/long position of the CS only. UAS without remote identification could be operated at certain flying sites recognized by the FAA.
>
> 2. There are certain situations when the UA would be prevented from taking off, and these depend on whether the UAS is standard or limited.
>
> a. For standard UAS, if the UA is being operated in an area where the internet is not available (rural area, for example), then it can still take-off if it is broadcasting. In order to take-off, the UAS must be transmitting (when internet is available) & broadcasting (all times) the full set of RID messages (including UA & CS lat/long).
> IMPORTANT: In both of these situations, for take-off, the messages MUST include the lat/long, so if the UAS derives lat/long through GPS, it must have a GPS position available. If the UA is in a location where GPS is not available and it cannot generate a GPS position, it could not take-off, because it would not be transmitting or broadcasting the FULL message set.
> IMPORTANT: If GPS is available at take-off, but the UA loses GPS after take-off, our proposal is that the loss of GPS would be indicated to the pilot and the pilot would have to land as soon as

practicable since the UAS is not sending the FULL message set any longer. The UA would not be forced to autoland in any situation. It's the pilot's responsibility to land at this point. IMPORTANT: for operations of a standard or limited UAS indoors where GPS is not available, if the UA is designed to use GPS as the lat/long position source, it would not be able to take off. Our rule has a provision for manufacturers to seek relief from the RID requirement when the UA is being manufactured and operated or "aeronautical research" purposes. So, if a manufacturer is building a prototype UAS for use ONLY in demonstrations indoors, the FAA could issue an authorization for the UAS to be manufactured and operated without RID, which would allow it to operate indoors.

b. For limited UAS, the same conditions apply except that, when the internet is not available, it would not take-off. Limited UAS are FULLY dependent on an internet connection, whereas standard UAS use an internet connection when it's available, but the broadcast feature allows standard UAS to operate when/where the internet is not available as well.

3. You are correct. If GPS is not available to a standard or limited UAS that uses GPS as the lat/long position source, it would not take off because it could not generate the RID message.

4. UA that weigh under 0.55 pounds which are not required to be registered are excluded from the RID requirement. I'll assume you are referring to "small" UAS that weigh over 0.55 pounds. As I stated in response #2, you are correct. If the UAS was manufactured with FULLY COMPLIANT standard or limited Remote ID, and the lat/long position is GPS derived, the UA would not take off if GPS is unavailable. As I stated in #2, manufacturers could seek an authorization to produce a "demonstration" model without RID for indoor use only. An authorization is not guaranteed, and would likely come with restrictions that ensure the UA is only operated for the requested purpose.

I hope your questions have been answered. Please provide any comments or suggestions you have to the docket. The best comments are those that include a rationale and, if appropriate, suggestions for alternative policy with supporting data or analysis.

Thank you,

FAA Office of Rulemaking

A craft under 0.55 pounds flown under Part 107 must have functioning remote ID as described on page 73 – however, this does not apply to indoor flight where the FAA has no jurisdiction.

While all Part 107 drones must comply with Remote ID, this compliance cannot be enforced in indoor airspace. Thus, it should be possible for a business to use a drone of any type indoors. But the FAA intends to prohibit the sale of non-compliant drones, precluding applications such as a professional video camera system used on an indoor movie set or to film indoor scenes in auditoriums and business settings. The indoor flight restriction also eliminates the use of drone video photography for sequences that travel from indoors to outdoors.

No accurate, reliable and tamper-proof method of determining latitude and longitude indoors without GPS has been defined, nor is it known whether such technology, if it exists, could operate on small UAS.

Consequently, the FAA's NPRM eliminates the use of small UAS technology in indoor setting and has the appearance of FAA de facto regulating indoor airspace.

In early February, a Thai soldier entered a shopping mall in Thailand and shot and killed over 20 people. Police made use of two drones donated by a citizen, and a third drone donated by a media outlet – to conduct surveys inside the mall[4]. The media drone had an IR sensor that successfully located the gunman. Unfortunately, the FAA's proposed rules eliminate most indoor flight in the U.S., making this scenario impossible and making life less safe for our police, who would not be able to call upon public volunteers for assistance.

FAA Re-authorization Act Prohibits FAA from Regulating UAS inside Mines

> **PL 115-254. Sec. 354. Treatment of unmanned aircraft operating underground**
> An unmanned aircraft system that is operated underground for mining purposes shall not be subject to regulation or enforcement by the FAA under title 49, United States Code.

In this NPRM per page 16, the FAA is prohibiting the sale of UAS>0.55 pounds that would be capable of operating underground. The NPRM violates PL 115-254 Sec. 354 by eliminating the sale of commercially built drones that would function inside mines.

Discussion and Recommendation

There is no currently available alternative for providing latitude and longitude from inside a building or mine.

Alternative 1

If GPS is not available, the Remote ID system could use "last known location". However, there is no guarantee this would be anywhere near the indoor flight. There can be no requirement on indoor accuracy since the FAA does not regulate indoor airspace. The craft could indicate to the REMOTE ID USS that it is using "last known coordinates, not current GPS", from which it could perhaps be deduced that this is an indoor flight.

Of course, this results in a loophole - anyone could conceivably put aluminum foil over the craft's GPS antenna and mimic no GPS signal available.

Alternative 2

The FAA permits the operator to manually specify this is an indoor flight and to disable the GPS mandate.

Such a craft would still be required to transmit a Remote ID containing operator information but not latitude and longitude. Thus, this craft would not necessarily be used for nefarious purposes as it would still be identifiable and would not be transmitting precise geolocation data of a child inside private property (see section on COPPA, later in these comments).

Alternative 3

Per the quote on NPRM Page 8, vendors may sell craft "For indoor use only".

[4] https://www.thaipbsworld.com/korat-mass-shooting-death-toll-jumps-to-27/

In the real world, there will be numerous new, non-compliant aircraft for sale on Amazon, Ebay, Alibaba and from many web retail vendors. If the FAA restricts legitimate indoor flight operations, this will create a large market of non-compliant drones.

A problem with saying users must purchase a separate craft for indoor flight is this doubles the costs for small UAS users who also need a craft for both indoor and outdoor use. This doubling of cost is not considered in the FAA's estimate of the costs of compliance.

Recommendation

The FAA needs to develop a workable and flexible identification system that enables indoor flight of small UAS. Eliminating indoor flight is not acceptable and must not occur as a result of this rulemaking.

Alternative 2 is recommended - it is simple and straight forward. It would maintain general compliance as users would buy Remote ID compliant drones that transmit ownership information - without causing users to purchase non-compliant small UAS.

Ways this might be accomplished include:

- Enabling craft to fly when GPS is not available such as when indoors.
- The FAA must expand the concept of FRIA to include, by default, all indoor airspaces and *inside flight "cages"* without requiring that "cages" be Federally certified FRIA locations. Flight cages could include "aviary netting" used at events such as EAA AirVenture to demonstrate quadcopter flights.
- Alternatively develop a system like all other laws that is based on trust and enforcement, not on inflexible one-size-fits-all under software control. Such a system would allow, for example, of allowing flight without GPS when no GPS signal is available - and to allow this to be an UAS configuration option.

Inconsistent Rules on Commercial Availability of Drones with and without Remote ID

A possible solution to the indoor flight restrictions may be hidden in the NPRM. From page 16 of the NPRM:

> "*The FAA envisions that upon full implementation of this rule,* ***no unmanned aircraft weighing more than 0.55 pounds will be commercially available that is not either a standard remote identification UAS or a limited remote identification UAS."***

The FAA expects all commercially made SUAS > 0.55 pounds to have functioning Remote ID, implying that non-compliant craft will not (or cannot) be sold in the U.S.

However, on page 8 and page 22, the FAA contradicts the statement on page 16:

> "All UAS **produced for operation in the airspace** of the United States would have to comply with the design and production requirements established in this proposal with exceptions for amateur-built UAS, UAS of the United States government, and unmanned aircraft that weigh less than 0.55 pounds."

A table on page 22 shows:

> No person would be allowed to operate a UAS **within the airspace of the United States** unless the operation is conducted under one of the following: (1) the UAS is a standard remote identification UAS and that person complies with the requirements of § 89.110; (2) the UAS is a limited remote identification UAS and that person complies with the requirements of § 89.115; or (3) the UAS does not have remote identification equipment and that person complies with the requirements of § 89.120.

Page 8 and page 22 emphasize that this restriction applies only to UAS "*for operation in the airspace of the United States*".

Because the FAA has no authority to regulate indoor airspace[5] or the sale of products used indoors, this implies commercially made UAS will be widely available without remote ID provided they have a "*For indoor use only*" sticker. Of course, no one would ever use such a craft outdoors. Ever.

The FAA has no authority to regulate retail sales of products used indoors. The FAA does not have the authority to regulate retail sales at all – the FAA's jurisdiction is the navigable airspace, not the shelves at Walmart. Non-compliant small UAS will be readily available from a variety of vendors just as FCC regulated non-compliant two radios are readily available from many vendors[6].

This creates a non-closeable loophole that renders much of this NPRM moot. The FAA's stated goal is to make most small UAS identifiable, trackable, and logged in real time for "national security". Except the FAA has no authority to prevent bad actors from using non-compliant craft, and non-compliant aircraft will be readily available to anyone who wishes to purchase them.

Recommendation

The NPRM aims to mandate real time tracking of nearly all small UAS in the U.S. and intends to enforce this by prohibiting the sale of non-compliant craft. However, non-compliant small UAS will be sold "for indoor use only", plus numerous non compliant SUAS will be widely available from on and offline vendors, easily accessible on Amazon, EBay and at other locations.

This issue blows a hole in the thought that this NPRM will restrict the airspace to compliant aircraft only. Any bad actor wishing to engage in criminal activities or mayhem will easily find alternative non-compliant aircraft for such use.

FAA's Proposed Use of FCC Part 15 Spectrum Leads to Interference and Crashes

The FAA proposes to use 47 CFR Part 15 of the FCC rules and regulations for transmission of Remote ID broadcast beacon signals. The FAA writes (page 136):

[5] https://www.faa.gov/uas/resources/policy_library/media/UAS_Fact_Sheet_Final.pdf

[6] The FCC regulates the radio spectrum and has requirements for "type accepted" radios (such as "Part 90" for business two-way radios) for use by various radio services. However, non-compliant two-way radios are widely available for sale.

> Additionally, for standard remote identification UAS, § 89.310(i)(2) proposes that the broadcast device use radio frequency spectrum in accordance with 47 CFR part 15 that is compatible with personal wireless devices **and must be designed to maximize the range at which the broadcast can be received**, while complying with the 47 CFR part 15 regulatory requirements

The requirement to "maximize the range" mandates that small UAS transmit at the 4 w ERP level (1 watt spread spectrum, 6 db gain antenna, which is the maximum permitted by 47 CFR Part 15).

> This proposed requirement would ensure that producers …. **Maximizing the broadcast range** would ensure that remote identification information would be available to the largest number of potential receiving devices within the limits permitted by law. **Maximized range** would also optimize future operational capabilities, such as detect-and-avoid and aircraft-to-aircraft communications where range is a factor.

Part 15 spectrum sharing relies heavily on low powered or highly directional signaling so as to minimize the interference to other Part 15 users and other licensed users of the radio spectrum that share the Part 15 bands.

The FAA describes its proposed ID system as being receivable by personal wireless devices, notably smart phones. The bands and modes that can be received by existing smart phones generally include Wi-Fi communications on the 2.4 Ghz and 5 Ghz bands, and Bluetooth on the 2.4 Ghz band.

Most small UAS in the recreational community, in recent years, are using combinations of the 902-928 Mhz band, the 2.4 Ghz band and the 5 Ghz Part 15 bands.

- 900 Mhz is typically used to send telemetry from the small UAS to the control operator.
- 2.4 Ghz is typically used to send flight control signals to the small UAS and sometimes to receive telemetry sent from the SUAS.
- 5 Ghz is used to send a video link (either analog or typically 8 Mbps digital) to the control operator.

Only the 2.4 Ghz and 5 Ghz bands overlap with commonly available personal wireless devices (i.e. smart phones).

The FAA, therefore, proposes transmitting Remote ID beacons on either 2.4 Ghz or 5 Ghz to insure compatibility with consumer electronics. In order to maximize the broadcast range[7], as called for by the FAA, this means using the 2.4 Ghz band for 4-watt ERP spread spectrum signals.

This leads to multiple problems.

1. 4 watts ERP is a strong RF signal, especially when located close to other 2.4 Ghz spectrum users – such as those flying other small UAS. Transmitting at the rate of once per second, this may cause direct interference and desense of nearby receivers, resulting in loss of flight control signals on other nearby SUAS. A narrow band 900 Mhz signal using low gain omni directional

[7] All things being equal except frequency, the range of 5 Ghz signals is about one-third that of 2.4 Ghz, therefore, the FAA is mandating use of 2.4 Ghz to achieve maximum range.

antennas can be received up to 40 miles away[8]. On the 2.4 Ghz band, this distance would likely exceed 10 miles.

2. The SUAS will be operating, potentially, at hundreds of feet above ground level. From this altitude, the potential point-to-point line of sight range – could be 10 or more miles (depends on whether using narrow band or spread spectrum signaling and the degree of forward error correction and other factors). From the high altitude of a SUAS in flight, the 4-watt ERP signal will interfere with other Part 15 devices and licensed services over a wide area.
3. This high-power level, by numerous SUAS at altitude, will increase the RF noise floor, ultimately reducing the range of the Remote ID beacons.

Prior to 1997, the FCC did not permit Part 15 devices to use "high gain" antennas as Part 15 systems were intended to communicate over very short distances. Short distances meant that the Part 15 frequencies could be re-used (or shared) by others located a short distance away (such as a hundred meters or more). In 1996, the FCC modified the Part 15 rules[9] to allow the use of "directional gain antennas"[10] on certain bands. In 2004, the FCC expanded the Part 15 rules to accommodate directional gain antennas on the 2.4 Ghz band[11], and the use of MIMO and phased array sectorized antennas[12]. The use of directional antennas focuses the RF energy in a particular direction, enabling re-use of the spectrum in areas where the antenna and its outgoing signals, are not being used. The key takeaway is that short distance – or highly directional transmission – enable re-use of the shared spectrum by multiple users.

The FAA, however, proposes that SUAS, flying potentially hundreds of feet in the air, be transmitting once per second at a maximum power level permitted for Part 15, to achieve the broadest possible range and for the signal to be received by the largest number of potential Remote ID receivers. This implies, obviously, the use of non-directional antennas.

This requirement is fundamentally at odds with the intent of Part 15 and how it works to share spectrum. This requirement will lead to raising the RF noise floor, at a minimum, **which will limit the useful range of Remote ID** and cause direct interference to other Part 15 users[13], including numerous consumer products located in residential settings, and licensed users. Thus, the FAA's proposed use of Part 15 – to maximize the power level and range of transmission – is at odds with the approach the FCC encourages for Part 15 devices.

High Power Part 15 Signals May Cause Loss of Flight Control Accidents

A related problem, as noted above, is that placing individual – or possibly numerous – 2.4 Ghz, 4 watt ERP Remote ID transmitters in close proximity (think of a group of "modelers" flying multiple compliant SUAS together in formation, in aerobatics competition, or in simulated "air combat") may lead to

---

[8] 900 Mhz product data sheet, retrieved from https://media.digikey.com/PDF/Data%20Sheets/MaxStream%20PDFs/XT09-DK.pdf

[9] I wrote the first draft of the public comments filed by Microsoft Corporation regarding the FCC's 1996 Notice of Proposed Rulemaking on Part 15 technology and its approval of directional gain antennas.

