# Submission 105 – Dr Andrew Tridgell

# RemoteID in Australia

Dr Andrew Tridgell, OAM
ArduPilot Systems Lead

# Introduction

I was dismayed to hear that Australia is considering implementing a drone RemoteID system that not just follows the US FAA model, but actually goes far beyond it. I have been heavily involved in implementing the US FAA RemoteID system and I believe it is a deeply flawed scheme. In this submission I will explain my concerns and why Australia should not follow down the path the US has chosen.

The key issues are:

- RemoteID as implemented by the US FAA would damage Australian UAV operators and vendors disproportionately, making us fall further behind vendors from countries like China
- The policy rationale behind RemoteID is intended to create aviation safety, but it can instead decrease safety by discouraging critical firmware updates and system changes needed for safe operation in specialised conditions
- The RemoteID system described in the Australian discussion paper, like the FAA RemoteID system, breaks with long standing regulatory practice of a cooperative approach between the industry and regulators. The approach described assumes that pilots are “bad actors”, creating an adversarial relationship which is damaging to the aviation industry
- The discussion paper describes RemoteID as increasing situational awareness with traditional crewed aviation, but does not achieve that goal, as the RemoteID signal would not be visible to crewed aircraft, and there is still no electronic conspicuity plan for general aviation aircraft outside of controlled airspace
- RemoteID will make education of students in the development, operation and maintenance of UAVs much harder
- RemoteID will impact on the ability to develop the next generation of professional UAV developers
- The broadcasting of RemoteID signals may encourage drone vigilantism, by providing uneducated members of the public with the means to target drone operations
- RemoteID will have a big negative impact on pilots involved in popular aeromodelling activities, both with MAAA/AMAS members and the general sports flying community

One of the key items I will be focussing on is the impact of the “tamper resistance” terms in the FAA RemoteID system. This seemingly innocuous requirement has a huge impact on the development, deployment and maintenance of UAVs.

The second aspect of RemoteID I will be focussing on is the split between “broadcast” and “standard” RemoteID, and why I think Australia should not adopt “standard” RemoteID at all.

# My Background

I am the systems lead for the ArduPilot autopilot system which is widely used throughout the world for a huge variety of UAV systems. A large part of ArduPilot development happens here in Australia.
I am also the lead developer of the ArduRemoteID RemoteID implementation, which is (to my knowledge) the only completely open FAA compliant RemoteID implementation. This system provides the software which runs on widely used RemoteID devices.

# About RemoteID

The key ideas behind RemoteID revolve around the following concepts:

- electronic conspicuity (being visible to observers using radio receivers)
- traceability (ability to trace an electronic conspicuity signal back to a vehicle owner)
- authorization (linking the conspicuity signal to an authorization to do the flight that is being done)
- drone location (including realtime drone location in the conspicuity signal)
- pilot location (including realtime pilot location in the conspicuity signal)
- tamper resistance (preventing users from modifying a vehicle so as to disable or modify some or all of the RemoteID functionality)
- design integration (building the RemoteID functionality into the vehicle at the design stage)

It is important to separate these concepts quite carefully. The FAA has not done a good job of separating them. For example, a recent FAA promotional video on RemoteID made claims about the ability of RemoteID to provide authorization in the conspicuity signal, but the actual FAA RemoteID standards do not do that.
The second thing that needs to be understood is the difference between what the FAA calls “broadcast” and “standard” RemoteID. There are a lot of detailed technical differences, but the key ones to understand for this discussion are:

- “broadcast” RemoteID is an add-on system, a bit like the widely used bluetooth tags that help you find your lost keys or wallet. It can be fitted to almost any vehicle type by attaching it either externally or in the fuselage (if the fuselage material does not block the signal)
- “standard” RemoteID is required to be designed into the aircraft rather than retrofitted, and also requires that it provides a highly accurate broadcast of the pilot position as well as the vehicle position. The FAA requires that all commercially sold UAVs come with “standard” RemoteID built in, which is a major problem for vehicles that are designed to be modular, maintainable and upgradeable.
- “standard” RemoteID must be incorporated in such a way that it prevents takeoff of the aircraft if the RemoteID system is not working

The discussion paper in Australia on RemoteID additionally conflates “standard” RemoteID with network RemoteID (NRID). The two are very different under the FAA system, and the FAA has not yet adopted network RemoteID, though there are some signs that they are considering adopting it in the future.

