Remote ID for Drones

A Policy Position Paper by the Drone Pilot Association of Canada

EXECUTIVE SUMMARY

The Drone Pilot Association of Canada (DPAC) has developed a policy position on drone Remote ID that balances accountability and privacy. DPAC is an organization of recreational and small commercial drone pilots advocating for safe and responsible drone use in Canada.

DPAC recognizes that Remote ID can enhance safety, security and accountability but also advises that Remote ID carries the risk of government over-reach for the drone community, potentially compromising reasonable freedom and privacy. As such, DPAC recommends:

- Remote ID should be mandatory for drones over 25kg or drones over 250g performing higher risk operations such as flying beyond visual line of sight (BVLOS). Otherwise, Remote ID should be optional for drones under 25kg, including particularly micro drones less than 250g.
- The Remote ID data packet be limited to the drone serial number and aircraft location coordinates. The control station/pilot location must not be transmitted, unless encrypted in such a way that only authorized law enforcement entities can determine that location.

DPAC has also developed recommendations for associated enforcement processes, affordability, and implementation timeline considerations.

DPAC suggests that it should be invited to Transport Canada policy forums and committees, such as CanaDAC, to ensure the interests of recreational and small commercial drone pilots are represented in Remote ID regulatory development discussions.

CONTENTS

Executive Summary 1
Contents 2
Introduction 3
Remote ID is a Rapidly Evolving Topic 3
DPAC Must Represent its Members on the Remote ID Issue 3
Background 4
Remote ID is Mandated in the United States 5
Remote ID is under Consideration in Canada 6
DPAC Policy Position 7
Recognition of the Importance of Remote ID for drones in Canada, with limitations: 7
Consideration of the Privacy Implications of Remote ID: 7
Opportunity to Contest Enforcement Action: 8
Accessibility and affordability of Remote ID solutions: 8
Adequate implementation time frame: 8
Invitation to join CanaDAC (or its Successor): 8
Conclusion 8
About the Drone pilot Association of Canada (DPAC) 9
Contact Us 9

INTRODUCTION

Remote ID is a Rapidly Evolving Topic

Remotely Piloted Aircraft System (RPAS) include rotorcraft drones (quadcopters, etc.), fixed wing drones, First Person View (FPV) drones, and radio-controlled model aircraft. Within this document we will refer to all such RPAS as 'drones' since this is terminology that is widely understood by everyone in the drone community.

Remote Identification (Remote ID) for drones refers to the ability of drones to transmit their identity, location, and other relevant information remotely to entities such as Public Security and Air Traffic Management authorities, other aircraft operators, and the public. This technology aims to enhance the safety, security, and accountability of drone operations by enabling the identification of drones in flight and the tracking of their movements.

The development of Remote ID technology and regulations for drones is a rapidly evolving topic as the use of drones has accelerated in recent years, and there is a growing need to ensure their safe operation in the national airspace. New developments and regulations are emerging to address the security and privacy concerns that come with the widespread use of drones.

Governments around the world are exploring different approaches to Remote ID for drones, including mandatory requirements for drone operators to equip their drones with Remote ID systems and to register their drones with the relevant authorities. There are also ongoing discussions about international standards for Remote ID, which would help to ensure a consistent and harmonized approach to drone regulation across different countries, and a simplified environment for drone manufacturers.

It should be recognized that criminal or terrorist use of drones is unlikely to be deterred by Remote ID regulations. Remote ID broadcast systems will undoubtedly be defeated or masked by those intent on unlawful activities. This fact must be balanced carefully against any accessibility or privacy concerns that Remote ID may impose upon honest citizens trying to enjoy this hobby or pursuing simple commercial operations.

In short, remote ID for drones is a crucial aspect of the drone operational environment that will continue to evolve and develop as the technology advances and the use of drones becomes more widespread. It is important for governments, drone operators, and other stakeholders to stay informed about the latest developments and to work together to ensure the safe and secure operation of drones in the national airspace.