[10] https://docs.fcc.gov/public/attachments/FCC-96-36A1.pdf

[11] https://ecfsapi.fcc.gov/file/6516285598.pdf

[12] I was working at Vivato when a colleague wrote and filed Vivato's comments on this FCC proceeding that expanded Part 15 directional antennas to include 2.4 Ghz and "smart" phased array type antenna technology.

[13] Part 15 devices, of course, are required to accept interference from other Part 15 devices and from licensed users of the same spectrum.

receiver desense and flight control interference, potentially causing loss of control of the SUAS. A 2011 article[14] in Model Airplane News noted that the 2.4 Ghz band was already crowded and Part 15 interference may have been the cause of model airplane crashes. I demonstrated this by flying an MJX Bugs 3 quadcopter (2.4 Ghz proprietary control link) near a GoPro camera sending video on 2.4 Ghz – causing loss of flight control[15].

Since the 2.4 Ghz Remote ID may be embedded within the normal control link between the flight controller and the small UAS, the requirement for maximum 4 w ERP signals means that all communications (including control data) will be at the high power level as it is not likely the SUAS will rapidly change its power output once per second to switch between Remote ID broadcasts and control link data.

As written, the FAA's use of Part 15 for Remote ID will increase interference to consumer devices and may result in the loss of control of recreational SUAS, which is a threat to public safety.

High Power Part 15 Remote ID will Cause Interference to Licensed Users

High power Part 15-based Remote ID will create interference to licensed users of the same spectrum used by Wi-Fi – yet the Part 15 rules prohibit causing interference to licensed spectrum users. Consequently, a Remote ID system must "listen before talking" and cannot be broadcast only.

When a Part 15 device causes harmful interference to a licensed spectrum user, the licensed user may request that the Part 15 device cease operation.

> 47 CFR § 15.5 General conditions of operation.
>
> (c) The operator of a radio frequency device shall be required to cease operating the device upon notification by a Commission representative that the device is causing harmful interference. Operation shall not resume until the condition causing the harmful interference has been corrected.

The FCC envisioned Part 15 devices as being primarily at fixed or portable locations. When a Part 15 device causes interference it can be physically located because of its limited transmission range. But under the FAA's NPRM, high power, high altitude Part 15 Remote ID systems traveling at a high speed would make discovery of the operator and contact with the operator to request termination of the interference, likely impossible. This implies Part 15 usage that would not comply with FCC rules.

Recommendation

- For reasonable broadcast range and to reduce interference from Remote ID broadcasts, and to reduce the probability of receiver desense in other local SUAS, the maximum power level should be set at 100 mw ERP (or similar).

---

[14] https://www.modelairplanenews.com/2-4ghz-is-it-all-its-cracked-up-to-be-join-the-discussion/

[15] Test was performed at an AMA certified model airfield under controlled conditions and with safety precautions in place. Upon loss of control signal, the Bugs 3 immediately turns off its motors and falls directly downwards. This test was done from a few feet of the ground. The GoPro's claimed Wi-Fi-based video transmitter range is a few hundred meters – it is probably operating at a power level in the 10s of milliwatt range and at least an order of magnitude less than the FAA's proposed Remote ID broadcast.

- Depending on the receiver and receiving antenna used, this power level will likely achieve 500m to 1000m range to a handheld smart phone (more than enough to receive a signal, on the ground, from a SUAS in the local area) and up to several kilometers point to point, in the air, at altitude.

- An appropriate power level will deliver reasonable range, reduce the interference potential to other Part 15 devices and to licensed services, and reduce the likelihood of desensing receivers on other SUAS and the potential loss of flight control.

- The FAA should consult with the FCC on the FAA's envisioned use of Part 15.

]

"Internet is available" May Require Use of Most Expensive Option, if Available, and Specifies a Technically Infeasible Use of Wi-Fi

The NPRM refers to small UAS connected to the Internet in real-time, typically via a smart phone app that will relay signals from drones to an Internet-cloud database, once per second. Repeatedly, the NPRM references when "Internet is available" but the FAA defines "Internet is available" in a way that makes this unaffordable in rural areas.

In addition, the NPRM suggests using Wi-Fi to connect the UAS to the Internet – ***but this is technically impossible if low cost is the goal. It is not possible*** **to use a smart phone to control a small UAS and simultaneously connect to the Internet over Wi-Fi.** The effect is the FAA is mandating purchase of a smart phone and cellular data service for all flights of small UAS that are required to be logged in a Remote ID USS.

The NPRM writes (Page 101):

> Under the proposed rule, the internet would be considered available **if cellular or other forms of wireless internet connectivity such as Wi-Fi are available in an operational area with sufficient signal strength to maintain a connection between the UAS and the internet**.

There are ***two major problems*** here.

One is that the FAA appears to misunderstand how Wi-Fi is used to control low cost small UAS – and the technical infeasibility of using Wi-Fi to both control the small UAS and connect to the Internet at the same time.

The second is that, as written ("*other forms of wireless internet connectivity*"), the NPRM implies if one's current cellular service does not provide coverage but a competitor does, then the operator of the small UAS is required to subscribe to the additional cellular service provider.

This makes no sense at all.

1. The use of Wi-Fi for Remote ID USS access is technically infeasible for how most smart phone control apps work on low cost quadcopters. Numerous small UAS use a flight control app on a smart phone to fly the small UAS. This app connects the phone to the SUAS using Wi-Fi and

provides a control interface and uses the smart phone to display still and video images from the quadcopter's camera.

In order to connect to the small UAS, the SUAS implements a Wi-Fi Access Point. The phone connects to the small UAS Access Point and then uses Wi-Fi to exchange data and control signals with the SUAS. ***The phone can connect to only one Access Point at a time. It is not feasible to use Wi-Fi to control the small UAS and to simultaneously connect the phone to a second Internet-connected Access Point for the purpose of Remote ID USS data logging***. This cannot be done.

The goal of a Limited Remote ID appears to be to provide a low-cost entry point. In theory, one could provide a separate flight controller that connects to the phone via USB or Bluetooth solely for the Remote ID USS logging, and then use the phone to connect to an AP for logging. But would dramatically increase the cost of the product. The Yuneec Breeze, for example, uses the phone as the flight controller – to keep costs low. You can fly and see video/stills from the quadcopter all from the phone, with no additional components. You can optionally add a separately purchased ($) conventional flight controller. The controller sends flight commands over Bluetooth to the phone, which then signals the quadcopter using the Wi-Fi link on the phone[16].

The FAA's concept of Limited Remote ID logging to a Remote ID USS using Wi-Fi cannot work. Instead, the phone would have to do data logging over cellular Mobile Data, increasing costs. The effect of these technical limitations is that the Limited Remote ID makes little sense – no one is likely to manufacture such a product and no consumer is likely to buy such a product. It's either lower cost SUAS with higher cost Mobile Data, or higher cost SUAS with lower cost Wi-Fi and less functionality. It's a crappy product that no one wants.

2. The NPRM relies on assumption of widespread cellular service capable of supporting Remote ID USS logging. While cellular coverage is good in many areas, there are others (such as half of my state) where access is non-existent or coverage is available from only one provider[17].

   If I have T-Mobile service, but there is no service – but Verizon has service available - does "Internet is available" mandate I purchase Verizon service for these areas? The way this is written in the NPRM, yes, I am now required to purchase Verizon cellular (another cost not listed in Compliance Cost estimates). In fact, since cellular coverage varies greatly by provider, in order to fly in the largest number of places in the State, the NPRM literally requires I purchase service from all possible cellular providers.

   Taken to an extreme, by 2024, SpaceX expects to have its Starlink, satellite-based Internet service in operation. Would I be required to subscribe to Starlink, and provide AC power and antenna systems in remote areas, to fly in very remote, unpopulated BLM or USFS lands in

[16] There is another model where the flight controller acts as a Wi-Fi Access Point, the phone and the aircraft both act as clients of the flight controller. But there is still no way to connect to a second Access Point in this configuration, either. Remote ID USS access over Wi-Fi cannot be done using existing models of flight control based on Wi-Fi.

[17] For example, I have T-Mobile cellular service. About half of my state, due to large areas of mountainous, unpopulated areas, has no T-Mobile cellular service. AT&T coverage is similar to T-Mobile in many of these areas, and coverage may mean "2G, no data" service, a detail not obvious from the high-level coverage map.

eastern Oregon, where the flight "risk" to anything is a limit approaching zero? According to the wording of the NPRM ("*other forms of wireless internet connectivity*"), yes, I would be required to purchase satellite Internet access for flight in remote areas.

Recommendation

- The FAA's requirement to use the most complex and expensive Internet access – *if available* – is unacceptable – and renders flight in remote areas accessible only to the wealthy and industrial corporate operations.

- The NPRM describes the suggested use of Wi-Fi for Remote ID USS logging in a way that is not technically feasible. The concept of a Limited Remote ID appears to be for low cost small UAS (e.g. quadcopters) controlled by phone and logging the operator's position to the Remote ID USS, presumably by low cost Wi-Fi. But since the phone can connect to only one Access Point at a time, this is not possible. This craft could only log its position reports using Mobile Data. This adds to the costs of compliance by mandating a smart phone and a data plan – even for toy quadcopters over 0.55 pounds flown by children.

- In addition, because Wi-Fi is frequently used as the flight controller data link to the aircraft, the Wi-Fi data stream can itself constitute the Remote ID beacon with the "message elements" embedded within this data stream. This enables creation of a low-cost broadcast beacon based Remote ID, and the potential for firmware updates to enable existing SUAS to comply with Remote ID transmissions. This is the only use of Wi-Fi that makes any sense.

- The NPRM must state that "Internet is available" means "reasonably available", and that it does not mandate purchasing potentially expensive service plans or satellite services in order to comply with this requirement. Particularly since the lack of service occurs primarily in unpopulated or low populated rural areas, although it can also occur in hilly and mountainous terrain in areas close to population centers.

- The NPRM should not specify an open ended "*other forms of wireless Internet connectivity*" mandate while simultaneously proposing a Standard ID that supports flight with broadcast beacon ID (no Internet access).

- The Limited Remote ID concept for low-cost entry-level drones is not a viable market product. It won't work over Wi-Fi, and options that could work over Wi-Fi greatly increase costs to the point that the product has no market appeal. The entire Limited Remote ID should be dropped from the NPRM and replaced with a simple broadcast-based Remote ID scheme for VLOS flight.

Effect of Remote ID USS app on smart phone battery capacity

The NPRM makes an assumption that a smart phone app will act as an interface to the Remote ID USS, transmitting updates at the rate of once per second. For many small UAS, the smart phone is also the "flight controller" for the small UAS.

This leads to the question: *What is the impact on battery life of requiring an app to obtain a GPS fix and transmit a position report every second over a cellular data link?*

I tested this assumption by creating a pseudo Remote ID USS logging app for a Pixel 2[18] smart phone running Android 10 and connected to the Internet via T-Mobile service.

The Remote ID USS app was run by itself. At the rate of once per second, this app read its GPS location (Remote ID requires the operator's location) and made a simulated data transmission into the Internet over the cellular connection, at the rate of once per second. After ten minutes of operation, the battery drain was between 6% and 13% of the battery capacity. Subsequent testing indicated this power drain is variable based on the cell site signal strength. Actual results will depend on the type of phone in use, condition of the battery, battery capacity, the specific cellular service provider, and the quality of the available cellular signal.

For the sake of a conservative estimate, we will assume that 10 minutes of flight represents about 5% of battery capacity. This implies 30 minutes of flight time could be 15% of battery capacity in addition to the power demand of a possible flight control app running on the phone (which by itself can be 30%-40% of battery capacity over 30 minutes). The addition of Remote ID USS logging can quickly lead to one half of the battery capacity being drained.

Discussion

Smart phones have a reasonably long battery life between charges due to use of various tricks to keep hardware turned off as much as possible. This technique is obvious when used to turn off the display after 15-30 seconds of inactivity, for example.

In general, the most power demanding features of a smart phone are the display, the GPS receiver, the cellular transmitter and the Wi-Fi transmitter. Other power demands come from computationally intensive tasks that fully use the CPU cores and/or GPU; less computationally intensive tasks may use only a part of a CPU (e.g. one of 4 cores, at a reduced clock rate), helping to reduce power consumption.

The hardware and the operating system work together to keep individual hardware components powered down or in a low power consumption state, as much as possible. The operating system can suspend software applications to prevent them from running needlessly and reschedule them to run at specific intervals to reduce power demand. From the Android Development Guide:

> *Doze* reduces battery consumption by deferring background CPU and network activity for apps when the device is unused for long periods of time. *App Standby* defers background network activity for apps with which the user has not recently interacted.
>
> While the device is in Doze, apps' access to certain battery-intensive resources is deferred until maintenance windows.[19]

A Remote ID USS logger is required to log data once per second. This keeps most of the phone hardware in an elevated power consumption state, continuously. This results in a rapid drain on the battery.

---

[18] The Google Pixel 2 is about one year old. The battery is in excellent health and has capacity similar to when the phone was brand new. The actual percentages shown here vary based on the type of phone in use, the size of the battery, the condition and temperature of the battery, the cellular service provider used and the strength of the cellular signal, plus whether a user has other apps running during the test. It is also possible that the test app could be optimized better.

[19] https://developer.android.com/training/monitoring-device-state/doze-standby

According to the Android Development documentation:

> When an app connects to the mobile network in the background, the app wakes up the CPU and turns on the radio. Doing so repeatedly can run down a device's battery.[20]

Further, because of "tail-time battery cost", the elevated power consumption remains in effect for a period of time after the cell transmitter has been turned off.

> Perhaps less intuitively, because the tail-time battery cost is relatively higher, it's also more efficient to keep the radio active for longer periods during each transfer session to reduce the frequency of updates[21].

"tail-time" refers to the need to keep the cellular handset in a heightened power consumption state for a period of time after transmission has completed[22]. What this means is that the phone hardware does not sleep in the one second interval between transmissions – but is kept in a high-power state.

Consequently, sending frequent, short data packets, has the worst impact on power consumption. Google recommends exchanging larger amounts of data, less frequently, to extend the battery life.

Stated another way, the FAA is, by design, forcing smart phone batteries to drain rapidly.

Based on my tests, a phone whose battery might last 2 days, when the phone is little used and sitting on a desk, might drain nearly half of its battery capacity during a 30-minute flight due to a combination of a flight control app and Remote ID USS data logging.

Recommendation

- The power demand on the smart phone battery life is an issue that does not appear to have been analyzed by others. More work should be done on this to characterize the battery impact.

- 30 minutes or more of flight time during a day is a reasonable expectation of use. If this drains half of a cell phone battery, this may be a problem for some users.

- 60 minutes of flight might result in a dead or nearly dead battery. This, in turn, could become a safety issue for pilots who may be in remote locations, have no way to recharge their phone, and unexpectedly find their battery is dead.

- At a minimum, this adds additional costs of compliance-extra time may be required to recharge batteries, plus the cost of external batteries (e.g. an Anker battery) to power or recharge the

---

[20] https://developer.android.com/topic/performance/vitals/bg-network-usage

[21] https://developer.android.com/training/efficient-downloads/connectivity_patterns

[22] Qian, F., Wang, Z., Gerber, A., Mao, Z., Sen, S., Spatscheck, O. (2010). "TOP: Tail Optimization Protocol For Cellular Radio Resource Allocation". The 18th IEEE International Conference on Network Protocols. **DOI:** 10.1109/ICNP.2010.5762777. Retrieved from: https://www-users.cs.umn.edu/~fengqian/paper/top_icnp10.pdf. I also measured this effect in research done for my own Master's thesis.

phone, particularly in remote locations, plus the safety issue of having a dead phone. In general, this results in an operational “hassle” factor that discourages compliance.

- This additional cost has not been considered in the costs of compliance.