# Classes of UAVs

The impact of RemoteID is quite different for different classes of UAVs. For this discussion four broad classes are useful:

- video drones, such as the commonly known small DJI multicopters that are so ubiquitous
- FPV “racing” drones, which are primarily flown via goggles and are usually light weight but fast vehicles
- recreational fixed wing and helicopter model aircraft, typically flown as part of a flying club (eg. MAAA or AMAS), usually without any on board flight controller, flown either entirely manually or with very little electronic assistance
- Utility drones, for industrial, agricultural, search and rescue, scientific research, environmental monitoring and other tasks where specialised capabilities are often needed

My own background is primarily in the last 2 categories of aircraft. Most people in Australia would think of the first class of vehicle when they hear the word “drone” and it is this class of drone that is primarily of concern regarding privacy issues raised that is one of the stated drivers behind RemoteID adoption.

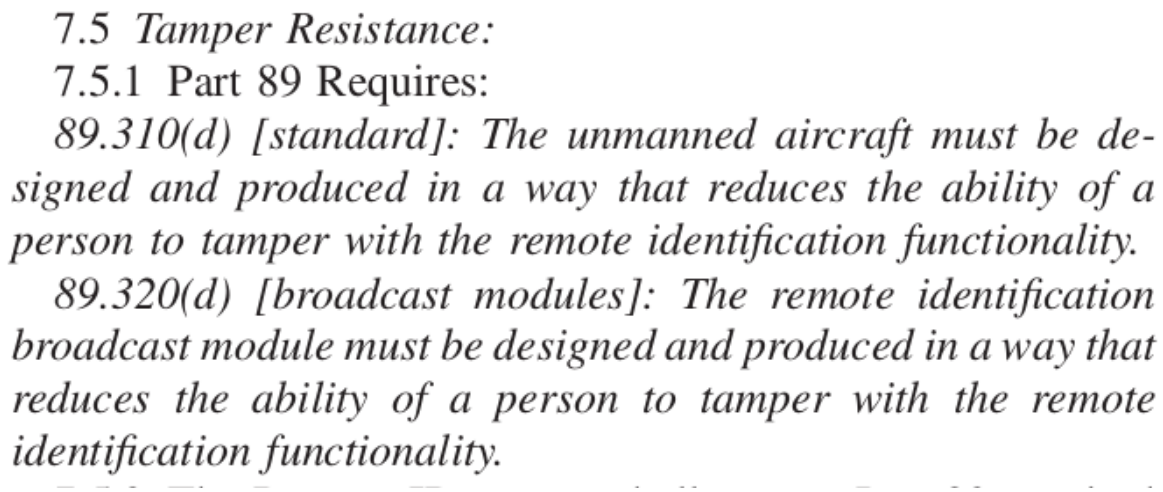
Australian companies have almost no presence in the production of video drones which are dominated by the Chinese company DJI. Australia does however play a leading role internationally in the last category of drone (what I call utility drones). It is this category which is most affected by the FAA-style RemoteID system.