DPAC Must Represent its Members on the Remote ID Issue

The Drone Pilot Association of Canada (DPAC) is an organization that represents the interests of recreational and small commercial drone pilots in Canada. As such, DPAC has a responsibility to provide clear guidance on its policy position regarding Remote ID.

DPAC's policy position on Remote ID reflects the views and concerns of its members, and it provides clear guidance on the association's stance on key issues such as the implementation of Remote ID requirements, privacy concerns, and the impact of Remote ID on the drone community in Canada. By taking a clear and proactive stance on these issues, DPAC can help to ensure that the rights and interests of its members are protected and that the drone community in Canada continues to thrive.

BACKGROUND

In the United States (US) Remote ID is a critical aspect of the drone operational environment that enables the identification and tracking of drones during flight. By transmitting information about their identity, location, and altitude, drones with Remote ID capabilities help to enhance safety, security, and accountability. [Remote Identification for Drone Pilots | Federal Aviation Administration (faa.gov)][1]

Remote ID implementation in the US has set a benchmark for implementation, so it is crucial to understand the Federal Aviation Administration's (FAA) current standard. Remote ID data packets are unencrypted and are broadcast at a rate of once per second (1 Hz) over unregulated Wi-Fi or Bluetooth frequencies. The broadcast is intended to be received by entities such as air traffic control systems, law enforcement agencies, and the public.

The Standard Remote ID message includes [RemoteID_Executive_Summary.pdf (faa.gov)][2]:

- drone ID (serial number of drone or a session ID)
- latitude/longitude, altitude, and velocity of the drone
- latitude/longitude and altitude of the drone control station
- emergency status of the drone
- time mark

As of February 2023, several DJI drones (including the DJI Mavic 3 Classic, Mavic 3 Cine, AVATA, Air 2S, Mini 3 Pro, Agras T40, Agras T30, M3T, M3E, M30, M30T) are now approved for Remote ID in the US. The newly manufactured versions of these drones comply with FAA Remote ID rules without any customization or add-ons required [DJI's Top Drone Models Approved For FAA's Remote ID Mandate (dji.com)][3]. The Remote ID serial number is the same as the aircraft serial number. This number can be located on the drone's battery compartment, packaging, the "About" page of the DJI Fly app, and within the drone's WLAN "Available networks" [User Guide for FAA Remote ID Compliance (dji.com)][4].

DJI states that – at the present time (February 2023) - drones with built-in Remote ID do not broadcast FAA Remote ID signals when flying outside of the US, and that drones that have built-in Remote ID brought into the US from a non-US country will broadcast FAA Remote ID signals when flying inside the US[4].

The Remote ID drone ID serial number can be linked to the owner of the drone through the serial number provided during the legally mandated drone registration process with both the FAA and Transport Canada (TC). The owner information is available to authorized personnel, by request to the FAA or TC. Although the normal presumption is that the registered owner of the drone will also be the operator or pilot of the drone, this is not necessarily true, particularly for drones used by organizations. Remote ID does not directly provide personal information about the owner, operator, or pilot of the drone.

The FAA requirement to broadcast the location of the control station – this presumably also being the location of the drone pilot – is a controversial issue because it has the potential to compromise the security of the pilot, potentially leading to confrontations with and harassment from members of the public.

[1] https://www.faa.gov/uas/getting_started/remote_id/drone_pilots
[2] https://www.faa.gov/sites/faa.gov/files/2021-08/RemoteID_Executive_Summary.pdf
[3] https://www.dji.com/newsroom/news/dji-top-drone-models-approved-faa-remote-id
[4] https://ag.dji.com/newsroom/ag-news-faa-remote-id-compliance

The FAA requirement for drones to broadcast unencrypted Remote ID information using non-proprietary radio frequencies compatible with personal wireless devices is aimed at ensuring that the information can be received and understood by any device within range of the drone, including the public and other interested parties. The government envisions the development of software for personal devices such as mobile phones and tablets that can receive, interpret, and display the Remote ID information, allowing the public to be aware of drone operations near them. This will inevitably empower the public to report any improper or suspicious drone usage to law enforcement and the regulator, making them partners in enforcing compliance with Remote ID and other drone regulations.