Android and Wi-Fi Connected Quadcopter Control Apps and Remote ID USS Logging

The default network programming model used by app developers does not permit an Android phone to connect simultaneously over Wi-Fi to a quadcopter while sending data to a Remote ID USS over Mobile Data.

I attempted to test run the simulated Remote ID USS app simultaneously with the Yuneec Breeze flight control app, however, this did not work because I could not have both Wi-Fi and Mobile Data enabled at the same time.

By default, Android prioritizes data transmission to use Wi-Fi. This means if Wi-Fi and Mobile Data are both "on", attempted Internet access will be routed to the Wi-Fi port – which goes to the quadcopter AP – which is not connected to the Internet.

When Wi-Fi is used by a phone as the control link to the quadcopter, the quadcopter is acting as a Wi-Fi Access Point - but without any Internet access. Consequently, the Remote ID USS app is sending its data over the Wi-Fi link - to the quadcopter - not over the Mobile Data cell connection to the Internet.

The solution is for app developers to directly manage the Wi-Fi and Mobile Data network connections independently, as explained in Android documentation[23]. *Prior to Android 5.0, this was not possible.*

The implications of this are that it will not be possible to use a Remote ID data logger

- On certain older phones
- In conjunction with older control software (unless updated by the manufacturer)
- The use of iPhone and iOS for this capability is unknown

NPRM and the Children's Online Privacy Protection Act

The NPRM’s enforced collection and minimum six-month retention of data (in Remote ID USS) when children are flying a small UAS conflicts with the Children’s Online Privacy Protection Act.

The Children's Online Privacy Protection Act (COPPA) sets requirements for the collection of personal data from children, whether the online service is directed to children or not. Online service is defined in a way that it encompasses the NPRM's recording of precise geolocation information tied to a personal identifier into an Internet database. Parental permission does not solve the problem – at any time in the future, the parent may request review, deletion and suspension of collected data. Age restrictions do not solve the problem either – once a parent discovers that a child flew a toy quadcopter and their data

[23] https://android-developers.googleblog.com/2016/07/connecting-your-app-to-wi-fi-device.html

recorded, the parent may subsequently request review, deletion and suspension of the data. The COPPA law has no exemption for the Federal government; government agencies must comply with COPPA.

COPPA applies to all children under age 13 - and per a bill[24] now under consideration in the House, this age may be raised to under 16. For that reason, this text, below, will refer to "under age 13 (or 16)" to reflect this uncertainty. The bill under consideration elaborates on the definition of protected geolocation data - the text in the new bill reads:

> PRECISE GEOLOCATION INFORMATION.— The term 'precise geolocation information' means historical or real-time location information, or inferences drawn from other information, capable of identifying the location of an individual or a consumer device of an individual with specificity sufficient to identify street level location information or an individual's or device's location within a range of 1,640 feet or less.

The FAA is Aware of COPPA

The FAA is aware that the Children's Online Privacy Protection Act (COPPA) applies to the FAA's collection of data involving UAS. On page 12 of the Unmanned Aircraft Systems (UAS) Registration Task Force (RTF) Aviation Rulemaking Committee (ARC): Task Force Recommendations Final Report. November 21, 2015, the FAA writes:

> 4.2.4 Should there be an age limit for registration?
>
> All sUAS flown outdoors and exceeding 250g maximum flight weight must be registered. However, **consistent with the Children's Online Privacy Protection Act, 15 U.S.C. §§ 6501-6505, the Task Force recommends a requirement that individuals be 13 years or older to register an sUAS. Although acknowledging that some sUAS may be operated by persons younger than 13, the Task Force would thus recommend that registered sUAS owners be 13 years of age or older, and that children under that age operate sUAS under a parent or guardian's registration**.[25]

Here, the FAA acknowledges that COPPA applies to FAA registration and resolves this by disallowing registration by those under age 13 but recognizing that such youth will continue to fly UAS under the registration of a parent or guardian.

This NPRM, however, requires real time tracking and the collection of geolocation data of pilots and their aircraft operations. In the event the craft is flown by a person under age 13 (or 16), this means the FAA mandates collection of personally identifiable data linkable to a protected class member under age 13 (or 16) and retention of that data for six-months.

Federal Government and Contractors Are Not Exempt From COPPA

Per COPPA, the Federal government and its contractors are not exempt from the privacy protections specified by COPPA.

---

[24] https://walberg.house.gov/sites/walberg.house.gov/files/PROTECTKidsAct.pdf
[25] https://www.regulations.gov/document?D=FAA-2015-7396-5594

COPPA Requirements, FAA Data Collection, Age Restrictions and a Technical Solution

First, we examine the requirements of COPPA as described by the Federal Trade Commission.

Then we look at how these rules impact the FAA's collection of data - knowingly or unknowingly - when children are operating small UAS.

Then we consider simple options such as age restriction - and show how this does not solve the problem either.

Finally, we propose a technical solution to this dilemma that involves a different approach to logging position reports in the Internet cloud.

I am not a lawyer. My background is engineering of computer products and services. When developing products and services, if I encounter legal questions that affect our product or service, I would seek outside advice. As I do not have a personal budget for legal assistance in making these comments, I am bringing these issues to the attention of the FAA.

COPPA Definitions that Apply to Internet Logging of UAS Operations

The previous section established that the FAA is aware that COPPA applies to the FAA's collection of data. The following text comes from the Federal Trade Commission's online information about COPPA and how to implement COPPA to comply with this Federal law.

Emphasis added to key phrases, below:

> **2. Who is covered by COPPA?**
> The Rule applies to operators of commercial websites and online services (including mobile apps) directed to children under 13 that collect, use, or disclose personal information from children. It also applies to operators of general audience websites or online services with actual knowledge that they are collecting, using, or disclosing personal information from children under 13. The Rule also applies to websites or online services that have actual knowledge that they are collecting personal information directly from users of another website or online service directed to children.

As we will see shortly, COPPA also applies to those who unintentionally collect data on children and learn they have done so, after the fact.

What is meant by an “online service”?

> **The term “online service” broadly covers any service available over the Internet, or that connects to the Internet or a wide-area network**. Examples of online services include services that allow users to play network-connected games, engage in social networking activities, purchase goods or services online, receive online advertisements, or interact with other online content or services. **Mobile applications that connect to the Internet**, Internet-enabled gaming

platforms, voice-over-Internet protocol services, **and Internet-enabled location-based services also are online services covered by COPPA.**[26]

The FTC calls out "**internet-enabled location-based services**" and "**connected toys or other Internet of Things devices**":

> **"Website or online service"**[27]
> COPPA defines this term broadly. In addition to standard websites, examples of others covered by the Rule include:
> - mobile apps that send or receive information online (like network-connected games, social networking apps, or apps that deliver behaviorally-targeted ads),
> - internet-enabled gaming platforms,
> - plug-ins,
> - advertising networks,
> - **internet-enabled location-based services,**
> - voice-over internet protocol services,
> - **connected toys or other Internet of Things devices**

Protected personal information includes geolocation information:

> Personal Information includes[28]
> **Name, contact information, serial number, unique device identifier geolocation information sufficient to identify a street name and city or town**; or

We have now established that the Remote ID USS database may collect COPPA defined protected information on youth including precise geolocation data.

The Federal Government is Required to Comply With COPPA:

> **6. Does COPPA apply to websites and online services operated by the Federal Government?**
> As a matter of federal policy, **all websites and online services operated by the Federal Government and contractors operating on behalf of federal agencies must comply with the standards set forth in COPPA**. *See* OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (Sept. 2003).[29]

PL 115-254 calls out privacy requirements in regards to UA and UAS:

> **SEC. 357. UNMANNED AIRCRAFT SYSTEMS PRIVACY POLICY.**

[26] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions
[27] *https://www.ftc.gov/tips-advice/business-center/guidance/Children's-online-privacy-protection-rule-six-step-compliance*
[28] https://www.ftc.gov/tips-advice/business-center/guidance/Children's-online-privacy-protection-rule-six-step-compliance
[29] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions

It is the policy of the United States that the operation of any unmanned aircraft or unmanned aircraft system shall be carried out in a manner that respects and protects personal privacy consistent with the United States Constitution and Federal, State, and local law.

An "age screen" may be employed to attempt to identify and avoid collecting data on children under age 13. The proposed Internet tracking system, however, is mandatory and provides no method to identify and exclude this data collection *at time of flight when the small UAS is operated by a protected youth*:

In circumstances where children are not the primary audience of your child-directed service, the amended Rule allows you to employ an age screen in order to provide COPPA's protections to only those visitors who indicate they are under age 13. Note that sites or services directed to children cannot use the age screen to block children under age 13. *See* FAQ D.2 above. Once you identify child visitors, you may choose to:

- Collect parents' online contact information to provide direct notice in order to obtain parents' consent to your information collection, use and disclosure practices; or
- Direct child visitors to content that does not involve the collection, use, or disclosure of personal information[30].

Suppose the Remote ID USS data collection is viewed as having a generic audience and is simply unaware of the age of the small UAS operator – the problem is that *a parent or guardian can inform the service at any future time they have collected protected data on a minor*:

5. I operate a general audience online service and do not ask visitors to reveal their ages. However, I do permit users to create their own blog pages, and my service has a number of online forums.

(a) What happens if a child registers on my service and posts personal information (*e.g.,* on a comments page) but does not reveal his age anywhere?
The COPPA Rule is not triggered in this scenario. The Rule applies to an operator of a general audience website if it has actual knowledge that a particular visitor is a child. If a child posts personal information on a general audience site or service but does not reveal his age, and if the operator has no other information that would lead it to know that the visitor is a child, then the operator would not be deemed to have acquired "actual knowledge" under the Rule and would not be subject to the Rule's requirements.

However, even where a child has not revealed his or her age on a site or service, an operator may acquire actual knowledge where it later learns of a child's age – for example, <u>through a report from a concerned parent who has discovered that her child is participating on the site.</u> <u>Where an operator knows that a particular visitor is a child, the operator must either meet COPPA's notice and parental consent requirements or delete the child's information</u>[31]<u>.</u>

[30] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Audience
[31] https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions#General%20Audience

Note the bold face second paragraph above as this is the crux of the problem. Parents and guardians can request review, deletion and suspension of data collection at any time after learning that data on their child has been collected.

Parents and Guardians Are Entitled to Request Review, Deletion and Suspension of Data Collection

Even if the FAA aircraft is registered to an adult, if the adult later finds that it has been operated by a protected child, the parent is legally entitled under COPPA to notify the Remote ID USS for the data collection, to request a review of the data, to request deletion of that data and to refuse further collection of data.

The Remote ID USS database operator has no choice in this manner:

> "… if you operate a general audience Web site and have actual knowledge that you are collecting personal information from children, you must comply with the Children's Online Privacy Protection Act." [32]

Further, the FAA and the Remote ID USS operator must enable parental review of the data, enable the parent to refuse any additional collection of the data, and the option to delete existing data.

> Even if parents have agreed that you may collect information from their kids, parents have ongoing rights — and you have continuing obligations.
>
> **If a parent asks, you must:**
> - **give them a way to review the personal information collected from their child;**
> - **give them a way to revoke their consent and refuse the further use or collection of personal information from their child; and**
> - **delete their child's personal information[33].**

Yet on page 24 of the NPRM***, the FAA requires data to be retained for six months:***

> The Administrator shall require any Remote ID USS to retain any remote identification message elements for 6 months from the date when the remote identification message elements are received or otherwise come into the possession of the Remote ID USS.

The FAA's NPRM and COPPA are in direct conflict. The FAA cannot collect and retain this data for six months per COPPA. The proposed Remote ID USS system violates COPPA whenever children are involved in operating a small UAS, with or without parental permission.

---

[32] http://www.coppa.org/comply.htm

[33] *https://www.ftc.gov/tips-advice/business-center/guidance/Children's-online-privacy-protection-rule-six-step-compliance*

This becomes more complicated when, say, I allow children who are not my children to fly a quadcopter in my backyard. Technically, I am not the parent or guardian – but I am now aware of a COPPA violation and I have no recourse to request removal of this data except to contact their parents/guardians, and provide them with the Remote ID USS contact information, the unique serial number and registration information of the small UAS that as flown, and then have them make contact with the Remote ID USS.

Note first the added complexity of doing all that. But also note that since the actual parent/guardian is not the owner of the small UAS, this could prove problematic if the operator of the Remote ID USS demands proof of ownership. We end up with a Catch-22 – the law requires the parent have access to this data but the actual parent does not own the craft that was involved and might be denied access.

Related – Remote ID USS May Collect Aerial Images of Children

> "However, the proposal does not prohibit designers, producers, or operators from including a capability for limited remote identification UAS to broadcast information or data unrelated to remote identification, **such as a camera feed or telemetry data**." NPRM, Page 97, Section X, A, 2, Paragraph 2

As explained later in these comments, some Remote ID USS may use a "free" business model, where they are funded by selling data collected from aerial drones. Automated drone fleets, and contracted Remote ID USS of unsuspecting recreational flyers, may be capturing high resolution imagery of children in their own backyards, in public parks, walking to and from school, and so on – connected to precise locations.

It is mandated by Federal law (COPPA) that anyone must be able to request access to review this data, delete this data and suspend collection of this data.

Suppose I see several drones overfly my home. I suspect (but do not know) that one or more may be taking aerial photos of my children. I am now expected to identify each drone operator (but probably cannot since their identity will be hidden behind a "Session ID"), somehow identify the Remote ID USS that is in use (but which is not, per the NPRM, publicly available), find contact information for their Remote ID USS, and then contact each of the Remote ID USS operators and give them time and location so they can enable me to review, delete or suspend data collection.

Seriously?

First, as a parent, I will not be able to assert my legal rights under COPPA because I will not have access to drone identifying information – I won't know who the operator is or which Remote ID USS has retained information.

Second, if I could contact the Remote ID USS, and I requested suspension of this data collection, each Remote ID USS would need to maintain a geolocation map of areas where data collection has been suspended. These areas will need to be provided to the drone fleets – in near real time – to prevent their future capture of additional images of children from the specified location.

At a minimum, the “message elements” contained in the Remote ID transmission should include an identifier for the Remote ID USS that is use and an anonymized Session ID that can be presented to the Remote ID USS host by a parent or guardian.

Discussion

COPPA applies to the FAA's anticipated collection of geolocation and personally identifiable information from children under age 13 (or 16) due to mandated requirements to log flight operations in a Remote ID USS database, if Internet is available.

Even if the data is collected without knowledge that the small UAS operator is a youth, if a parent or guardian learns of this, they have a legal right to notify the Remote ID USS operator and to request review, deletion and to refuse collection of any more such data.

This request, however, is easy to spoof and there is no foolproof way - in any practical, scalable sense - to prevent others from using this requirement to have data collection turned off or deleted. This is yet another loophole.

The FAA could, during aircraft registration, state that no one under age 13 (or 16) may be allowed to operate the small UAS. Banning kids would be a public relations mess for the FAA. It would shut down youth aviation STEM programs completely. Further, if Congress raises the age limit to 16, this has the oddity that children age 14 and 15 may legally pilot sailplanes and hot air balloons - but could not legally fly a toy airplane. This would be quite something - Civil Air Patrol cadets could not legally fly a toy airplane until age 16 – while simultaneously learning how to fly a sailplane.

Another possibility is to employ an age screen at time of each flight. However, this would be cumbersome, easily spoofed, and once a child has flown anyway, COPPA's requirements for parental review, deletion and suspension of data collection still remain in effect.

Thus, prohibiting flight by those under age 13 (or 16) does not resolve the problem as children will fly anyway, with or without parental supervision. When a parent learns of this, the parent has a legal right to request to review the data, delete the data and to refuse permission to collect anymore data.

