



TELSTRA CORPORATION LIMITED

Radiocommunications exemptions for law enforcement use of drone jamming devices

Public submission

13 July 2020



01 Introduction

We welcome the opportunity to provide our views to the ACMA's consultation on **radiocommunications exemptions for law enforcement use of drone jamming devices (consultation paper)**. We note in 2019, the ACMA made the *Radiocommunications (Unmanned Aircraft and Unmanned Aircraft Systems) Exemption Determination 2019* (the 2019 Exemption Determination) to facilitate access to and use of a defined counter-drone capability by the Australian Federal Police (AFP), which continues to be in effect. This consultation is proposing a very similar exemption but with far broader scope: it will apply to members of all Australian police forces, and it encompasses a far wider range of class licenced frequencies.

We agree with the ACMA's observation that rapid innovation in the drone technology environment has led to drones becoming more accessible and easier to use. As drone use becomes more widespread, there is also growing concern around malicious use of these devices and increased risk to public safety and national security. While we acknowledge there is public interest in providing counter-drone capability for law enforcement operations in response to threats, and we support the intention of this exemption, we are concerned about the following:

- we question whether the proposed exemption will deliver the outcome sought [C-i-C];
- technical details of the jamming devices are required by stakeholders to understand the potential impact to users of adjacent bands and the possibility that the devices might also technically be capable of accidentally jamming bands used for public mobile telecommunications services (PMTS), even if the proposed exemption does not allow for such conduct. Alternatively, if such detail is considered too sensitive to share with mobile carriers, appropriate oversight could be achieved by the ACMA using the accredited person scheme to certify the counter-drone equipment being used by the police would not interfere with PMTS services in adjacent frequencies;
- [C-i-C];
- expanding the use of counter drone devices to more agencies may result in an uncoordinated usage and increase the risk of disproportionate interference to communications networks; and
- as jamming devices are proliferated within our jurisdiction and their usage is increased, risk of misuse also goes up accordingly. As a result, we believe there is a higher risk of an unintended consequence that these jammers will impact mobile networks.

Therefore, we strongly recommend that the exemption determination should have express protections against interference into frequency ranges used for PMTS that may potentially be impacted by these devices.

Finally, drone security needs a holistic range of options to manage low altitude airspace management, including electronic tracking and registration of drones – jamming is only one part of the solution.

Our thoughts are explained in more detail below.

02 Our views on the proposed exemption determination

2.1. Limitations of drone jammers

The proposed determination authorises operation of drone jamming devices across numerous frequencies set out in the *Radiocommunications (Low Interference Potential Devices) Class Licence*



2015 (the Class Licence), including frequencies available for use on a shared basis by industrial, scientific and medical (ISM) devices. Additionally, frequency ranges set out in a footnote to the *Australian Radiofrequency Spectrum Plan 2017* (ARSP) may also be jammed. This significantly expands the frequency ranges authorised for operation of drone jamming devices, compared to the 2019 Exemption Determination. In the consultation paper, the ACMA explains that while the majority of drones operate in the 2.4 GHz and 5.8 GHz bands (used for WiFi):

*"spectrum requirements for drones are becoming more varied, and the pace of technological change and innovation could see unexpected changes. Currently, drones could also conceivably operate across a number of frequency bands provided for under the Class Licence. Additionally, drones manufactured overseas may be configured to comply with overseas spectrum regulatory arrangements which are not always the same as those implemented in Australia."*¹

We agree with this observation, however expanding the range of class-licensed frequencies is at best only a temporary and partial response, because drone technology is advancing beyond just relying on various class licenced frequency bands. [C-i-C]

[C-i-C]

Therefore, we are concerned that devices permitted by the proposed exemption will not fully deliver the desired outcome. An approach that relies on jamming is reactive and not adequate for resolving the problem. [C-i-C]

In the longer term, we believe drone security needs to be considered more broadly as part of the whole of Government response to this issue (as referred to in Recommendation 5 and 8 in the Australian Government response² to the Senate Standing Committee report into the *Current and future regulatory requirements that impact on the safe commercial and recreational use of Remotely Piloted Aircraft Systems (RPAS), Unmanned Aerial Systems (UAS) and associated systems*) that considers how best to manage low altitude airspace, including electronic tracking and registration of drones.

[C-i-C]. [C-i-C]. [C-i-C]. We believe that as a regulatory agency with significant technical expertise in radiofrequency spectrum matters, the ACMA has an important role to play in advising other government agencies on this issue.

2.2. Technical details of the jamming device are required to understand the potential impact to users of adjacent bands

We have not been provided with the specification of the technical characteristics of the drone jammers proposed for use by the police. Without an appropriate explanation of the technology being used, it is difficult to accurately assess the risk of potential interference to users of adjacent frequencies. [C-i-C]

Given licensees of adjacent frequencies will not be given prior notice of the use of these devices in cases of emergency, it is essential the ACMA make technical details of the transmitters used in these devices, including power output levels (EIRP), centre frequency, bandwidth and emission masks, available to

¹ Consultation paper; p9.

² Australian Government response to the Senate Standing Committee on Rural and Regional Affairs and Transport report: "Regulatory requirements that impact on the safe use of Remotely Piloted Aircraft Systems, Unmanned Aerial Systems and associated systems", November 2018, https://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Rural_and_Regional_Affairs_and_Transport/Drones/Government_Response



licensees of adjacent frequencies. This will assist adjacent licensees to predict the extent and type of interference that may be caused in the event these devices are used. In the event of any future interference to our networks, such information may be useful in identifying a signature associated with the use of such jamming equipment.

Alternatively, if the technical details of the jamming devices cannot be made readily available due to security sensitivities, we suggest the ACMA consider the accreditation scheme as a mechanism to ensure compatibility of jamming devices with other services in adjacent frequencies (i.e. an accredited person could certify the counter drone equipment being used by the police would not interfere with use of PMTS in adjacent frequencies). As the ACMA is aware, the accredited person mechanism under Part 5.4 of the *Radiocommunications Act (Cth) 1992* has been used successfully for interference management and coordination for many years and enjoys a high degree of confidence amongst mobile carriers.

2.3. The exemption determination should expressly protect PMTS frequencies

There is always a risk of misuse associated with jamming devices, whether purposeful or accidental. This risk increases as jamming devices are proliferated within Australia and their usage is increased. As a result, we believe there is a higher risk of an unintended consequence that these jammers will impact mobile networks. The ACMA's 2018–19 *Communications Report* notes that in the most recently measured period over 75% of emergency calls were made from mobile phones. This emphasises the need for protection of mobile communications from interference.

Therefore, we strongly recommend that the exemption determination should have express protections against interference into frequency ranges used for PMTS that may potentially be impacted by these devices. As we have suggested in the previous paragraph, this could be confirmed by certification by an accredited person, which would provide valuable independent oversight and reassurance for mobile carriers regarding the risk of potentially serious interference.

2.4. [C-i-C]

[C-i-C]

[C-i-C]

[C-i-C]

[C-i-C]

03 Notification protocol

Currently, [C-i-C]. In our view, a better way of ensuring mobile network operators are notified of any use of drone jammers, is through the use of a centralised database with a user interface that the police can access to record the necessary information about use of counter drone measures. The added advantage of such a system will be that all network operators will have a central place to refer to for instances of drone jammer use by the police. We will be happy to provide further input about this matter as a follow up to this submission.



Also, we believe the notification protocol can be bolstered by including accountability measures so that all parties can be confident that the protocol is used appropriately. [C-i-C]. This will help ensure compliance and provide mobile network operators with greater confidence that the information provided is accurate and up to date.