The ease with which the public will be able to generate complaints to law enforcement or the regulator using such Remote ID monitoring applications on their personal devices is controversial because it appears to target drone operators for enhanced accountability. The prospect that Remote ID broadcasts could be captured and used as evidence leading to legal sanctions including fines for drone operators, in a manner like the present use of Photo Radar against motorists, is seen by many as an unwelcome and unwarranted expansion of the "surveillance state".

As Remote ID is phased in it will also place an obligation onto drone users to upgrade their drones, or even purchase new drones, to be compliant with the regulations. This will create a financial burden that will be borne by drone operators.

Remote ID is Mandated in the United States

The Remote ID rule applies to all drones that require FAA registration (i.e., weighing 0.25 kg or more), that are engaged in commercial operations under Part 107, and to Foreign Registered drones that operate in U.S. Airspace. There are three ways to be compliant:

1. Operate a "Standard Remote ID Drone" that broadcasts the required data message as an essential part of is operation, using technologies that are integrated into the drone during its production. This is expected to be the normal path to compliance for drones that will be manufactured with this rule in place (mandatory for manufacturers after October 2022).
2. Operate a "Remote ID Broadcast Module" as a separate device that is attached to the drone during its operation and broadcasts the required data message (which varies slightly from the Standard Remote ID data message). This provides a path to compliance for the existing fleet of drones which have not been manufactured with this rule in place.
3. Operate a drone without Remote ID, but only at specific FAA Recognized Identification Areas (FRIAs). This provides a path to compliance for the many Model Aircraft and Hobbyist drone users who do not want to or cannot use Remote ID Broadcast Modules on their drones. It does however restrict them to specific geographic locations and forbids users from flying such drones anywhere else - even over their own property.

The Remote ID rule requires the drone to broadcast a Remote ID data packet at a rate of once per second (1Hz) over Wi-Fi or Bluetooth frequencies "from takeoff to shutdown". It further requires that the drone must not be able to launch if the Remote ID is not functioning after a pre-launch self-test, and the drone must land "as soon as practicable … while using aeronautical decision making" if the Remote ID fails in flight. In addition, the Remote ID implementation must be "tamper proof". Hence, the FAA is making Remote ID a critical flight system for drones.

Significantly, Standard Remote ID will be required for any drone that will operate Beyond-Visual-Line-of-Sight (BVLOS). Retrofitting an existing drone with a Remote ID Broadcast Module will not make it eligible

for BVLOS. Hence, the FAA is in effect decreeing that the existing fleet of drones are unsuited to BVLOS, and only future Remote ID compliant drones - yet to be manufactured - will be allowed to conduct BVLOS flights. (For the time being the FAA Waiver System for BVLOS remains available. However, the likelihood that a non-compliant drone will be granted a waiver once compliant Standard Remote ID drones become available is vanishingly small.)

The rule also outlaws the use of ADS-B Out on drones to avoid oversaturation of the ADS-B system and preserve function for manned aviation. (There is an allowance for the existing fleet of ADS-B equipped drones to continue to operate within U.S. airspace under Air Traffic Control (ATC) direction).

Remote ID is under Consideration in Canada

Currently, Canadian Remotely Piloted Air Systems (RPAS) operations require special permitting to fly in controlled airspace and Beyond-Visual-Line-of-Sight (BVLOS) and are separate from manned aviation operations. Beginning in 2019 the Trials Executive Steering Committee (TESC), which was made up of representatives from Transport Canada (TC), NAV CANADA, and the Department of National Defence (DND), was mandated to establish the technical and operational requirements for RPAS to operate routinely in Canadian airspace with conventional aircraft. In May 2020, the TESC issued a "RPAS Traffic Management (RTM) Services Trials Call for Proposals Phase 1-Round 1" to identify the necessary services for an air traffic management system for RPAS in Canada, within which they defined 29 services for Canada's RTM System. (Figure 1)

Remote Identification was marked as a service for implementation in Phase 2 of the TC RTM plan.