Banning flight by youth does not fix this problem.

A Potential Solution to the Conflict with COPPA

There is a possible technical solution that meets most FAA requirements and greatly reduces the issues with COPPA.

The most straightforward solution for the FAA is to require Internet-based tracking of Part 107 and other commercial operations and Beyond-Visual-Line-of-Sight (BVLOS) only and not for routine recreational flights. According to the FAA, "You must be at least 16 years old to qualify for a remote pilot

certificate"[34]. At first glance this proposal appears to eliminate all tracking of recreational craft. However, I propose, below, a novel solution to resolve this.

By restricting data collection to commercial and BVLOS operations, the FAA largely excludes flights by those under age 16 and therefore, complies (mostly) with COPPA.

This leads to a technical solution to avoid violating COPPA while continuing to collect data useful for commercial air traffic management services, and simultaneously enhancing the likelihood of rule compliance by recreational flyers.

Recommendation: A Technical Solution to Reduce COPPA Violations

Let us assume that recreational aircraft use broadcast beacon-based Remote ID only. All recreational flights transmit their location and altitude in real time. This information may be received by other craft and used for collision avoidance or other purposes.

Automated and Part 107 drone fleets would receive the broadcast beacon-based Remote ID transmissions, including the location and altitude of recreational craft while their own commercial SUAS are in flight. Because both aircraft would be "in the air" the transmission distance of these beacons would be a maximized "line of sight" distance.

For the purposes of an air traffic control database, commercial drones would strip personally identifiable information from the beacon broadcasts of recreational small UAS and relay the anonymized data (craft type, latitude, longitude, altitude) into the Internet cloud Remote ID USS where it may be used for automated air traffic management services.

By anonymizing the data, this data collection would then fully comply with COPPA.

Law enforcement would have access to broadcast beacon Remote ID transmissions, including the operator information, by receiving the beacons directly. Law enforcement would have access to flight locations recorded in the cloud database for subsequent tracking of flights (assuming flight occurs while other commercial operations are in progress and relaying this information) - or could set up their own broadcast beacon ID receivers at special events (such as a stadium or parade or festival).

By submitting anonymized data into the cloud, this data could be used to provide air traffic management services to the commercial operators – without compromising the personal information of children who may be operating small UAS. Recreational flights would be tracked, by location, and law enforcement could access historical tracking data.

In the event there are no commercial operations in the area to receive these broadcast beacons:

- This means small UAS airspace utilization is low and there is no need for automated air traffic management service. If there are no commercial operations underway to monitor these broadcast beacons, this means small UAS are most likely controlled by humans - which can “see and avoid” and should take actions to avoid other craft in flight.

[34] https://www.faa.gov/news/fact_sheets/news_story.cfm?newsId=20516

- If in remote locations (most of the United States land mass outside about two to three dozen large metro areas), these beacons do not need to be closely monitored as these flights are a risk to no one.
- If law enforcement needs to collect data, consistent with COPPA, they can set up their own broadcast beacon ID receivers at special events, such as a game at a stadium, or a public parade, or other areas where they are concerned about security (indeed, the NPRM envisions law enforcement receiving Remote ID directly). These receivers could collect and store the remote ID information including the operator ID under the "one-time use" exemption of COPPA.
- Airports could set up broadcast beacon ID receivers if concerned about illegal flights close to the airport. Such receiving systems could readily pick up beacons from miles away from drones flying at higher altitudes of 50', 100', 200' or more - the only drones we need to care about. High gain antennas would readily receive transmissions at great distances. I previously worked for Vivato Wireless where we built smart antenna panels that provided high speed Internet connections to notebook computers with standard, low powered, internal Wi-Fi - *located miles away, demonstrating the ability to receive even weak signal beacons at great distances.*

In addition to using airport located ID receivers, the existing LAANC system may be used to receive authorization and logging of flight operations within the airport traffic area. Indeed, LAANC suffices as a system based on training, trust and enforcement and should be used to certify operations of R/C model aircraft, instead of the FAA's byzantine FRIA concept.

This proposed solution resolves:

1. the COPPA conflict,
2. Eliminates 4th Amendment privacy issues regarding the government logging flights inside private homes or personal properties (see comments on this elsewhere in this filing)
3. Continues to provide information for air traffic management services

- Puts the burden of cost on the specific air space users that benefit from air traffic management services
- Dramatically lowers costs and complexity to recreational users
- Increases the likelihood of compliance
- Continues to utilize Remote ID so that all craft owners can be identified in flight by law enforcement
- Enables direct monitoring and logging via local ID receivers installed, as needed, at airports or by law enforcement at special events
- Removes the complexity and difficulty of Internet access requirement in numerous and large areas that have no viable Internet access available.
- Because Part 107 prohibits operations by those under 13 (or 16) by virtue of the Part 107 age requirement, this (largely) eliminates the likelihood of the Remote ID USS collecting data on protected youth.
- Since the ID is a simple transmission using U.S. Part 15 frequencies that are also typically available for unlicensed devices internationally, this leads to a potential global standard solution based on simple technology and using smart phone apps as generic receivers.

NPRM Appears to violate the 4th Amendment and Other Laws

Significant issues arise from the NPRMs requirement to log flights conducted inside buildings, including private residences, into an Internet database accessible to law enforcement. The government is requiring the installation of a surveillance device inside homes, which conflicts with the 4th Amendment, and possibly violates laws that prohibit collecting the electronic communications of U.S. citizens. In situations where indoor flight is conducted by children, this appears to violate the Children's Online Privacy and Protection Act.

4th Amendment Issues

If you fly a small UAS inside your home, and if you can get a GPS signal, then your small UAS is required to transmit its location and operator information via serial number - including name, operator's location and contact information - from inside your home into a government managed - or third-party managed on behalf of the government - database. This would include instances when the craft is operated by a minor child. If Internet access is available, this data must be logged in a Remote ID USS in real time. The FAA is requiring us to enable real-time monitoring and surveillance of activities inside our own homes, via an Internet database accessible to law enforcement in real time.

My own home is a single floor house with blown in attic insulation, not aluminum foil backed insulation. I can receive GPS signals inside my home. In fact, using Google Maps on my phone, the GPS information reveals which room I am located in, inside my home. This is highly precise location information, and this precision is frightening when we consider it may be tracking a child inside the home – in violation of COPPA.

As stated by the Pacific Legal Foundation,

> "In short, the government isn't allowed to record a person if that person is somewhere where they can reasonably expect that their conduct will remain private…."[35]

Yet this is precisely what the NPRM requires - that the government, via third party proxy, will record activities inside the privacy of our own home, down to the level of individual rooms, and in an area where we have a reasonable expectation of privacy.

If the 4th Amendment issue is not apparent, consider this in a different context: Assume the Federal Communications Commission requires remote ID of televisions. Each time someone turns on the TV, the FCC requires that you log in an FCC Internet database the location of the TV, the name of the operator and the channel being watched. Do you see the 4th Amendment problem now?

Outsourcing the data collection to a 3rd party does not resolve the 4th Amendment issue. If it did, then local police could hire private investigators to infiltrate homes without warrants - going through a proxy does not resolve the 4th Amendment problem.

- One solution, as with the issues involving COPPA, is to use a "broadcast ID only" - and not mandate logging into an Internet database.

- Another is to provide a way to designate indoor flight – without reliance on GPS and position reporting.

[35] https://pacificlegal.org/with-5g-arriving-the-supreme-court-needs-to-rule-on-what-digital-privacy-means/

- Another alternative is for the FAA to ban indoor flight of drones; however, the FAA does not have authority to regulate indoor airspace. Consequently, the “indoor use only” exemption applies. However, that still does not resolve the problem when someone flies a compliant small UAS indoors – the logging continues to occur.

5th Amendment Issues

The NPRM provides no mechanism - such as disabling remote ID or GPS location - for which indoor flights can be completed while complying with the proposed rules. By banning use of our indoor private property – by rules whose benefit is for someone else - the FAA's NPRM may be violating the 5th Amendment prohibition against the taking of private property without compensation, for the benefit, as described in the NPRM, of industrial applications of the outside airspace. Thus, this might represent a "regulatory taking" of private indoor airspace for the purpose of a public function. This item is left as an exercise for lawyers to sort out.

Foreign Intelligence Surveillance Act Issues

The Foreign Intelligence Surveillance Act prohibits government agencies from generally intercepting and collecting the electronic communications of American citizens. See 50 U.S. Code Sec. 1801[36].

> Definitions. (f) Electronic surveillance, (1) the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes;

and

> (3) "the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States; …"

The NPRM on Remote ID mandates the intentional acquisition and recording of radio communications by American citizens, in various scenarios, “in which a person has a reasonable expectation of privacy” such as flying a small UAS inside their home, garage, backyard or inside their business. The NPRM may violate the Foreign Intelligence Surveillance Act.

State Laws

[36] https://www.law.cornell.edu/uscode/text/50/1801

Many states – but especially California – have state laws on information privacy[37]. In California, consumers have a legal right to request deletion of personal information collected about them (similar to COPPA but the California rule applies to everyone including adults). This is in direct conflict with the FAA's mandate that Remote ID USS retain data for six months, both in terms of Remote ID flight data but also including aerial imagery and other data recorded by the Remote ID USS. California also has a law similar to COPPA that permits "permits minors to remove, or to request and obtain removal of, content or information posted on an Internet Web site, online service, online application, or mobile application".

Recommendation

- American citizens have a "reasonable expectation of privacy" in their own homes. The requirement to send electronic communications defining our indoor activities is analogous to government spying on our activities inside our home. The only way around this is for the sale of "indoor use only" small UAS or to enable a configuration option to fly small UAS indoors, without data collection.

- Note – small UAS sold as "indoor use only" implies that anyone who wishes to also fly outside must purchase two small UAS. As this is potentially expensive, most people will fly their "indoor use only" craft outdoors. The logical solution is to enable an "indoor use only" configuration setting, which not only allows flight when GPS is not available, but also restricts Remote ID to broadcast beacons only.

- Without these changes, the FAA is mandating the collection of electronic communications concerning a model aircraft, even a toy operated by a child, from the privacy of our home in violation of the 4th Amendment and for children, a violation of COPPA and state laws.

The FAA might argue that by flying we are thereby giving consent. But that argument fails by analogy:
- By using a telephone, we are granting consent to the government to listen to our phone call?
- By using email, we are granting consent to the government to collect our email?
- By using a TV, we are granting consent to the government to log our viewing habits?

Alternatively, the FAA might argue that indoor flight will be banned, thereby eliminating the 4th Amendment issue. But the FAA has no authority to regulate the indoor airspace.

- The only workable solution is to enable all small UAS to have an "indoor flight only" mode of operation, and to include mechanisms to not monitor children or to skip the Internet data logging requirement entirely for recreational small UAS. *Indeed, consistent with all of the problems inherent in Internet data logging, the elimination of mandatory Internet loggings is the only workable solution. Remote ID, yes – logging in the Internet-cloud, No, except for BVLOS flights.*

[37] https://www.ncsl.org/research/telecommunications-and-information-technology/state-laws-related-to-internet-privacy.aspx

This NPRM Fosters Development of Nationwide Aerial Surveillance System

Some commercial interests have stated that business models for Remote ID USS access may be "free"[38]. Typically, when something is free, it means one's privacy is for sale. This implies that "free" Remote ID USS providers will collect additional information from the drone, via the Internet connection – obtaining information that can be sold for profit.

The NPRM says:

> "However, the proposal does not prohibit designers, producers, or operators from including a capability for limited remote identification UAS to broadcast information or data unrelated to remote identification, **such as a camera feed or telemetry data**." Page 97, Section X, A, 2, Paragraph 2

Literally, this means the Remote ID USS may conduct low altitude (100' to 200') high resolution photography of our homes, yards, children, businesses. Imagine the public's perspective when they find out that all small UAS (both industrial and recreational) may be conducting surveillance of their children. Their anger may result in violence to remote pilots who may have no control over this data collection.

The public will not tolerate invasive, high resolution photography of their homes and children from 100' above their homes. As explained earlier in the section on COPPA, enabling parents to contact the Remote ID USS, request review, deletion and suspension of data collection is complex for parents and guardians and implies complexity for the Remote ID USS operator who must map out exclusion zones recognized by their drone fleet customers.

This requirement appears to be enforceable by the Federal Trade Commission per the FAA Reauthorization Act of 2018:

> SEC. 375. <<NOTE: 49 USC 44801 note.>> FEDERAL TRADE COMMISSION AUTHORITY.
>
> (a) In General.--A violation of a privacy policy by a person that uses an unmanned aircraft system for compensation or hire, or in the furtherance of a business enterprise, in the national airspace system shall be an unfair and deceptive practice in violation of section 5(a) of the Federal Trade Commission Act (15 U.S.C. 45(a)).

The "message elements" transmitted by a Remote ID beacon broadcast do not identify the Remote ID USS in use. If a parent observes a drone flying over their backyard, in order to comply with Federal and State laws, the parent needs to be able to identify the drone (using a serial # or Session ID) *and the Remote ID USS they are using* so they can request a review and possible deletion of protected information recorded about their children playing in their backyard. An identifier for the Remote ID USS should be included in the message elements that are present in a Remote ID broadcast.

[38] https://kittyhawk.io/blog/separating-fact-and-fiction-about-the-remote-id-for-drone-nprm/

This national surveillance system is untenable and unacceptable to everyone. At a minimum, all American's must have access to information about those who are photographing their children.

This NPRM Threatens National Security

In January 2020, the U.S. Department of the Interior grounded all of its foreign made drones over concerns that such drones could hypothetically conduct surveillance and transmit intelligence data over the Internet[39]. The US Army grounded its Chinese-made drones in 2017 over fears of their use for espionage[40]. In February 2020, the U.S. Department of Justice accused intelligence officers in China of stealing personal data on 145 million Americans[41] and previously told Americans not to use Huawei or ZTE phones[42]. According to the then Director of the FBI, the use of connected technologies "…provides the capacity to maliciously modify or steal information. And it provides the capacity to conduct undetected espionage."[43]

While the left hand is citing threats to national security of Chinese-made drones[44], the right hand is simultaneously mandating all drones be connected to the Internet in real time, most of which will be made in China.

There is no way for a user to know if this connection will be used to transmit surveillance data to a third party. Prior to this NPRM, if the device never connected to the Internet, you could be sure no data transmission took place. Now, users have no way to know and no way to prevent unauthorized surveillance and spying via their small UAS platform. Members of the general public, who may find their own homes and children photographed from above, have no way of knowing where this data is stored and who will have access to it.

In spite of the government's own fears of using electronic consumer products for surveillance by China, the FAA is proposing to mandate surveillance by drones mostly made in China – which will be interfaced to the Internet and remote data collection services – the exact scenario one hand of the government fears while the other hand mandates it.

Mandating real-time surveillance conducted by foreign-made drones is wrong from a national security standpoint. For example, there are a number of Internet-connected home security cameras that enable a homeowner to view their home remotely. Because these units are made in China, and because they store imagery, temporarily, in servers that may be located in China, some consumers are concerned they may be secretly watched. High tech companies admit they had staff listening to voice recordings inside people's homes, ostensibly to improve voice recognition capabilities[45]. We know this listening in was conducted by staff in foreign countries.