The key hallmarks of these utility drones are:

- they are highly modular, with either a system integrator or end user combining components from a variety of vendors to produce a vehicle that is suitable for the specific task. For example combining GPS modules, lidars, radio systems, optical flow sensors etc, all of which require reconfiguration of the aircraft’s flight control system
- both the end users and system integrators commonly reconfigure the flight control system to meet specific flight tasks
- it is common to update the flight control software to customise it for the specific task it is performing

# Tamper Resistance vs Maintenance Resistance

At the heart of the issues with FAA RemoteID, and with the discussion paper for RemoteID in Australia, is the “tamper resistance” wording which I reproduce here from ASTM F3586-22:


7.5 *Tamper Resistance:*

7.5.1 Part 89 Requires:

*89.310(d) [standard]: The unmanned aircraft must be designed and produced in a way that reduces the ability of a person to tamper with the remote identification functionality.*

*89.320(d) [broadcast modules]: The remote identification broadcast module must be designed and produced in a way that reduces the ability of a person to tamper with the remote identification functionality.*

This extremely vague wording causes major problems. What does “reduces the ability” even mean? What is and isn’t sufficient to meet this requirement?

This tamper resistance requirement when viewed from the point of view of a UAV operator is really “maintenance resistance”. It puts requirements on the design and construction of UAVs that make them more difficult to update and maintain.
The impact of this “maintenance resistance” is highest on the types of highly modular and configurable drones that Australian industry has become known for. It has almost no impact on drones such as DJI video multicopters, as those are already locked down and have very little end user configurability. This means RemoteID will severely impact the competitiveness of Australian drone makers as it severely degrades the key feature that makes their vehicles attractive to end users.
This tamper resistance also relates to the push worldwide for consumer rights to repair. Mandating that drones have reduced ability to repair and maintain is going against the trend for consumer rights.

## Parameter Lockdown

In order to achieve tamper resistance the vendor selling the vehicle needs to lock down many of the standard configuration parameters in the vehicle. For example, they may need to lock down the GPS type, the RemoteID options, the CAN bus options and others. These need to be locked down as otherwise it would be very easy for a user to disable the RemoteID feature which means it would not meet the tamper resistance requirement.
This means the end user is unable to change these options in the firmware. That drastically reduces the ability of the end user to perform configuration changes which may be needed for specific operations, such as changing the GPS type to one more suitable for the task (for example, implementing moving baseline GPS yaw, or converting for use indoors).

## Firmware Lockdown

The UAV industry is still young and software (firmware) updates are still very common when issues are discovered, and especially when bugs are fixed that impact safe operation of the vehicle. In order to meet the FAA RemoteID requirements the vendor may need to lock down

the firmware before shipping to the user to prevent the end user changing to a firmware version without RemoteID enabled. This lockdown can prevent end users from updating to fix critical bugs without the vendor supplying a new firmware.
Normally end users can update to the latest release with a simple GUI tool built into commonly used ground station software, and are automatically informed when a new release is available. The nature of the RemoteID tamper resistance requirement means the standard releases are not able to be used and each vendor needs to create a custom firmware. These releases will lag behind the standard releases or may not be available at all if the vendor is unresponsive.

## Licence Plate or Ankle Bracelet?

To understand the impact of the traceability requirement let's try to apply it in a more familiar context. The FAA (and other aviation regulators) often refer to RemoteID as "a licence plate for the sky". So what would happen if the licence plate on your car had this tamper resistance requirement along with the other "standard" RemoteID requirements?

- the licence plate would have to be designed so it could not be unscrewed from the car or painted over
- the licence plate would need to be linked to the car's ignition so that you cannot start the car if the licence plate was obscured
- the car would have to be designed in such a way that car owners would not be able to do any maintenance that could impact the licence plate
- the licence plate would need to be visible from several kilometres away

This would be completely impractical for the automotive industry and for motorists who want to do basic maintenance on their cars.
We can also imagine what this would be like in crewed aviation with ADSB. Imagine if the ADSB was both mandatory and physically wired into all crewed aircraft so that it was linked to the engine ignition. It would be impossible for either a pilot or a maintenance engineer to make any changes that impact the ADSB, preventing basic maintenance on the aircraft. This is what is happening with RemoteID for drones.
I think a much more apt analogy for RemoteID is the GPS ankle bracelets that are used with prisoners on home release.

