Submission 126 – John Gotovac

John
Gotovac
[redacted]

06 July 2023

Department of Infrastructure, Transport,
Regional Development, Communications and the Arts
GPO Box 594
Canberra ACT 2601
Australia
drones@infrastructure.gov.au

Re: Remote ID Discussion Paper

To Whom it may Concern

References:
A: Remote Identification (Remote ID) – Discussion Paper for Public Consultation, Department of Infrastructure, Transport, Regional Development, Communications and the Arts, dated June 2023.

Introduction

Hello and thank you for the opportunity to provide feedback on the discussion paper proposing options and considerations for applying Remote Identification (Remote ID) for drones flown in Australia (Ref A). I support the need to explore and develop new systems to manage the operations of current and emerging drone technology in Australia and hope my submission can be assist in this matter.

Enclosed are my responses to the discussion paper questions (Ref A para 8), based primarily from my perspective as a MAAA registered Radio Control (RC) recreational flyer

of micro, very small and small classified Remote Piloted Aircraft (RPA), as classified under CASA Part 101.

I work in aviation, I occasionally fly traditional balsa wood visual line of sight (LOS) radio RC operated airplanes, but these days I regular fly my own custom home built First Person View (FPV) very small and micro quadcopters.

For my response, please don't hesitate to contact me on any points of discussion.

Sincerely

John Gotovac

[redacted]

Enclosures:

1 – Response to Remote ID Discussion Paper (Ref A)

Enclosure 1

Discussion Paper questions and Reponses

Data and access questions

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

- Air Navigation Service Providers:
  - Drone location, registered drone operator data.
- Other registered air space users:
  - Drone location data only.
- Federal and State Police:
  - Drone location and operator contact details. Only in response to reported incidents involving drones.

2. Should there be a data collection standard?

- Yes, only enough so the registered owner of a drone is contactable by CASA.
- BRID signals to be detected by sensors only for the purpose of managing controlled airspace and no fly areas.
- Drone location and operator personal data to be registered with CASA only.
- Drone location data to be only disclosed to other registered users and CASA approved 3rd party agencies and aviation support service providers.
- Personal information to be disclosed by CASA to law enforcement agencies by exception to support investigations into reported incidents involving the use of drones.

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

- BRID. Keep it simple and cheap.
- A cheap and small BRID module that can be easily fitted to a drone, without the need to integrate into a separate phone of internet provider WIFI network.
- Collected drone flying location data can be presented in commercial 3rd party mobile phone applications as recommended by CASA, with notifications and alerts for when airspace restrictions and no fly zones are to be complied with.
- Operators can manually declare when they are flying, no need for a module to arm or register with a network before it takes off.

- Pilots in areas that have no BRID or network coverage to fly their drones under due regard operating conditions.

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

- Remote ID only to only be applied for drones with a mass greater than 250g, possibly 500g.
- Note: ID modules need to be small and within an affordable price range, say 20g at about $50.00 for a module. If BRID modules are too heavy or overpriced, people won't fit them, especially if a GPS has to be also fitted.
- Exemptions: No Remote ID on RPAs flown for recreation and sport at CASA approved MAAA Model Aircraft Clubs sites or approved events. As they are already recognized as being compliant in managing the RPA operational risks at these sites, with well established safety practices and culture.
- Importantly, remote ID and Drone registration should be promoted and supported to assist in more flying of drones in more places, not as a means to restrict and deter non compliances by registered users. The more registered users there are, the easier it is to identify malicious and criminal use of drones by operators that would naturally avoid using remote ID all together.

5. How can Remote ID privacy issues be managed?

- Track the drone and not the person.
- Do not disclose drone operator details to the general public, only provide general information on where the drone is operating and that it is a registered operator.
- Police to be prudent in addressing drone incidents with registered users, with a no blame approach to promote safety education and address non complaint users
- I would be comfortable logging into a CASA approved phone app to declare that I'm flying a drone, and don't need an integrated system to be tracked with the drone. I believe most operators would do this at their free will in preference of being subject to an indirect personal tracking device.

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?

- BRID only, when a cheap and light module is available from multiple suppliers.
- Shouldn't be any complicated as a toll bridge tag that is fitted to a car windscreen.
- No NRID, as it is dis-proportionally expensive and complex for regulators, drone manufacturers and operators to integrate, and would obstruct form any effective industry development and innovation in the practical use of personal, commercial and industrial drones in Australia.
- For relatively larger drones, there are commercial aviation manned aircraft systems available that are already being fitted, such as ADS-B.
- Finally, many RC aircraft and drone RC equipment utilise telemetry systems that can have remote ID integrated into already existing hardware and software. Requires acceptance of open source software providers to implement. For consideration.

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

- Near or below managed airspace.
- Privately owned land and property.
- Designated drone no-fly zones in public areas.
- Sensitive Government facilities.
- Public events, places of worship, sensitive areas, etc.

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?

- Governance to be applied to ensure no price gouging by remote ID manufacturers and suppliers.
- A specification and price range for a remote ID needs to be specified for the Australian market that is readily acceptable and affordable for manufacturers and by people who need to fit remote ID to their drones.
- Remote ID should utilise the RF spectrum in a manner that does interfere with the current spectrum RF spectrum allocation for RC aircraft and drone operations, including 2.4Ghz and 5GHz RF bands

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

- I understand some standard encryption protocols and keyed identification solutions should suffice.
- Security requirements and educational material to be provided for drone operators to protect their remote ID details.

Usage questions

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

- Cost of fitting additional equipment, including GPS systems.
- Cost of replacement of non-compliant commercially of the shelf (COTS) drones that cannot be retro fitted with remote ID.
- May expose drone operators to being hunted and harassed from random or disturbed individuals.

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

- Roll it out to all operators, easiest, but is dependent on price and availability of BRID modules.
- Exemptions and waivers to be applied as applicable.

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

- Usual RF spectrum management and telecommunications standards for aeronautical operations.
- I think it best to see how the adoption of remote ID plays out in the USA, then see what the market has to offer, but a locally made unit for our needs would be good.

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

- Manufacturers and suppliers of electronic equipment to enable opportunities to keep the cost down and maintain supportability of the BRID modules, and the BRID airborne and ground receiver stations.
- Owners and managers of lands and parks that would be applying drone no fly zones along with the creation of a network of drone friendly spaces.

end