[39] https://dronedj.com/2020/01/29/interior-department-grounds-drone-fleet-with-new-order-issued-today/
[40] https://www.defenseone.com/technology/2017/08/us-army-just-ordered-soldiers-stop-using-drones-chinas-dji/139999/
[41] https://www.nytimes.com/2020/02/10/us/politics/equifax-hack-china.html
[42] https://www.theverge.com/2018/2/14/17011246/huawei-phones-safe-us-intelligence-chief-fears
[43] https://www.cnbc.com/2018/02/13/chinas-hauwei-top-us-intelligence-chiefs-caution-americans-away.html
[44] The U.S. government has made several, well publicized claims that China-made drones represent a threat to our national security but has not provided any public evidence that supports these claims.
[45] https://www.cnn.com/2019/08/19/tech/siri-alexa-people-listening/index.html

With this NPRM, the FAA is mandating a national security nightmare as all drones will be required to be connected to the Internet in real time and citizens will have no way of knowing what data is being collected and who has access to that data.

Recommendation

- This surveillance system is why the FAA must not mandate an Internet-based data collection system for all drones, particularly consumer products (recreational drones) where consumers have no ability to evaluate if products are used for international espionage.

Is Privatization of UAS Air Traffic Management Permitted?

The NPRM proposes to use the Remote ID USS data for air traffic control services.

In this NPRM, the FAA is mandating that small UAS subscribe to a Remote ID USS, a purpose of which is to provide air traffic management services for air traffic control.

> The FAA is therefore proposing to require the remote identification of UAS to enable the agency to identify unmanned aircraft flying in the airspace of the United States and locate the operators of those aircraft. Remote identification equipment would provide identifying information for UAS similar to how ADS-B and transponders provide identifying information for manned aircraft. **This information would also be essential for the management of the flow of air traffic as more UAS integrate into the airspace of the United States. (NPRM, Page 45)**

A Limited Remote ID small UAS is required "**to land as soon as practicable** when it cannot transmit the message elements through an internet connection to a Remote ID USS." (Page 23).

> Operators of UAS could use remote identification information available from a Remote ID USS or broadcast directly from other unmanned aircraft to know the location of UAS operating nearby. **Such data could be used in UAS detect-and-avoid and aircraft-to-aircraft communication systems to aid in unmanned aircraft collision avoidance.** (Page 51)
>
> If the Internet is available, but the UAS cannot connect to a Remote ID USS, **the UAS would be designed such that it could not take off**. (Page 93)

The FAA defines Air Traffic Control 14 CFR 1.1[46]:

> *Air traffic control* means a service operated by appropriate authority to promote the safe, orderly, and expeditious flow of air traffic.

By the FAA's definitions, Remote ID USS is used as automated air traffic control –authorizing take off, ordering urgent landing and to prevent aircraft collisions. By definition, the Remote ID USS acts as an air traffic control system.

[46] https://www.ecfr.gov/cgi-bin/text-idx?SID=e1a9e3932a3bc1e19e96786680c835ca&mc=true&node=pt14.1.1&rgn=div5

Will there be a fee for this air traffic control system?

The FAA hypothesizes that users will pay a $2.50 monthly fee ($30/year) for compliance with the Remote ID USS. As noted later in these comments, there is no valid estimate of actual costs. Some think it might be free while others might cost $10/month. If any fee is charged, it becomes a fee-for-service, privatized air traffic control system, similar to NAV CANADA, which charges small general aviation aircraft an annual subscription fee per aircraft.

In 2017, Congress was asked to approve the "privatization" of air traffic control services, turning over ATC to a non-government entity funded by user fees. This privatization request came from the White House and the airline industry, the latter of which sought expanded control of a non-government air traffic control system. The bill that went to the House exempted general aviation from user fees[47] (which would be like exempting recreational flyers from Remote ID USS fees). Congress, however, rejected this privatization request and has not authorized a user fee based "private" air traffic control system[48].

In the Remote ID NPRM, the FAA is proposing a fee for logging flights in a third-party, non-government run Remote ID USS, for the purpose of air traffic management. This is not the same as FAA contracting out services to third parties (such as contract towers, or maintenance services, which does not require Congressional legislation)[49]. Instead, this is the FAA authorizing independent, third party organizations to charge their own fee-for-service to provide air traffic control services.

Literally, the FAA is proposing a privatized air traffic control system for UAS but does not appear to have authorization from Congress to do this. Congress has not made a distinction between automated air traffic control and human-run air traffic control when it refused requests for the FAA to privatize air traffic control and charge user fees.

If Congress said no to privatizing ATC, under what authority does the FAA set up a privatized ATC for UAS?

Recommendation

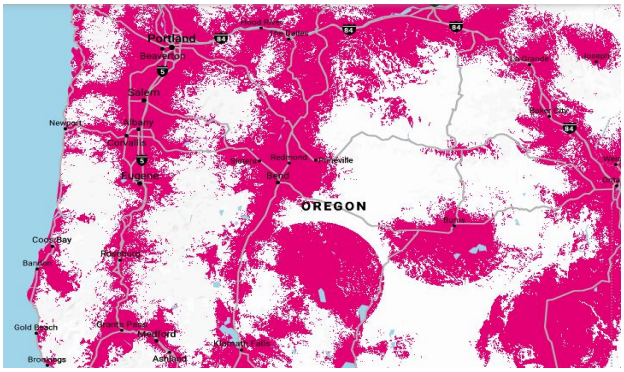
- The NPRM needs to explain the FAA's authorization for a privately-run, potentially user fee funded air traffic control system.
- Lacking authorization from Congress, the FAA needs to run (or contract) the Remote ID USS itself, at no charge to users.
- Or, the FAA needs to seek authorization from Congress for a third-party run, non-government, fee for service privatized air traffic control system.
- Or, the FAA needs to rethink the Internet-based, real time logging, fee for service-based private air traffic management system.

[47] https://thehill.com/policy/transportation/339763-house-panel-approves-proposal-to-privatize-air-traffic-control
[48] https://www.usatoday.com/story/travel/flights/todayinthesky/2017/07/25/senate-panel-rejects-air-traffic-control-privatization/508479001/
[49] Elias, B. (2017). Air Traffic Inc.: Considerations regarding the corporatization of Air Traffic Control. Congressional Research Service. Retrieved from: https://fas.org/sgp/crs/misc/R43844.pdf

Issues with Limited Cellular Service Coverage

I live in the half of a state (Oregon) that has little cellular service coverage (see map, below). The "claimed" coverage map of T-Mobile is about half the state's land mass. T-Mobile nationwide coverage is claimed to be on par with other major cellular services.

White space indicates “no service” and magenta indicates some type of service (but may be weak, intermittent or not providing high speed data services). When we zoom in on the map, we often find that solid color areas are highly fragmented coverage zones or 2G (no data), or roaming without data.



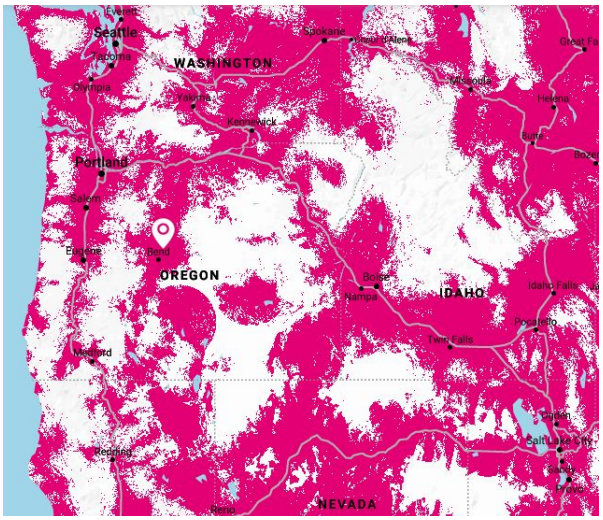
Of course, these maps are a generous interpretation of coverage:

- Some of this "coverage" is provided via roaming agreements where data services are limited or non-existent (2G service only) – but you cannot see this in the high-level view.
- Zooming in to “solid” color areas frequently shows them as spotty coverage.
- Coverage maps lie, as stated in Congressional testimony and based on experience here in Oregon. In a Congressional hearing in early 2019, Rep. Welch of Vermont called coverage maps "bogus": "When I sit here and hear what I believe is your sincere goal to serve rural America and bring 5G to rural America, in Vermont we [currently] have no G…so I’m a skeptic" [50] Another representative questioned rural coverage: "Congressman Ben Ray Lujan challenged T-Mobile CEO John Legere to detail how the deal would incentivize more deployments in rural areas, which have historically failed to attract strong operator investments.”

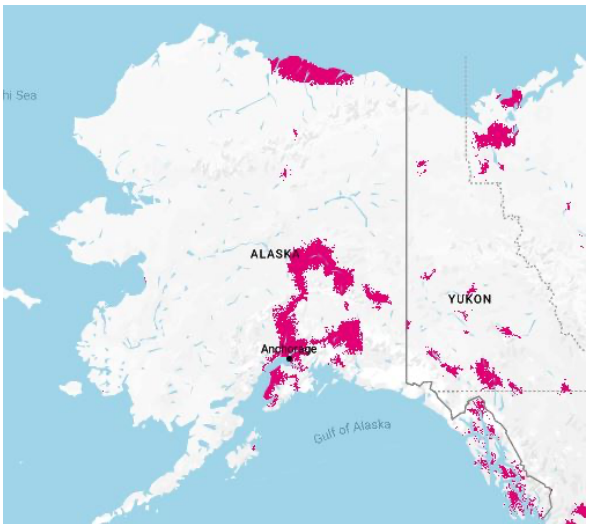
I can locate areas on this map showing “coverage” where there is, in fact, no coverage.

Let’s pull back from Oregon to view coverage in the mountainous west. Vast areas have no coverage (ignoring the bogus coverage problem).

[50] See https://www.mobileworldlive.com/featured-content/top-three/congress-grills-sprint-t-mobile-on-rural-coverage/ and
https://www.theledger.com/news/20190214/these-maps-are-bogus-lawmakers-tear-into-cellular-execs



In Alaska, which is larger than Texas, Montana and California - combined - the lack of coverage is dramatic. AT&T's coverage is slightly greater than T-Mobile's coverage.



Much of this land is public land - USFS, BLM and state public lands that are open to the public and which are open to recreation activities including camping, fishing, boating, hunting, horseback riding, mountain bike riding, off road ATV and motorcycle use and flying of model aircraft, plus commercial activities including ranching, farming, logging, mining and more.

This lack of coverage is another reason that Remote ID for VLOS should be based on simple beacon broadcasts, rather than Internet access. Internet-connectivity should only be required for Beyond Visual Line of Sight operation. *Consumers in these areas will never see drone package deliveries as the population is spread out too far, and the "Value density" is too low for investments in drone deliveries. There is no need for Remote ID USS in these areas.*

The FAA's concept of a low cost Limited Remote ID SUAS requires always on Internet access – and is useless in half of my state. No one will build these, and no one will buy them. A better alternative is that Limited Remote ID is a low cost, VLOS, broadcast-beacon based Remote ID only.

Recommendation

- The FAA's expectation of Internet available in much of the U.S. is not based on reality - and will not be available years from now due to difficult terrain and low population density. It is absurd to suggest mandatory Internet connectivity where so much land mass has no cellular service.

- A far more reasonable solution is to mandate low cost broadcast ID. Internet access/Remote ID USS is only needed for Beyond Visual Line of Sight operations.

- Change the concept of Limited Remote ID to a VLOS, broadcast beacon-bases system. And ditch the arbitrary 400-foot range limit. Our model airfields runway is 450 feet long – with the 400-foot range limit, we couldn't even reach the end of the runway yet this is well within "visual line of sight".

Compliance costs

Section 1 - Cost of Replacing Existing Drones

The NPRM largely bans existing model aircraft, quadcopters and "drones" used by consumers within three years of enactment. Some models will be permitted to fly at FRIAs, for a limited period of time. For flyers that are not now members of the AMA and a local flying club (for example, they may be weekend "park flyers" or fly on their own property), this may add approximately $150 per year (membership fees) to their costs of compliance. This cost does not appear to be included in the FAA's compliance estimates.

Per the NPRM, most consumer level small UAS cannot be updated; the NPRM prohibits retrofitting such craft. If not used at FRIA (with attendant costs), then all of these small UAS and accessories must be trashed and new compliant drones purchased.

> Based on industry information and market research, the FAA estimates at least 93% of the current part 107 fleet and at least 20% of the current recreational fleet would be eligible for retrofits, thus minimizing the costs for operators and producers. (Page 189).

The 20% figure comes from the estimated market share of DJI in the recreational category and the view that DJI products can be retrofitted by DJI (Page 190).

In other words, 80% of the recreational fleet will be thrown away – recreational users bear essentially all the costs of this rule making but see no direct benefits.
The FAA uses an inappropriately low estimate for the number of existing SUAS that would become obsolete:

> The FAA assumes members of a nationwide community-based organization own, on average, two aircraft, which may have an average lifespan that exceeds ten years. (Page 194)

Yet in a footnote to this item, the FAA notes that AMA has 200,000 members with each member having an average of over 9 aircraft, totaling 1.8 million aircraft. A figure vastly larger than the estimated 1.4 aircraft per user of the recreational community. Additionally, there are many more flyers ("park flyers") who are not members of the AMA.

The FAA estimates an average small UAS life span of 3 years based on an expectation of frequent upgrading of products and uses this as the basis for the three-year grace period (page 194).

This 3-year estimate is unrealistic. In 2019, I purchased a used Yuneec Q500 drone that was three years old when I bought it, plus I purchased three additional batteries, and later bought a new camera for it. Unfortunately, shortly after I made this purchase, the FAA released its NPRM in which it states the average life span is 3 years and my drone is already considered dead. Really?

Section 2 - Cost Model Low Balls Costs of Aircraft

The FAA's model appears to low-ball the investment in existing drone aircraft in order to minimize the estimated costs of compliance.

> Based on the FAA fleet forecast for small unmanned aircraft, the FAA estimates the average number of aircraft owned by each part 107 operator to be 2.4 and the average number owned by each recreational flyer to be 1.4 aircraft. (Page 193)

As there is no inventory of existing craft, by recreational users, these estimates are little better than numbers pulled from hats.

The FAA assumes that consumers have a small number of drones and assumes a low dollar value for these drones. *The FAA neglects to include the costs of additional batteries, battery chargers, tools and other items that may be unique to each aircraft.*

For my own small UAS, I typically have 2 to 4 batteries from OEM or non-OEM third party suppliers. At the 4-battery level, my investment in batteries may be greater than the cost of the aircraft, yet this cost is ignored in FAA estimates.

Section 3 - Aircraft Registration Fees

The FAA desires a registration fee for each individual craft. While the proposed fee is minor on a per craft basis, there are many individuals that have multiple aircraft and these fees add up. For the recreational model flyer, the AMA has said their typical member has about 9 aircraft. This becomes $45 plus the cost of AMA and local club (FRIA) membership at about $150, plus potentially another $30/year (FAA estimate) for Remote ID USS services, and we are now over $200 per year in "service" fees.

There is no need to charge a fee for each individual aircraft. It is an extremely simple software issue[51] to continue with the pilot registration system and for each pilot to add each unique aircraft serial number linked to their inventory.

[51] From my bio, I know a few things about software projects.

The FAA is registering each aircraft individually because that made sense for full size manned aircraft. This makes no sense for fleets of tiny model aircraft, adds complexity, costs and reduces the likelihood of compliance.

Section 4 - Annual Subscription Fee for Air Traffic Management Service

The NPRM requires most small UAS flyers to subscribe to an Internet-connected Air Traffic Management Service.

> "The FAA further discusses some of its assumptions related to Remote ID USS business models in the accompanying Regulatory Impact Analysis, where it assumes (while acknowledging significant uncertainty) the average publicly available Remote ID USS will charge $2.50 as a monthly subscription ($30 annually) cost to users of its service." (Page 102)

The basis for the $2.50 per month estimate is wrong. The FAA drew this estimate from LAANC subscription prices and assumed that LAANC and Remote ID USS are identical. The FAA then averaged sample prices of $0 and $5 together to come up with a $2.50 estimate. (The FAA assumes the subscription cost will be a flat rate and will not vary by the number of UAS operated by an entity. UAS service providers may charge additional fees for other services not related to this proposed rule.)

