Submission 141 – Michelle Rossouw

Response to “Remote Identification Discussion Paper for Public Consultation”

Michelle Rossouw

[redacted]

28 July 2023

This document is entirely my own opinion.

Introduction

I am dismayed to see that Australia is intending on implementing Remote ID. Having followed the implementation of Remote ID in the US and seen the negative impact it is having, I had hoped that Australia would not go down this same path.

I also noticed that on this “have your say” page, the first question you’re asking for feedback on is “Should a Remote ID mandate be developed?”, yet the very introduction on this page says, “We are consulting on the Drone Remote ID Discussion Paper to decide how best to successfully adopt Remote ID for drone use in Australia.” This makes it unclear whether the implementation of Remote ID is up for discussion at all, which erodes trust.

What evidence?

The first problem with this discussion paper itself is the lack of evidence to support its statements. I find this very concerning and it makes this public consultation much less useful than it should be, given that we do not have any real evidence that Remote ID is necessary at all. At minimum, research needs to be done on the advantages and disadvantages of Remote ID before going any further in this process, to ensure that Remote ID doesn’t end up causing more harm than good, which I believe is a very likely outcome at the moment.

Tamper resistance? More like ankle bracelet.

The main issue with the implementation of Remote ID is the “tamper resistance” requirement. This assumes that all drone users will try to break the law and disable it, instead of assuming that most users are law-abiding citizens. The analogy that has often been used to promote Remote ID (by the FAA and others) is that it is a “licence plate for the sky”. Yet a licence plate isn’t welded to a car – a simple screwdriver or other tool can remove it. This tamper resistance would make Remote ID more like an “ankle bracelet of the sky”. It says, “you are all criminals, and we must track you at all times to make sure you don’t break the law.” This is not a good way to treat drone pilots. This will set up an adversarial relationship between drone pilots and CASA that will in all likelihood cause harm to all involved.

One of the ways it could cause harm is that this tamper resistance would likely require making it impossible to change certain parts of the firmware, such as the GPS type. It may

even make it hard or impossible to upload custom firmware to a drone. This would impact on universities and other research groups, as research requires that the researchers be able to upload their own custom code. While the idea of allowing exemptions seems like a solution, the tamper resistance would still need to be removed to allow that, and big companies that sell drones may not be very responsive on that front.

I also find the timing of this discussion paper - so shortly after the FAA implemented Remote ID - rather interesting. Too short, in my opinion, to see what problems their implementation may cause. This is especially true when it comes to research groups, as the effects of discouraging an entire generation from drones and other STEM-related research will take rather long to become apparent. This could happen in two ways: Either directly, via the above mentioned impediment to research, or by the extra effort to fly a drone for hobby use making fewer people interested in doing so. One only needs to do a quick Google search to see how much hobbyists learn about electrical engineering among other things during the process of building their own drone. This is an excellent gateway for more people to become interested in STEM careers. At minimum, allowing home-built drones and drones sold for educational purposes to not have the tamper resistance requirement would help mitigate that problem.

Tamper resistance also likely won't stop the few people who really are determined to break the law. They will likely find a way around it just like they've found ways around other restrictions.

Remote ID is also likely to result in law-abiding citizens being caught for the wrong-doing of law breakers: Because their drones will be the only ones broadcasting the Remote ID data, whereas the law breaker who may have been flying in the same area will have disabled their Remote ID module. Thus authorities wouldn't even know they were there, and would likely blame the law-abiding citizen instead.

It seems the real problem here is that there are already too many drone laws to be reasonably enforced. People generally don't speed, because they know there might be a cop around the corner. But when people break drone laws, usually nothing happens. Remote ID won't change that. It will just be another law for the law breakers to ignore, but that law abiding citizens have to follow.

Broadcasting live position data

Even without the tamper resistance requirement, the licence plate analogy still falls flat: A licence plate doesn't broadcast a car's ID and exact position for kilometres as Remote ID is required to do by the FAA. There is already a lot of hate towards drone pilots and requiring the drone and/or pilot's exact location to be transmitted will only make it easier for vigilantes who hate drones to attack and possibly injure pilots. This has already happened in some countries. If Remote ID must be implemented, I believe it should broadcast only the ID and no position, and only on low power, such that it can only be received from ~100m away, similar to a car's numberplate. This would help mitigate the problem while still retaining the ability to identify a drone if it is flying too close to people.

From a technical perspective, even a small module is difficult to implement because of the GPS requirement and not all drones have that. This becomes even worse if the operator position is required, as that requires a bidirectional link between drone and operator. Many

drones are likely too small to be able to carry this extra hardware without negatively impacting on their flight performance and their already short battery life.

The discussion paper mentions Remote ID being useful for traffic management systems. This is another area where we need evidence that it's actually necessary before considering it: Drone pilots keep their drones below 400 ft and away from airports, and crewed aircraft stay above that other than at airports. As far as I know, there has not been a single crewed aircraft crash that was confirmed to be caused by a drone. I don't see any evidence that we need anything more.

Network Remote ID (NRID) is even worse, requiring that the drone and/or pilot's live location be transmitted to the internet at all times. Imagine the uproar there would be if a law was made that all cars must have a GPS-enabled device wired into the ignition that transmits the car's current position and licence plate to the internet at all times. NRID is the direct equivalent to that for drones.

This data-gathering is also not necessarily a good thing. After the breach of trust when police used QR code check-in data for law enforcement, (https://www.smh.com.au/politics/federal/breach-of-trust-police-using-qr-check-in-data-to-solve-crimes-20210903-p58om8.html) the public are unlikely to trust that their data will only be used for what it's intended for. This is a time to build trust back up, not break it down further by placing these kinds of restrictions and data gathering on law-abiding citizens.

Conclusion

I do not believe that Remote ID is a necessary nor a reasonable restriction to place on drone users. A tamper resistance requirement would make researchers and other developers' work hard or impossible. The requirement to broadcast the drone or pilot's current location is not only a privacy issue, but is also likely to result in drone-hating vigilantes attacking drone pilots.

If Remote ID must be implemented, allowing home-built drones and drones sold for educational purposes to not have the tamper resistance requirement, this would greatly reduce the negative effects on STEM careers. If Remote ID broadcasts only the ID and no position, and only on low power, such that it can only be received from ~100m away, similar to a car's numberplate, this would help mitigate the privacy and safety issues while still retaining the ability to identify a drone if it is flying too close to people.

Firstly though, I believe some research needs to be done to find out whether the statements and assumptions made in the discussion paper are actually true, how the implementation can be done from a technological perspective, and what impact that implementation would have on the various groups using and developing drones, and whether there are actually more benefits than the great harms and risks.