The Canadian Drone Advisory Committee (CanaDAC) was convened for a two-year term starting in May 2021 to advise TC regarding strategic policy to support the development of future RPAS policy and planning. Remote ID is among the many issues being considered by CanaDAC. A Remote ID Working Group has also been active but has not yet produced a report.

It is not known if the CanaDAC will be extended or renewed beyond May 2023, although this seems likely as many RPAS issues remain unresolved in Canada. If so, CanaDAC will most likely continue to be the primary forum at which the policy issues surrounding Remote ID in Canada are debated.

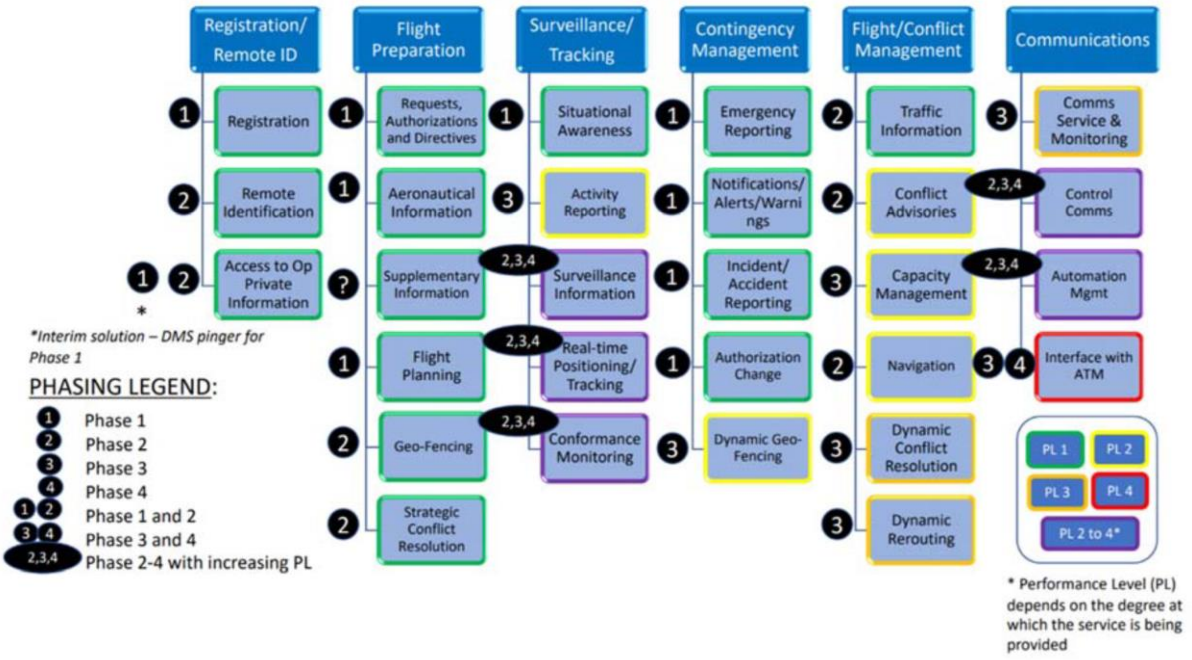

Figure 1 - RTM Services (Transport Canada, 2020)

DPAC POLICY POSITION

Recognition of the Importance of Remote ID for drones in Canada, with limitations:

- DPAC recognizes the potential for Remote ID to enhance the safe and responsible operation of drones in Canadian airspace.
- We believe Remote ID is not necessary for micro Remotely Piloted Aircraft Systems (mRPAS – under 250g).
- We believe that Remote ID should be optional for drones between 250g and 25kg.
- We believe Remote ID should be mandatory for drones over 250g operating BVLOS or when conducting other higher risk operations if Remote ID can be shown to measurably enhance safety.
- We believe that Remote ID should be mandatory for drones over 25kg.