The basis for this $2.50 per month estimate is faulty.

From an IT perspective, the requirements of LAANC are entirely different than Remote ID USS. The former collects a one-time data record from the user and logs it. No personally identifiable information is collected. Remote ID USS, on the other hand, is a real time data logging service, obtaining records generated at a once per second rate, which are then logged in the cloud, accessible on the back end, in real time, to multiple users. These records are associated with personally identifiable information making them subject to privacy laws and privacy compliance costs and a public interface for access to the retained data.

Simultaneously, there is a Remote ID USS “back end” that is delivering real-time location data to other users and air traffic management systems.

A Remote ID USS is far more complex than LAANC and has significantly higher network bandwidth and transaction costs.

The FAA's attempt to compare LAANC to Remote ID USS fails. The $2.50/month estimate is based on a faulty assumption the Remote ID USS is identical to LAANC when clearly, it is not identical.

Section 5 – NPRM Mandates purchase of a smart phone and cellular data service

As explained earlier in these comments, the FAA proposes use of cellular data, Wi-Fi or other Internet access to send operational data to a Remote ID USS. But as described earlier, the use of Wi-Fi is not possible when the goal is low cost aircraft. A smart phone cannot simultaneously connect to the small UAS Wi-Fi Access Point and to a separate Internet connected Access Point. The effect is that the FAA is mandating purchase of a smart phone and sufficient cellular data service plan for so-called “low cost” SUAS not flown at a FRIA. The cost of smart phones and cellular data service is not included in the costs

of compliance. I am sure that VerizonTMobileAT&TSprint love that the FAA is mandating purchase of their service.

Section 6 - The Advisory Committee Notes on Compliance

The Advisory committee recognized that most flyers wish to be compliant, but the likelihood of compliance depends on costs and ease of achieving compliance.

The Advisory Committee wrote:

> "The assumption is that most owner/operators want to be compliant. The likelihood that they will comply depends upon the relative ease of complying, the perceived costs of complying, the penalties for non-compliance, and any potential rewards from compliance. One could think of the "Likelihood of Compliance" to include the "Motivation to Comply" along with the "Deterrence of Compliance"[52].

Unfortunately, the FAA ignored the Advisory Committee and chose a path of near maximal costs that requires throwing away existing aircraft, batteries and other accessories, a per aircraft registration system that unnecessarily requires a fee for every aircraft one owns (even though this is a simple database problem that does not require a per aircraft fee), an annual Remote ID USS subscription fee. Use of older aircraft is permitted only at FRIA fields which will generally cost on the order of $150 per year (AMA and local club fees).

The result is the FAA will see low compliance. A better approach would be to make reasonable compromises that achieve nearly all the same security and safety goals at far lower costs (described in our Recommendations section at the end of this document).

Recommendation

There are numerous errors in the estimated costs of compliance that enabled the FAA to estimate lower costs than will be found in the real world.

- The costs of compliance left out potentially requiring a smart phone (if not currently owning a compatible one), possibly updating a smart phone (requires Android 5 or newer) and requiring a more expensive cellular service plan when it covers an area that a less expensive plan does not cover.
- The costs of compliance left out the cost of accessories such as batteries, battery chargers and tools that may need to be disposed of once the FAA grounds existing non-compliant craft in three years.
- The costs of compliance left out the requirement that “park flyers” purchase AMA and local flying club memberships to use their existing model aircraft at FRIAs.

The actual costs of compliance will be significantly greater than that estimated by the FAA.

---

52 https://www.faa.gov/regulations_policies/rulemaking/committees/documents/media/UAS%20ID%20ARC%20Final%20Report%20with%20Appendices.pdf

To reduce the costs of compliance, the FAA should take several steps:

- The 3-year grace period is arbitrary, not supported by data and is unreasonable, considering the low risk of continued use. *Aircraft operated safely today do not become threats to national security due to their age!*
- There must be an option to attach a remote ID device to existing aircraft. There is no reason to prohibit this, particularly since non-compliant SUAS will, in fact, be sold, forever (per the "indoor use only" exemption, and that the FAA cannot stop the sale of non-compliant craft which will be widely available). Why not make it easy to comply with remote ID by adding an upgrade to existing craft?
- The FAA's per aircraft registration system is unnecessary. This is a software issue and is not required. There is no reason I cannot register as pilot and then list my inventory of aircraft and list each aircraft's serial number. There is no reason to mandate individual aircraft registration and charge separate fees. It would be far simpler to continue to register by pilot, and then have each pilot register their aircraft. This is a simple database issue. Keeping this simple will ensure that small UAS are actually registered.
- The FAA's estimated fees for air traffic management are based on a mistaken comparison of LAANC to Remote ID USS even though they are completely different.
- In 2017, Congress chose not to authorize the FAA to privatize air traffic control services – it is not clear that the FAA can privatize a fee-for-service air traffic control for small UAS.

The FAA has chosen a path of maximum compliance costs rather than following the advice of its Advisory committee to encourage compliance at reasonable costs. There is no value to the recreational flyer to require Internet connectivity (except for BVLOS). Remote ID broadcast suffices to meet the national security and law enforcement requirements specified by Congress in PL 115-254. There is no need to mandate Internet connectivity.

Environmental Assessment Required

Per the FAA's own documents, it appears this proposed rulemaking requires an Environmental Assessment. I was unable to locate a relevant Environmental Assessment for this NPRM.

This NPRM impacts the environment in two ways:

1. A primary purpose of this proceeding is to open the airspace for large fleets of automated drones flying at low altitudes over residential homes and businesses. These fleets have the potential to increase ambient noise levels, to crash into birds in flight, to crash into property causing damage, and to fall from the sky causing injury to humans and animals.
2. The FAA's proposed rules require that millions of existing model aircraft and consumer quadcopters be permanently grounded and likely to be thrown away in trash/landfills.. This includes the large-scale disposal of plastics, composites, Lithium polymer batteries, fuel powered combustion engines, electronic components, servos, motors and more. What impact will this mandated disposal have on the nation's landfills and environment?

I was unable to locate an FAA Environmental Assessment of the impacts of this proposed rulemaking.

The FAA states that the "FAA's efforts to manage airspace capacity and change aircraft routing"[53] may require environmental review. The FAA states that "aircraft noise continues to be the public's primary objection to near-term aviation growth… Noise and emissions will be the principal environmental constraints on NAS capacity and flexibility unless they are effectively managed and mitigated."[54] Yet this NPRM is intended to open the skies to very low altitude flights by thousands of large, automated drones, flying directly over residential areas.

FAA Order 1050.1F, Paragraph 1.8[55] states

> The FAA decision-making process must consider and disclose the potential impacts of a proposed action and its alternatives on the quality of the human environment. In meeting its NEPA obligations, the FAA should seek to achieve the policy objectives of 40 CFR §1500.2 to the fullest extent possible. The FAA must integrate NEPA and other environmental reviews and consultations into agency planning processes as early as possible.

40 CFR Section 1500.2 Policy covers the basic and broad requirements for an environmental assessment:

> (d) Encourage and facilitate public involvement in decisions which affect the quality of the human environment.
>
> (e) Use the NEPA process to identify and assess the reasonable alternatives to proposed actions that will avoid or minimize adverse effects of these actions upon the quality of the human environment.
>
> (f) Use all practicable means, consistent with the requirements of the Act and other essential considerations of national policy, to restore and enhance the quality of the human environment and avoid or minimize any possible adverse effects of their actions upon the quality of the human environment.

Per 40 CFR Section 1500.2. Applicability and Scope, describes the types of FAA activities subject to an environmental assessment:

> The requirements in this Order apply, but are not limited, to the following actions: grants, loans, contracts, leases, construction and installation actions, procedural actions, research activities, **rulemaking and regulatory actions**, certifications, licensing, permits, plans submitted to the FAA by state or local agencies for approval, and legislation proposed by the FAA.

40 CFR Section 1500. Paragraph 1-10.13. Environmental Impact Categories lists a variety of example categories for which an environmental assessment is required. The following categories are relevant both to the issue of disposal of model aircraft grounded by this NPRM, and to the impacts of low altitude autonomous drone flights which are made possible by this rulemaking proposal.

---

[53] https://www.faa.gov/air_traffic/environmental_issues/ared_documentation/
[54] https://www.faa.gov/nextgen/how_nextgen_works/eande_safety/eande/in_depth/
[55] https://www.faa.gov/air_traffic/environmental_issues/ared_documentation/media/Order_1050_1F(07162015_final_version).pdf

40 CFR Section 1500. Exhibit 4-1. Significance Determination for FAA Actions. Under "Hazardous Materials, Solid Waste, and Pollution Prevention", the FAA must consider the impacts if the FAA's actions would:

> Produce an appreciably different quantity or type of hazardous waste;
> Generate an appreciably different quantity or type of solid waste or use a different method of collection or disposal and/or would exceed local capacity;
> Or Adversely affect human health and the environment

Several other categories apply to the effects of low altitude flights on various population groups:

Socioeconomics

- Disrupt or divide the physical arrangement of an established community;
- Cause extensive relocation when sufficient replacement housing is unavailable;
- Cause extensive relocation of community businesses that would cause severe economic hardship for affected communities

Environmental Justice
The action would have the potential to lead to a disproportionately high and adverse impact to an environmental justice population, i.e., a low-income or minority population, due to:

- Significant impacts in other environmental impact categories; or
- Impacts on the physical or natural environment that affect an environmental justice population in a way that the FAA determines are unique to the environmental justice population and significant to that population.

Light Emissions
The degree to which the action would have the potential to:

- Create annoyance or interfere with normal activities from light emissions; and
- Affect the visual character of the area due to the light emissions, including the importance, uniqueness, and aesthetic value of the affected visual resources

Visual Resources / Visual Character
The extent the action would have the potential to:

- Affect the nature of the visual character of the area, including the importance, uniqueness, and aesthetic value of the affected visual resources;
- Contrast with the visual resources and/or visual character in the study area; and
- Block or obstruct the views of visual resources, including whether these resources would still be viewable from other locations

I was unable to locate an existing environmental assessment of these issues, which are required to be investigated per the FAA's own rules.

Recommendation

- The FAA needs to complete the required Environmental Assessment if one does not already exist.

Amateur Built Regulations Stifle Innovation

I have met EAA members who built newly designed aircraft but first test flew their designs as scale R/C models. One, for example, was a retired Boeing engineer who built a delta-wing "flying boat" aircraft and showed it off at the Arlington, Washington fly-in. He test flew his innovative concept aircraft as a scale model before beginning construction of the full sized aircraft; the scale R/C model was on display at the fly-in.

There are several Youtube channels where hobbyists are creating innovative flying craft. for example, check out youtube.com/BPS.space and his "Sprite" electric ducted fan craft, currently test flown in his driveway. This NPRM would isolate testing at remote FRIAs, which will gradually be eliminated, under rules that will eventually ban home designed and constructed aircraft. This NPRM is a direct threat to U.S. innovation.

The NPRM's "50%" rule essentially eliminates amateur built model aircraft. The typical home built model aircraft fabricates a fuselage but purchases motors (gas, turbine or electric), servos, propellers, batteries, micro controllers with control software, flight control receiver and flight control transmitter. Under this rule, almost no one will qualify for the "50%" rule effectively banning home construction of model aircraft, an activity that has been safely undertaken for 90 years.

The FAA proposes to eliminate FRIA fields entirely, over time:

> After that date, the number of FAA-recognized identification areas could therefore only remain the same **or decrease**. **Over time, the FAA anticipates that most UAS without remote identification will reach the end of their useful lives or be phased out. As these numbers dwindle, and as compliance with remote identification requirements becomes cheaper and easier, the number of UAS that need to operate only at FAA-recognized identification areas would likely drop significantly.** (Page 174)

The FAA's intent is that home building and custom one-off construction are eventually ended. The FRIA concept, and the limitations on construction, eventually eliminate custom-built drones used in agriculture, wildlife biology, geology, filmmaking and other "non-aeronautical" business functions and research.

This proposed ban does not lead to increased safety. As noted repeatedly in my comments, bad actors will have a readily available supply of low cost, non-compliant Remote ID small UAS. Consequently, these restrictions on law abiding, safe remote pilots make us no safer, but harm youth STEM programs, harm innovation, harm research and harm American business competitiveness and public safety.

It is notable that both Neil Armstrong and Burt Rutan got their start in aviation as young R/C model aircraft builders. This NPRM means we are less likely to see such incredible aviation and space innovators in the future.

Recommendation

- The FAA's proposed rules essentially kill small scale aeronautics innovation – and kill the use of custom developed small UAS for non-aeronautical research projects and business functions. Even if such custom craft qualified under the 50% rule, they could only be flown at a diminishing number of FRIAs – *which are not the location of the research or business projects*.
- Better is to permit the installation of a Remote ID unit onto homebuilt aircraft.
- Alternatively, permit the development of "core" kits that include only basic functionality and Remote ID – and to permit customization around this core. In this way, traditional home building may continue, and traditional custom built/one-off SUAS for business and research applications may continue.
- Eliminate the FRIA concept and instead allow the use of LAANC (which works fine today) to notify the FAA of flights and allow the use of "bolt on" Remote ID for existing aircraft.

Restrictions on Custom Built Model Aircraft Stifle Non-Aeronautical Research and Business

The FAA proposes an exemption for "aeronautical research" custom SUAS building – but with an unknown level of bureaucracy requiring application to the FAA for permission. This exemption, however, does not apply to other types of research. Our flying club was approached by members of a bird sanctuary interested in designing and building their own small UAS for use in raptor research. Under this NPRM proposal, no such craft could be developed *and flown where the research project is undertaken* as custom built aircraft could only fly at FRIA sites. There are numerous examples of non-aeronautical research that will be shut down by this NPRM – forestry, wildlife biology, geology, GIS, agriculture. I have a family member who is a consulting scientist. Her firm uses a customized $5,000 drone, out fitted with specialized sensors, for research in agriculture, hydrology and other fields. Under this NPRM, this drone would be banned as it will never be a manufactured product – and no one can afford to meet the FAA's strict requirements for manufacturing a one-off product.

Recommendation

- Permit the installation of a Remote ID unit onto homebuilt aircraft.
- Alternatively, permit the development of "core" kits that include only basic functionality and Remote ID – and to permit customization around this core. In this way, traditional home building may continue, and traditional custom built/one-off SUAS for business and research applications may continue.
- Eliminate the FRIA concept and instead allow the use of LAANC (which works fine today) to notify the FAA of flights, and allow the use of "bolt on" Remote ID for existing aircraft

No Method to Report Stolen or Sold Small UAS

The NPRM repeatedly points to the need for Remote ID for law enforcement to track the operator of the small UAS. One of the Remote ID message elements is a unique serial number associated with the operator of the craft.

A criminal may readily steal a small UAS (just as they steal any other item) and then use that craft in acts of crime or civil disobedience. Police would intercept the Remote ID and pursue innocent individuals.

There is no mechanism detailed in the NPRM for how to report a lost or stolen small UAS and have that information stored in the UAS registration database.

If I sell my SUAS, do I login and say I no longer own it? Who provides the identity of the new purchaser? How does this information get authenticated?

I am guessing the FAA does not want to have a "bolt on" add-on Remote ID unit for model aircraft because of fears that it would be tampered with, leading to incorrect identification of an aircraft. However, the same problem occurs when a model aircraft is stolen and then used by a nefarious bad actor. That is not a reason to prohibit add-on Remote ID transponders.