- a GPS ankle bracelet provides remote monitoring of the prisoners position
- a GPS ankle bracelet is made to be tamper resistant because you are fitting it to people who are known to be criminals

The aviation regulations should not treat drone pilots in this way.

# Trust in Aviation Regulation

This brings me to one of the key issues with the whole RemoteID design as implemented in the FAA system. Prior to RemoteID, aviation regulation was largely based on the premise that the members of the community that are being regulated (including pilots, maintenance engineers, system integrators, aircraft vendors etc) are all generally "good actors". The assumption is that the vast majority will follow the rules, and this is backed up by having warnings, fines or revoking of authorizations or licences when rules are not followed.
In Australia, the aviation regulations are evidence-based and created in a cooperative manner with members of the aviation industry, based on an assumption of trust.

The RemoteID design breaks with that tradition in a fundamental way. It starts off by assuming that the community has lots of “bad actors” and so uses lockdown mechanisms (such as tamper resistance) to try to achieve the regulatory goals. This punishes the vast majority of good actors while not really having an impact on bad actors because bad actors can still trivially bypass any technical measures that are put in place.
In 2023 we’re at the point now where approximately half of all pilots in Australia are remote pilots. On current trends that ratio is going to get higher and higher, so looking forward 10 or 20 years it is likely that the vast majority of pilots will be remote pilots. If Australia copies the FAA RemoteID system then it is setting up a very adversarial relationship with a large part of the aviation community. That would not be good for aviation in Australia.

## Standard versus Broadcast RemoteID

The issue of trust is also central to the difference between “standard” and “broadcast” RemoteID. The key motivation between the two types of FAA RemoteID is one of not trusting pilots. The “standard” RemoteID system, which is what is required for any commercially sold vehicle in the USA, requires very tight integration with the UAV, and also requires very tight integration with the ground station or UAV hand controller. The reason for this tight integration is twofold:

- similar to the tamper resistance, it is an attempt to prevent users from disabling the system
- the desire to have accurate pilot position to make it easier for law enforcement to find the pilot

Both of these reasons are badly flawed. The tamper resistance won’t stop anyone who is determined to bypass it, and it only takes one person to work out how to disable it and publicise it for anyone to know how.
The requirement for pilot position is a very complex way for law enforcement to find the pilot. A much simpler solution is to either have the system broadcast the initial position (takeoff position) which is almost always where the pilot is, or just wait for the UAV to land, and go to that location. Most drones have a short battery life and will land near where the pilot is located.
In trying to get the pilot position the FAA RemoteID system introduced a much more complex and error prone communication path between the pilot and the vehicle. On some systems where the hand controller already incorporates a GPS this can be achieved in a reasonable manner, but on many systems preferred by experienced UAV pilots there is no GPS built into the hand controller.
If Australia does adopt a RemoteID system I would strongly recommend not adopting the “standard” system that the FAA has chosen. Going with only what the FAA calls “broadcast” will provide for a much simpler and less intrusive system.
This is complicated by the way that the Australian discussion paper on RemoteID has conflated “standard” and “network” RemoteID.

# Impact on Education

Australia plays a huge role in the international UAV industry, especially in the “utility” drone category I outlined above. The engineers that allowed us to gain this position largely came from a background of tinkering with drones as hobbyists. The ability to modify the flight

control software on small drones is key to ensuring that we have a continuing stream of highly skilled engineers in the future.
The tamper resistance requirements in the FAA RemoteID scheme would severely limit what upcoming engineers could modify on their vehicles. It would make it harder for them to modify and legally fly their modified drones which is essential to the learning process.
The same applies in schools and universities. We need students exposed to much more than just flying DJI drones - we need students to be able to modify the software that makes drones fly and learn the skills that will set them up for a career in UAV design and aerospace. That can't happen if the drones the school wants to use are locked down with RemoteID tamper resistance requirements.