Consideration of the Privacy Implications of Remote ID:

- DPAC recognizes the potential privacy implications of Remote ID, including the collection and sharing of personal data which could compromise the privacy rights of drone owners, operators, and pilots.
- DPAC calls for a thorough and transparent evaluation of the privacy implications of Remote ID, with appropriate measures put in place to protect the privacy rights of drone owners, operators, and pilots.
- DPAC calls for the operator or pilot location to not be provided to the public, as it could compromise the privacy and safety of the operator. Where RPAS manufacturers are currently

transmitting operator location to comply with FAA requirements, DPAC calls for a rule requiring that they explicitly block or encrypt that data transmission when operating in Canadian airspace.

- DPAC calls for the drone identity broadcast through Remote ID to be limited to providing the Serial Number of the drone only, which would provide sufficient information for regulatory and safety purposes while protecting the privacy of the owner, operator, and pilot.

Opportunity to Contest Enforcement Action:

- DPAC recognizes that enforcement action arising out of Remote ID findings could impact the rights and interests of drone owners, operators, and pilots.
- DPAC calls for an assurance that any enforcement action arising out of Remote ID findings would provide an opportunity for the accused to contest or explain the situation to an independent body, to ensure that the enforcement process is fair and transparent.

Accessibility and affordability of Remote ID solutions:

- DPAC recognizes that the implementation of Remote ID – if mandated - may impose costs on drone operators, including the purchase of new equipment or upgrades to existing equipment.
- DPAC calls for the development of accessible and affordable Remote ID solutions that are suitable for a wide range of drone operators, including hobbyists and commercial operators.

Adequate implementation time frame:

- DPAC acknowledges that the implementation of Remote ID may require significant changes to the way in which drones are operated in Canada.
- DPAC calls for a reasonable and adequate implementation time frame that allows drone operators to adjust to the new requirements and make necessary investments in Remote ID solutions.

Invitation to join CanaDAC (or its Successor):

- DPAC recognizes the importance of engaging with relevant stakeholders in the development and implementation of the Remote ID regulatory system.
- DPAC calls for the association to be invited to join the relevant strategic policy forum, such as CanaDAC or its successor, to ensure that the interests of recreational and small commercial drone pilots are represented and heard.

CONCLUSION

The Drone Pilots Association of Canada (DPAC) is a national organization representing recreational and small commercial drone pilots across the country. As a leading voice in the drone community, DPAC is dedicated to promoting the safe and responsible operation of drones in Canadian airspace, while also advocating for the interests of drone pilots and the broader drone community. Through its advocacy work and outreach activities, DPAC is working to ensure that Canada's drone regulations and policies are balanced, practical, and effective, and that the interests of all stakeholders are considered.

To this end, DPAC has developed a policy position on Remote ID which is designed to strike a balance between the need for accountability and transparency in drone operations and the privacy concerns of

drone pilots. DPAC believes that this balance is essential to ensuring that the interests of all stakeholders are considered and that any new policies or regulations are practical, effective, and proportionate.

DPAC's commitment to monitoring developments in the Remote ID space and engaging with relevant stakeholders reflects the organization's dedication to advancing the interests of its members and promoting the safe and responsible use of drones in Canadian airspace. By staying informed and engaged, DPAC can ensure that its policy position remains relevant and effective in the rapidly evolving landscape of drone technology and regulation.

ABOUT THE DRONE PILOT ASSOCIATION OF CANADA (DPAC)

The Drone Pilot Association of Canada (DPAC) is a rapidly growing voluntary association representing and advocating for close to 2000 registered members. Membership is free, and our members are primarily recreational and small commercial drone pilots who fly in Canada. The association is governed by a six-member steering committee that meets monthly to consider issues of interest or concern for the membership and meets quarterly with Transport Canada to discuss drone issues and regulations.

DPAC has a web presence at Home - Drone Pilot Association of Canada[5].

The official DPAC Facebook Group, which has over 4,300 members, can be found at Drone Pilot Association of Canada Group | Facebook[6].

Contact Us

This policy position paper represents to collective work of the DPAC steering committee. Please contact Stephen Bogner at Stephen.Bogner@gmail.com for questions or comments.

[5] https://www.dronepilotassociationofcanada.com
[6] https://www.facebook.com/groups/592682344571622