Recommendation

The FAA needs to specify that its aircraft registration system has a feature to report stolen and sold aircraft, and how this will work.

Relative Risks of Small UAS Operations

To justify an expansive, complex and expensive regulatory regime for recreational flyers, the FAA, starting on page 54 of the NPRM, cites alleged drone sightings including one ten miles (or possibly 17 miles – it's so vague it mutated) away from the Newark Airport, and the 2018 Gatwick Airport scenario, and other incidents outside the United States. There was never confirmation that drones were involved in the Newark instance, and it was not close to an airport. This "sighting" came weeks after the Gatwick incident –since Gatwick every plastic bag blowing in the wind is a "drone"and every light in the night sky is a "drone".

At Newark, ***"Industry experts say pilots probably saw something in the air but doubt it was a drone***"[56] The FAA omits this exculpatory information from its NPRM.

The Gatwick incident did not involve consumer drones:

> Sussex Police said it was not terror-related but a "deliberate act" of disruption, **using "industrial specification" drones**[57].

The Police said on their Twitter account – these were not hobby drones but drones just like the ones Sussex Police itself flies. Most of the media then proceeded to illustrate their articles with photos of toy quadcopters. Some media reports said the disruption was due to "toy drones". In fact, the FAA omits that the only confirmed drones flying over the Gatwick Airport were those operated by the Sussex Police themselves, and that the police admit that many alleged sightings were of Police drones.

> "Some of the sightings of drones which kept Gatwick Airport on shutdown may have involved the police's own craft, a senior officer has admitted."[58]

[56] https://www.washingtonpost.com/transportation/2019/01/23/did-pair-drones-interfere-with-flights-newark-airport-or-was-it-something-else/
[57] https://www.bbc.com/news/uk-england-sussex-46623754
[58] https://www.rte.ie/news/world/2018/1229/1019460-gatwick-drone-police/

The Sussex Police has 40 officers trained in flying drones for police work and a fleet of expensive Aeroyon industrial drones (about US$100,000 *each*[59]) plus DJI Matrice drones that fit the description of the "industrial specification" drones allegedly seen. The Police flew their own drone fleet over Gatwick looking for the alleged drones – but their drones have no unique visual identification and cannot be distinguished from alleged illegal drone flights.

As summarized at Wikipedia[60]

> No videos or photographs of the drone were handed to the police. The lead investigator from Sussex Police questioned whether there had been a drone at all. Giles York, Chief Constable, later said police thought that original sightings were of an unauthorised drone, but it was possible that later sightings may have been of a drone used by Sussex Police.

During the period of the initial alleged drone sighting, the weather was windy and rainy – not the conditions in which drones are likely to be flown. Gatwick was said to have over 140,000 people pass through the airport on the first day of this event (holiday travel). The airport employs 21,000 people. Police and media both set up 24 x 7 stake outs, with the police employing military grade anti-drone technology. Yet there was not a single useful photo or video or confirmation of the alleged drone.

All of the above exculpatory information is omitted from the FAA's NPRM argument on drone risk.

The week before Gatwick, there was widespread publicity of a collapsed nose cone on an Aeromexico flight landing at Tijuana with media, including the NY Times, falsely reporting this was due to a drone strike[61]. Five months later, we learned the nose cone collapsed due to a failed repair job done previously[62]. No drones were involved.

Another example cited by the FAA involved a drone dropping leaflets over a crowd. Leaflets. And the hypothetical safety hazard of the drone falling out of the sky on to people. The news report cited by the NPRM was far more concerned about the inflammatory rhetoric of the leaflet than the drone itself. This was not a big, scary drone threat. Again, a major point omitted by the FAA.

The FAA cites a drone that flew over an MLB game [63] but leaves out that it was flown by … *a child*[64]. Once again, exculpatory information is omitted by the FAA.

Next, the FAA cites drone incidents outside the United States, over which the FAA has no jurisdiction.

The FAA has cited poor quality, unconfirmed, often evidence-free examples as justification yet the FAA intentionally:

- *Omits important facts and exculpatory information*

---

[59] https://www.sussex.police.uk/police-forces/sussex-police/areas/au/about-us/governance-and-processes/drones-unmanned-aerial-vehicles/
[60] https://en.wikipedia.org/wiki/Gatwick_Airport_drone_incident
[61] https://www.nytimes.com/2018/12/20/world/europe/gatwick-airport-drones.html
[62] https://www.bloomberg.com/news/articles/2019-05-30/drone-impact-ruled-out-in-mexico-incident-with-damaged-jetliner
[63] https://www.usatoday.com/story/sports/mlb/redsox/2019/04/13/drone-fenway-park-juvenile/3457190002/
[64] https://bpdnews.com/news/2019/4/13/bpd-investigation-update-drone-observed-over-fenway-park-recovered

- *Cites references that go to "page not found" errors*[65]
- *Cites incidents outside the U.S. where the FAA has no jurisdiction*

Every example of improper SUAS operation provided by the FAA and occurring in U.S. airspace would have been resolvable with a simple, broadcast-beacon based Remote ID; a complex Internet connected Remote ID USS would add no additional capability.

Many of the examples are on par with the child's fear of "monsters under my bed".

As justification for the FAA's NPRM on Remote ID. The NPRM claims that "*Remote identification would also aid in preventing terrorist attacks*" (Page 56). Because terrorists will definitely use fully complaint drones as non-complaint drones would never be available, and terrorists would be incapable of building their own from widely available parts, instructions, and YouTube videos – or because terrorists are just too stupid to buy non-compliant drones online. Of course.

Remote ID is a fine idea to reduce "run of the mill" incidents – no problem with that - but arguments suggesting Remote ID will stop terrorists are absurdly stupid.

Gatwick resembles the mass hysteria of the Dec 2019/Jan 2020 reports of fleets of drones flying over Colorado, then Nebraska, then North Carolina and California. These sightings were subsequently determined as primarily due to mass hysteria[66]. Remote ID will not play any role in eliminating mass hysteria – indeed, *if you see an imaginary drone lacking an imaginary Remote ID – this is obviously a conspiracy of secret drone flights!*

Years ago, any unrecognized object in the sky was called a "UFO"; today, we no longer have UFO sightings. Instead, everyone jumps to the conclusion that it's a "drone". Actual evidence is not required, as illustrated by the FAA's own NPRM.

It is unfortunate the FAA cites poor examples lacking in confirmation, omits critical facts and cites non-existent URLs, as the evidentiary basis for regulation. The FAA's arguments on public safety are weak when examined in detail. (If I had time, I would look at all of them in detail but the FAA has denied requests to give the public adequate time to review this complex rulemaking proposal.)

As of today, no one has died due to quadcopters.

---

[65] The following references, cited by the NPRM, go to "page not found" errors. (1) https://www.justice.gov/usao-ndca/pr/sacramento-area-resident-charged-flying-drone-over-nfl-games-violation-%20national-defense, (2) https://www.washingtonpost.com/transportation/2019/01/22/drone-activity-halts-air-traffic-newark-liberty-international-airport/?noredirect=on&utm_term=.c0e920a9e756, (3) https://www.theguardian.com/uk-news/2018/dec/21/gatwick-airport-reopens-limited-number-of-flights-drone- disruption, (4) https://www.justice.gov/usao-mdga/pr/illegal-drone-operator-sentenced-attempting-drop-drugs-georgia-state- prison

[66] https://www.vice.com/en_us/article/884xv3/the-colorado-mystery-drones-werent-real

- To put that in context, consider that there were 14,400 aircraft collisions with birds at just 700 of the 15,000 airports in the U.S. in 2017[67]. 285 people have died in aircraft crashes since 1988 due to bird strikes. *0 people died due to drones*.

- In 2017, nearly 40,000 people died as a result of gun-related injuries[68]. No one has suggested real time, Internet-based tracking of firearms. *Meanwhile there were 0 deaths due to drones.*

- Nearly 700,000 hit and run injury accidents have occurred every year since 2006, according to AAA[69]. No one has suggested installing Remote ID on vehicles and establishing a real-time tracking system of every vehicle in the United States. *Meanwhile, there were 0 deaths due to drones.*

- Over a five-year span, the FAA identifies 14 "incidents" involving "drones". Compare that to the number of safety incidents involving manned aircraft, which are vastly fewer in number. In the week following the release of this NPRM on December 26, 2019, 13 people were killed in small aircraft crashes (*none involving drones*).

- In 2018 and 2019, 346 people were killed by the FAA having certified an unsafe Boeing 737 MAX. *Meanwhile, there were 0 deaths due to drones.*

Congress has already acted to deal with naïve and stupid quadcopter pilots by requiring all recreational flyers to pass a Federal written exam on aviation safety and Federal aviation regulations[70], a point that everyone seems to have forgotten, including the FAA.

Meanwhile, all of the following continue to inhabit the skies without Remote ID:

- Paragliders
- Powered parachutes
- Hang gliders
- Experimental home-built aircraft
- Aircraft flying outside of controlled airspace (ADS-B out not required)
- Model rockets
- Kites
- Widely available "For indoor use only" small UAS
- Widely available small UAS of all types, from Amazon, EBay, Alibaba and numerous other vendors.
- *And birds, yes, the same birds that have killed 285 people since 1988*.

Recommendation

To justify a software-based, government command and control system for all model aircraft in the U.S. the FAA:

---

[67] https://www.faa.gov/airports/airport_safety/wildlife/faq/
[68] https://www.pewresearch.org/fact-tank/2019/08/16/what-the-data-says-about-gun-deaths-in-the-u-s/
[69] https://newsroom.aaa.com/2018/04/hit-run-deaths-hit-record-high/
[70] https://www.zdnet.com/article/new-faa-rules-for-recreational-drone-flyers-introduce-temporary-no-fly-zones-and-a-training-requirement/

- greatly exaggerated the risk of past incidents,
- omitted key details and exculpatory information,
- cited missing references,
- cited incidents outside the U.S. where it has no jurisdiction,
- ignored that Congress has set in motion a Federal written exam requirement for all SUAS pilots
- and failed to place SUAS risk in context with other existing risk.

The FAA's evidence is surprisingly poor for something that is allegedly a big scary risk to public safety. Once this poor support for the "risk" argument is recognized, the need for such heavy handed and draconian regulatory impositions is unjustified.

Software-based Enforcement Prevents Using U.S. Sold Drones Outside the U.S.

The FAA is attempting to solve a poorly-defined claim of "high risks" with a Rube Goldberg regulatory scheme of high cost, complexity and one-size-fits all automated control systems – which fail to prevent bad actors from engaging in mayhem but stifle innovation – and prevent U.S. sold drones from operating in other countries.

The FAA believes it can contain alleged risks by using software to automatically control the operation of all SUAS – moving regulation from a trust and enforcement concept (as is done for all other laws) into enforcement by software. This is similar to the approach taken on the Boeing 737 MAX MCAS – where flight control was handed off to an automated software system, rather than pilots. What could possibly go wrong with such an approach?

This software-based control has another side effect – it likely prevents drones sold in the U.S. from operating outside the United States – where the FAA has no legal jurisdiction. Since compliant drones may not operate if Internet access is unavailable or if a Remote ID USS is unavailable, as is likely the case when flown outside the U.S., then U.S. sold drones cannot take flight. Travelers from the U.S would need to purchase another drone at their foreign destination. This is another cost of compliance that the FAA omits from its analysis.

And of course, they will bring that non-compliant drone with them upon returning to the U.S. Yet another NPRM loophole rendering much of the NPRM moot.

The NPRM Bans Large Paper Airplanes Unless 14 CFR 1.1 is Modified

No one thinks the FAA will enforce rules against large paper airplanes but the definitions used by the FAA do eliminate the use of hand launched large paper airplanes (and balsa wood gliders) greater than 0.55 pounds in weight.

14 CFR 1.1 defines a small UAS as:

- "Small unmanned aircraft means an unmanned aircraft weighing less than 55 pounds on takeoff, including everything that is on board or otherwise attached to the aircraft.

- "Unmanned aircraft means an aircraft operated without the possibility of direct human intervention from within or on the aircraft."
- "Aircraft means a device that is used or intended to be used for flight in the air."

A paper airplane is a device used or intended to be used for flight in the air. It is operated as an unmanned aircraft without the possibility of direct human intervention from within or on the aircraft. A balsa wood model airplane is similarly defined as a small UA.

Unless 14 CFR 1.1 is modified, this NPRM bans the flight of large paper airplanes and hand launched balsa wood model aircraft except at FRIA sites – unless they come from a manufacturer with pre-installed, compliant Remote ID!

The FAA notes it is proposing to add a new definition for "small unmanned aircraft *system*" (adding "system") to distinguish between unmanned aircraft and unmanned aircraft systems. The implication is the rule applies to small UAS and not small UA. If this wording is not added to 14 CFR 1.1, then the NPRM limits the flight of hand launched paper airplanes to FRIA.

Recommendation

This definition of small UAS must change such that it refers to UA that have a control system. If this is not done, then large paper airplanes are banned outside of FRIA. Of course, no one believes the FAA will enforce a ban on large paper airplanes.

Personal Impacts of this NPRM

As noted in terms of compliance costs, it appears this NPRM requires I throw away perhaps $1,500 worth of fixed wing and quadcopter aircraft, extra batteries usable only with these model aircraft, certain battery chargers, and flight control transmitters. This is a bitter moment when it would be simple to attach a small Remote ID transponder to many of these aircraft. I am not happy about the FAA effectively demanding I trash perfectly good, and perfectly adaptable aircraft and their accessories – with no benefit to public safety.

As of this NPRM, I have chosen to suspend purchase of new aircraft, accessories or components as I have no idea if anything I buy would be usable in the future.

I used to fly light aircraft as a private pilot and was interested in becoming current again and resuming manned flight. But I ran into limitations. I long ago suffered an injury in an accident which I have since learned could impact my ability to obtain a medical certificate due to changes in FAA's medical requirements since I last flew. It is my understanding that though I am now well, this old injury requires the local FAA Aviation Medical Examiner to forward the medical application to Oklahoma. To obtain clearance I would have to obtain old medical records that may no longer exist and spend an estimated $5,000 on medical tests (per AOPA) to prove that I healed, which is prohibitive.

As I have a significant interest in aviation, I turned to flying and building model aircraft and anticipated doing this for years to come. Unfortunately, the NPRM has thrown a wrench in my continued involvement in model aviation.

An FAA insider, who is also an R/C model aviation enthusiast, has said that unfortunately, the FAA's actions are likely to bring the 90 years of safe R/C model aviation to an end.

Our local flying club airfield, in use for nearly 30 years, is just under 3 miles from a towered airport. The club has an outstanding relationship with the FAA Tower management and the airport management. The NPRM, however, says 10% of existing AMA-type airfields will not receive FRIA approval because they are located in "sensitive areas", a term the NPRM does not define. Since about 10% of model airfields are located within 5 miles of a towered airport, I presume "sensitive area" means the FAA will shut down use of this airfield for use by traditional R/C model aviation.

I have suspended new investment in model aircraft and anticipate letting my AMA and local flying club memberships lapse when they expire at the end of 2020 or in 2021 under the assumption the FAA intends to shut down the hobby.

Locally, our city government sponsors an annual Aviation Day to share aviation with the local community and to encourage youth to study and consider careers in STEM fields. This event has participation from the local airport, our local model flying club, local FPV quadcopter groups, the EAA, the Civil Air Patrol, local educators including the community college Aviation program, the Parks and Recreation program, Part 107 commercial remote pilots, aviation-related arts and crafts, non-profit organizations, *and a large indoor flying event at an exhibition hall at the County Fairgrounds – where children may safely learn to fly quadcopters indoors inside a large, metal roofed, exhibition hall*. As GPS signals are not receivable inside, this part of the program would be ended (all of the drones used have exceeded 0.55 pounds)[71]. The local community – and youth – become shut out from "hands on" participation.