# Deeply Flawed FRIA Process

As part of the FAA RemoteID system the FAA added a "FRIA" system (FAA Recognised Identification Area). A FRIA is an area where RemoteID devices are not needed. The process for making an area a FRIA is very difficult and as a result there are very few FRIA areas approved.
If we do have to have RemoteID in Australia then this FRIA system should be inverted. The concerns that have been expressed about drones that are leading to the push for RemoteID do not make sense for the vast majority of the Australian continent. For example, a person flying a drone on a farm in outback NSW does not pose a privacy risk to anyone. So we should default the whole of the Australian continent to not need RemoteID and only apply it in areas where it really would make sense, for example in higher density urban areas.
This is similar to what is done now with the "OK2Fly" app which lets pilots know which areas they can fly in. That app could be extended to show areas where a broadcast RemoteID beacon is needed.

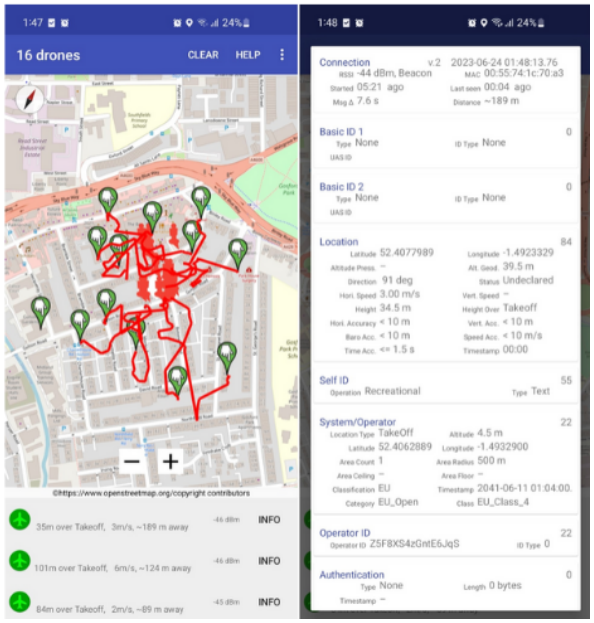
# Harassment of Drone Pilots

An increasing problem in the drone ecosystem is members of the public harassing drone pilots. There are numerous reports and videos showing pilots being harassed as they make perfectly legal flights.
The RemoteID systems will just make this sort of harassment more common. It means any self-styled drone vigilante will be able to see any drones flying within a large area, allowing them to go and express their dislike of drones to the pilot. This can create dangerous situations where the people harassing the pilot interfere with the flight, or prevent safe landing as members of the public are blocking the landing area.
The broadcast information also provides ideal information for those who may wish to steal expensive drones. Many drones are worth tens of thousands of dollars, and broadcasting their location may create a new class of illegal drone theft.

# RemoteID Spoofing

The adversarial approach the FAA has taken to RemoteID has created a backlash in the drone community. This has inevitably resulted in some people trying to disrupt the system.

One example of this is a RemoteID spoofing system which runs on very cheap and easily available hardware. Here is an example of someone running it in the US:




In this example the spoofing system is broadcasting RemoteID signals for a fake swarm of 16 drones. While this particular case is just an annoyance so far, a much more insidious use would be to spoof the ID of a real drone in order to cause trouble for a legitimate drone operator.

It should be noted that ADSB as used in crewed aircraft is just as easily spoofed with similarly cheap hardware, yet we haven't seen a significant problem of spoofing of ADSB despite it being used for decades. I think the adversarial approach used by the FAA for RemoteID has contributed to this problem.

# Conclusion

RemoteID as embodied in the FAA system and as envisioned in the June 2023 Australian discussion paper is deeply flawed. It would have a disproportionate impact on the Australian drone industry and may reduce drone safety as it impacts the ability to maintain and update vehicles.

If we must have a RemoteID system (and I don't think we should) then we should not mandate any tamper resistance, and should only implement broadcast RemoteID and that should only be in specific areas of Australia where the benefits outweigh the costs. We should not attempt to include real-time pilot location and should not require that RemoteID be designed into vehicles in a tightly coupled manner.