Submission 110 – Confidential

Thank you for the opportunity to consider the RemoteID concept and submit suggestions for your consideration.

I am a member of a drone racing club and have some interest in RPAS technology.

I hope this helps. Good luck.

Remote Identification (Remote ID)

Public Consultation of June 2023 Discussion Paper

Data and access questions

1. Who should have access to Remote ID data and to what information?

In looking at the problem of balancing 'safety' and 'security (incl privacy, crime, etc),' it may be easier, less complicated and more affordable to prioritise public safety by promoting the data as being freely available. Those who have deliberately invested efforts into gaining the knowledge and technology to monitor RPAS activities can be assumed to have a level of trust to use it appropriately, similar to the public utility of 'Flightradar24: Live Flight Tracker' app.

a. With the advent of modern technology being readily available to record and analyse the total Remote ID database, it might be appropriate for the Insurance Companies to be included in the agencies entitled to access the database for the purposes of validating insurable and uninsurable behaviours and claims.

b. The sharing of the Remote ID data could have the following unintended consequences:

   1) Sharing the locations of good vantage points used by operators to gain desirable data and images that are commonly desirable, resulting in new locations frequented and crowded by drone operators to the annoyance of local residents.

   2) The knowledge of these advantageous operator locations may also become synonymous with the locations of otherwise discretely kept secret information for observing celebrities and VIPs at their home or other frequently visited locations.

   3) Similarly, drone operators might be able to deduce and share operator locations that are advantageous for observing otherwise low-profile and secret locations and activities, inadvertently benefiting public activists, protestors, and criminals.

2. Should there be a data collection standard?

The data system design should follow an open system architecture and the data should follow a commonly used, future-proofed, non-proprietary standard to minimise the inconvenience of system upgrades and changes to the users. Ultimately, the system and data should be interoperable and interchangeable with an international global standard.

3. What is the best method of providing Remote ID data to relevant stakeholders?

This should be reviewed in a dedicated 'Stakeholder Analysis.' Stakeholder needs and uses will vary when the representative user can range across:

a. Non-drone operators need to be considered (i.e. shared, similar to Flightradar24 or denied due to concerns for privacy and user demands on the system).

b. a simple individual hobby user.

c. a collective group of individual public users (eg racers, STEM group, school group, group of trainees, etc).

d. a business agency (eg user, insurance, training/education, data collectors, systems developers, etc).

e. an example of a current government agency affected by their use of drones and the public use of drones in their operating areas (eg security, public infrastructure surveillance, etc).

f. a newly appointed government agency to be capable and responsible for providing governance, assurance, and public support (eg help desk) to support the delivery of trusted data and exercising governance over:

    1) drone and user registration data and database;

    2) the timely collection, processing, and distribution of RemoteID data; and

    3) assures data certification standards for RemoteID data confidentiality, availability, and integrity.

4. What types of drone operators should be required to carry Remote ID equipment to operate drones? What should be exempt and why?

Consider adopting an Insurance Risk-based approach. Users should be encouraged to consider the risks and consequences of their actions in their use of drones with the size, mass, and capability to cause harm (ie physical, non-physical, etc) and/or damage. If a drone warrants a RemoteID registration, it should also be mandatory to require the user to hold a valid third-party injury and property damage insurance policy. The problems resulting from the rapid proliferation of public hire e-scooters and hire by non-compliant and uninsured users highlights the risks of errant drone users operating without insurance.

A variation to the insurance requirement is when the drones are deliberately being operated totally within a controlled airspace environment where a separate agency has accepted responsibilities for:

a. owning the insurance policy to cover the activities and people invited to operate within that controlled environment,

b. vets the people as being suitably competent and drones as being suitably functional and fit-for-purpose to meet the requirements of the operating environment and insurance policy, and

c. negating the need for individual users to have their own personal insurance policy when approved by this entity to operate in this activity in this environment.

This might be applied to demonstration/exhibition events, drone racing clubs, training schools, for example.

5. How can Remote ID privacy issues be managed?

The government-appointed agency should manage the centralised total database for RemoteID registration data, including the associations between individual user's personal identity details, the CASA-managed Aviation Reference Number, and the unique identifier assigned for each drone. The drone unique identification could be shared similarly to flight numbers in the Flightradar24 app in the same way that the public expects car registration number plates to be publicly visible when the motor vehicle is in use, 24/7.

During this build-up phase, consider, building scenarios to describe typical and extreme cases that help to define the boundaries of responsibilities for the User, the governance agency, and other key stakeholders (eg insurance) to test and further develop in future public consultations.

Be aware of the potential for inadvertent consequences from data users being able to aggregate data from data tracking from a future RemoteID system. Note the problems experiences by US users of the Strava FitBit recorded in case studies (refer www.wired.com/story/strava-heat-map-military-bases-fitness-trackers-privacy/).

Technology questions

6. Is Remote ID (BRID, NRID or both) an appropriate solution for Australia? Are different types of Remote ID more fit-for-purpose in different contexts or applications? Are there other types (or variations of types) of Remote ID that should be considered?

It is appropriate that when a drone has been identified as being capable of presenting a reasonable risk to the safety of the public and property (e.g. it has an all up weight and operating speed that can generate enough momentum to cause harm or damage on impact) then it should be declared, assigned a unique identifier, and insured.

7. What factors should Remote ID mandates be based on, e.g. location, airspace related, other?

The RemoteID data should include the following parameters:

a. Operator's Aviation Reference Numbers,

b. Location of operator,

c. Drone Unique Identifier,

d. Drone system and usage category identifier (i.e. should match the actual drone and the details listed in the applicable insurance policy),

e. The current location of the drone,

f. The aggregated tracking locations of the drone over past time periods (i.e., the multiple different sorties, triggered by multiple launch/landing events), and

g. Status of registration and 3rd-party injury and property damage insurance.

8. What technical requirements, standards and governance arrangements should be considered in the introduction of Remote ID to position for integration with adjacent systems, including the development of the UTM ecosystem?

Open system architecture and compatibility/interoperability with global standards.

Be aware of data and cyber security concerns to avoid collaborating with certain publicly identified overseas equipment manufacturers and suppliers known to be deliberating harvesting data from the users of their consumer products.

9. What features does Remote ID require to ensure tamper resistance and to mitigate security issues (including cyber risks)?

Need to anticipate the misappropriation of drone unique identifiers to misrepresent illegal activities, stolen drones, and cost-cutting (e.g. misrepresenting a large-sized commercial drone as a small-sized recreational drone to illegally benefit from cheaper insurance premiums).

Usage questions

10. What impacts could mandatory equipage have on drone operators?

Updated education, increased burden for purchase and installing mandatory equipment, decreased system performance due to increased vehicle weight, and new compliance requirements for certification and regular reviews. Nothing new here when compared to other initiatives in systems and procedures to improve public safety for individual and collective users.

11. Should mandatory equipage be rolled out to all drone operators, or phased through types of operators and/or operations?

Consider a phased approach to enable test and evaluation efforts to provide opportunities to review and improve as the rollout progresses. The types of operators/operations should be categorised based on insurance risks and commenced with the stakeholder group categorised with the highest insurance risk.

12. Are there existing standards that should be considered/adopted to facilitate Remote ID uptake in Australia?

Nil response.

13. Who should we be engaging with, particularly outside of the aviation industry (e.g. telecommunications providers)?

Nil response.

Regards