The message we deliver is that aviation is not accessible to the public – aviation is for corporations and the wealthy.

On a personal level, this NPRM has caused much stress and anxiety. I see the eventual end of R/C model aircraft flying, a sharp increase in costs, the loss of my investment in the hobby, and an FAA whose mindset treats me and other flyers as if we are common criminals who must be baby sat to safely fly a model plane. Meanwhile, the FAA denies an extension on public comments and appears to treat the public with disrespect. We deserve far better from the FAA.

The clear message delivered by the FAA is: *Flight is something to be seen, but not participated in by the public – except by corporations and the wealthy.*

Concluding Summary of Key Points

There are so many problems with the FAA's proposed Remote ID USS Internet logging that the Remote ID USS must be made optional for non-BVLOS operations. Remote ID USS logging should be mandatory for BVLOS flights only.

[71] This needs to be held indoors because it is held in fall, when inclement weather and high wind often prevent outdoor flight. Second, the location is close to an airport, albeit, with a 100-foot LAANC authorizable ceiling for outdoor flight.

Instead, the FAA should use a broadcast-based beacon Remote ID that satisfies the direction of Congress, meets the recommendations of the FAA's own advisory committee, and avoids violations of COPPA and the 4th Amendment.

Here is a summary of key points:

- Congress directed FAA to develop standards for "remote identification" but did not specify what features that requires. Congress wrote in PL 115-254:

  > SEC. 2202. IDENTIFICATION STANDARDS.
  > (a) In General.--The Administrator of the Federal Aviation Administration, in consultation with the Secretary of Transportation, the President of RTCA, Inc., and the Director of the National Institute of Standards and Technology, **shall convene industry stakeholders to facilitate the development of consensus standards for remotely identifying operators and owners of unmanned aircraft systems and associated unmanned aircraft.**

  The FAA has gone beyond the intent of Congress to require mandatory Internet-based logging of all flights, in real-time, and the eventual ending of home built model aircraft. The only Congressional requirement is the development of a Remote ID system.

- The FAA ignored its advisory committee of stakeholders. The UAS-ID Aviation Rulemaking Committee recommended that model aircraft ("limited recreational operations") be excluded from any remote identification requirement. Instead, the FAA developed rules limiting existing model aircraft to FAA-recognized identification areas (FRIAs), which will, over time, be shut down and lead to the eventual prohibition of the flight of homebuilt model aircraft. These steps go well beyond the intent of Congress which directed the FAA to develop Remote ID standards only, and beyond the recommendations of the Advisory committee.

- The FAA has sought to reduce the general public's input in this proceeding. The FAA established an advisory committee that was, per a report from DJI, "stacked" almost entirely with those who stand to benefit professionally and financially from a substantial increase in regulations. The Committee, per DJI, had almost no representation from the general public that would bear the greatest burdens of the regulation. According to DJI:

  > "Less than 7% of the members of the ARC were stakeholders who would primarily face burdens and/or costs from a future Remote ID requirement, while 75% of the members stood primarily to gain from a future Remote ID requirement, either because of their interest in law enforcement tools or in the furtherance of their business objectives or prospective sale of Remote ID technologies or services."[72]

  The FAA then ignored the key recommendations from its own committee of stakeholders.

[72] A DJI Technology Discussion Paper: *Understanding the U. S. Federal Aviation Administration UAS Identification & Tracking ARC Report,* DJI Policy & Legal Affairs Office December 19, 2017

- The FAA released a preliminary draft this NPRM on December 26, 2019, the day after Christmas, at a time when media and resources at organizations are out of the office on vacation, and when the public is least likely to begin work on analyzing the proposal.

- The NPRM went in a direction substantially different from that which the public was led to believe was coming, based on the advisory committee report. Thus, the public was caught off guard and ill prepared to respond.

- The NPRM is a complex rule making proposal, 319 pages in length, with thousands of pages of supporting documents. Yet the FAA provided only 60 days for the public to review, analyze and comment on this proposal. Members of the general public do not have staff available to assign the task of conducting this review – we can only do what we can, in our spare time. The AMA , AOPA and the EAA requested extensions to the public comment period, which the FAA sternly denied using harsh wording saying it did not have time for more public input.

  At every opportunity, the FAA has minimized public input.

- There is no requirement in PL 115-254 that Congress requires real time location tracking databases or that the FAA should eventually ban homebuilt model aircraft.

- The advisory committee suggested having an add-on remote ID transponder upgrade for existing aircraft. There is no technical reason this cannot be done. The FAA (or Homeland Security) mistakenly believes it can limit future small UAS sales to “compliant” only craft and eliminate home built aircraft. However, due to the “indoor use only” problem, the requirements of COPPA to permit deletion of collected data and suspension of data collection, and that many non-compliant craft will be widely available, the FAA is engaged in a fantasy illusion of security and compliance that will never happen. Thus, there is no reason to not permit adding remote ID to existing small UAS.

- The FAA says only compliant aircraft with functioning GPS and Remote ID may be sold. The NPRM says if GPS is not working, then Remote ID is not working, and therefore, the craft may not take flight. This effectively eliminates indoor flight of small UAS – and the FAA is de facto regulating indoor airspace over which it has no authority, but in the case of mines, violates Federal law.

- Alternatively, per the description on Page 8 of the NPRM, vendors may place a “for indoor use” only sticker on the side and sell anything they want as the FAA has no authority to restrict sales, nor regulate indoor airspace. This necessary loophole means the FAA’s attempt to lock aircraft in to compliance, fails.

- In the event that a GPS signal is received indoors, say inside a home, the NPRM generally requires that this flight transmit, in real time, once per second, operator information and latitude/longitude to a third-party Internet database directly accessible to the FAA, Homeland Security and law enforcement. This means the FAA is mandating surveillance inside one's private home, in violation of the 4th Amendment. It may also be in conflict with the 5th Amendment and the Foreign Intelligence Surveillance Act.

- In the event that a child is at the controls (which there is no way to prevent), this results in collection of personally identifiable information including geolocation data in violation of the Children's Online Privacy and Protection Act.

- If a parent discovers the child has flown the craft (with or without permission, indoors or outdoors), the parent has a legal right under COPPA to notify the collector of the data, to request to review that data, and to request to delete that data. COPPA adds significant complexity to the implementation of the Remote ID USS database. Effectively, anyone could request review, deletion and suspension of collected data by asserting their rights under COPPA. This Federal law requirement means the FAA's attempt to force location tracking, fails.

- The Remote ID USS requires the use of an Internet connection which the FAA mistakenly believes is readily available. As our comments have shown, this is not true.

- The FAA defines "Internet is available" in a way that if your cell service does not have coverage, but another service does, then you are required to purchase that additional service. This is completely unacceptable. Taken to an extreme, this could require purchasing satellite-based Internet access. The NPRM's wording makes no sense – why define a Standard Remote ID able to work in a broadcast beacon mode when Internet is not available then?

- The FAA defines Internet is available to include Wi-Fi and appears to view this as a way of reducing costs for those flying a Limited Remote ID SUAS. This however is technically infeasible when the phone is used as a flight controller (to reduce costs). When a small UAS control app running on a phone connects to the craft using Wi-Fi, the craft is configured as a Wi-Fi Access Point – which has no Internet access. The phone has no feasible way of connecting to a separate Wi-Fi AP to gain Internet access; the phone is technically capable of connecting to one AP at a time. The FAA's suggestion to use Wi-Fi for this purpose is technically infeasible. *The overall effect of this is that the FAA is mandating all pilots purchase a smart phone, and all pilots purchase cellular Mobile Data services – because this is the only technically feasible way to simultaneously control the craft over Wi-Fi (e.g. smart phone as flight controller) and to log the operational data to a Remote ID USS.*

- The FAA's NPRM mandates that broadcast-based Remote ID beacon transmissions use the highest power and antenna gain permitted by Part 15 – 4 watts ERP – from SUAS hundreds of feet above ground level. This is not how the FAA intends for Part 15 to be used. The FAA's requirements will increase the noise floor, which reduces the range of reception by other SUAS, will cause interference to other Part 15 and licensed users (who have priority spectrum access), and may cause desense of other SUAS control links when SUAS are flown in close proximity to each other, leading to crashes of SUAS.

- The FAA is badly misinformed on Internet access availability, has written its NPRM to potentially mandate higher cost (if not extremely high cost) Internet access, and has specified a technically infeasible use of Wi-Fi for its intended use for low cost SUAS Remote ID USS operation. In addition, the Internet data logging will, in certain situations, violate COPPA and the 4th Amendment (and possibly additional Federal and State laws and amendments), and establishes a nationwide, aerial-based real-time surveillance system of Americans. The FAA must require an identifier for the Remote ID USS in use to be included in the message elements that are present

in a Remote ID broadcast so that parents can easily identify who has taken and stored low altitude photos of their children.

- The mandatory use of data logging – including potentially other data such as imagery and Wi-Fi signals - into a Remote ID USS, from Chinese-made drones (and others) creates a national security risk. Many government agencies have grounded their fleets of drones with fears they are being used for espionage. In this NPRM, the FAA mandates a nationwide surveillance system of foreign-made drones connected to the Internet and potentially logging all kinds of data into databases. This is insane and a huge national security risk.

- Software-based enforcement of regulations leads to drones that cannot fly indoors, and prevents drones sold in the U.S. from flying in other countries due to lack of Internet access and suitable Remote ID USS. In effect, the FAA is regulating the operation of drones in foreign countries when that drone is purchased in the U.S. Travelers may need to buy a second drone when traveling outside the U.S., an additional cost not included in the cost of compliance. And of course, they will bring that non-compliant drone back into the U.S. upon their return.

- There are so many problems with mandated Internet data logging that this requirement is infeasible – *and creates a national security risk*. The FAA - and other Federal laws and regulations - have established a contradictory set of constraints such that it is not possible to implement this NPRM as defined. This leaves a limited set of alternatives to satisfy the Congressional directive to implement Remote ID.

- The viable solution is to implement a broadcast beacon-based Remote ID system for VLOS and use the Internet Remote ID USS for Beyond Visual Line of Sight operations only.

- As described in my comments, this broadcast beacon ID may be used in conjunction with automated drone fleets relaying received beacons into the Internet, or the use of ground-located beacon ID receivers. This can be constructed in a way to reduce the likelihood of COPPA and 4th Amendment violations.

- That the FAA itself defines Standard Remote ID to operate in a broadcast beacon mode illustrates the FAA recognizes that broadcast beacon ID is sufficient and meets the intent of Congress.

- The rules on Amateur built small UAS prevent the design and development of innovative small UAS for use in non-aeronautical research projects such as wildlife biology, forestry and geology. This is completely unacceptable. This problem can be resolved by continuing to use LAANC to receive authorization for flights by non-compliant aircraft. There is no need to isolate flights to FRIA “reservations”, which are eventually closed and eliminated.

- Requiring drone pilots to spend significant amounts of money to replace existing aircraft, pay registration fees, subscribe to Remote ID USS and smart phone data services, and to potentially pay annual membership fees to the AMA and local flying clubs – in order to fly SUAS in locations far from any risks is a sure fire way to discourage compliance. Since Congress has already directed the FAA to establish a written examination covering aviation safety and Federal Aviation Regulations, for all recreational pilots – *education is the key to safe operation and far*

more effective than expensive and confusing regulations. Safe operation will come from a trained and educated community – not from a software-enforced regulatory scheme that is full of required loopholes.

General Recommendation

To enable indoor flight, to avoid conflict with privacy laws, to avoid creating a threat to national security, to avoid the impossibility of using Wi-Fi as the FAA has envisioned, and to make compliance more likely, the following steps should be taken to implement Remote ID:

- Use Internet-based Remote ID USS for Beyond Visual Line of Sight (BVLOS) operations only, and optional for other operations.

- Use broadcast-based beacon Remote ID for flights within visual range of the remote pilot; use of a Remote ID USS may be optional but not required for VLOS flights. Pilots flying VLOS are able to redirect their flights away from other SUAS, including automated BVLOS flights (which apparently are unable to "see and avoid" birds and objects that may not have a Remote ID broadcast).

- Change Limited Remote ID to broadcast-based ID transmission and eliminate the arbitrary 400-foot restriction (the runway at my former airfield is more than 400 feet long – since our pilot operator location is at the end of the runway, we could not fly to the end of the runway with a compliant aircraft!)

- Use widely available technology such as data embedded in Wi-Fi flight control data streams, or separate Bluetooth 4.2/5.0 broadcasts – which can be easily received by anyone using a smart phone or tablet app without requiring specialized Remote ID receivers. Longer distance reception can be provided using directional antennas or high gain omni-directional antennas at the receiver.

- Limit Part 15 device power to 100 mw (+20 dBm or similar levels) to reduce interference and receiver desense problems.

- Use LAANC authorization instead of FRIAs. LAANC exists and works well. Do not kill off R/C model aviation and home building; do not end youth STEM aviation programs and innovative research in aeronautics *and the use of custom built SUAS for research in other fields of endeavor*.

- Accommodate indoor flight operations by permitting an "indoor" flight configuration without GPS – small UAS would continue to transmit a broadcast-based beacon Remote ID during indoor flight.

- Aircraft flying BVLOS – such as automated drone fleets – could receive broadcast Remote ID from non-Internet connected craft and relay their information into a Remote ID USS for the purpose of air traffic management. If there are no BVLOS drones in the area, this indicates drone traffic is light and that air traffic management services are not needed.

- Enable the addition of a broadcast based Remote ID module to existing small UAS, so that they do not need to be trashed (this is better for the environment). Intel has demonstrated Open Drone ID based on Bluetooth 4.2 and 5.0 that can be received at up to 1 km or greater distance using high gain receiving equipment[73]. DJI has proposed using the Wi-Fi control link to the aircraft as the Remote ID as it is a simple matter to embed the required "message elements" in the data stream, which can be received, in the clear, by a smart phone app. The technology to enable upgrades exists and improves public safety by equipping existing SUAS.

- Eliminate the Limited Remote ID category. It was viewed as a "low cost" entry point that would enable development of a low cost small UAS controlled via smart phone flight controller app and potentially logging via Wi-Fi. However, the use of Wi-Fi for Remote ID USS data logging is technically infeasible for the reasons outlined in my comments. Consequently, this would require a mobile phone and Mobile Data service, negating the presumed cost savings. No one will build a Limited Remote ID SUAS and no one will buy one either. Either eliminate this category or convert it to a broadcast-based Remote ID beacon for VLOS (and eliminate the arbitrary 400-foot range limit).

- These recommendations greatly reduce the national security threat imposed by requiring all consumer drones to be connected to the Internet and potentially sending surveillance data in real time to foreign adversaries who would use consumer drones for espionage. It complies with the government's own recommendations concerning the security vulnerabilities of using foreign-made drones.

- These recommendations meet the direction given by Congress, avoids eliminating indoor flight, reduces privacy risks and does not require the elimination of the model aviation hobby. The methods described above can be implemented at low cost, increasing the likelihood of compliance.

- This solution is potentially compatible with the European Union standard for Remote ID[74], which is consistent with previous FAA statements that it would like to see a solution that is harmonized worldwide. This in turn would lead to higher production volumes and lower costs, and greater likelihood of compliance.

Thank you for listening and, hopefully, creating a legal, workable solution for Remote ID that improves public safety while retaining reasonable airspace access for all, not just corporations and the wealthy.

Edward Mitchell, M.S., M.B.A.
Redmond, OR
edwardm1-remoteid@coldstreams.com

[73] https://www.opendroneid.org
[74] https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32019R0945&from=EN