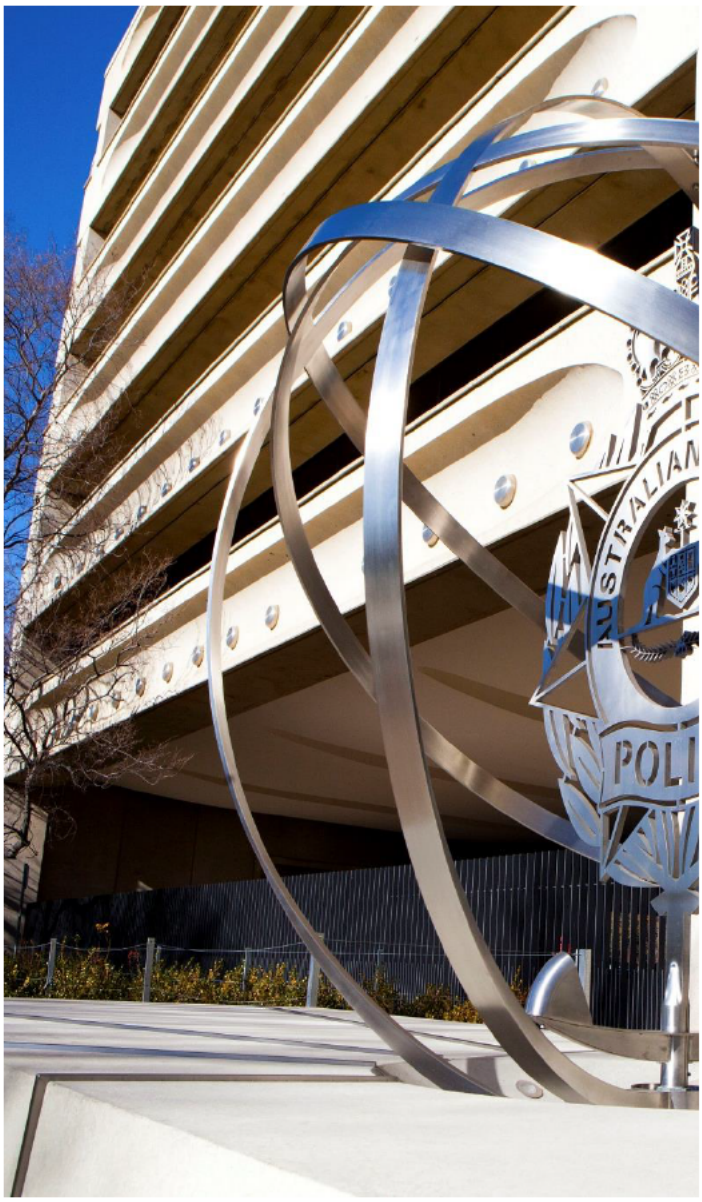
AFP
AUSTRALIAN FEDERAL POLICE



Parliamentary Joint Committee on Intelligence and Security

Inquiry into the Telecommunications Legislation Amendment (International Production Orders) Bill 2020

14 May 2020

Submission by the AFP (Responses to Questions on Notice)

This submission to the Parliamentary Joint Committee on Intelligence and Security inquiry into the Telecommunications Legislation Amendment (International Production Order) Bill 2020 provides AFP responses to questions taken on notice at the public hearing on 14 May 2020, including a diagram of AFP's understanding of the current Mutual Assistance Request (MAR) process and proposed International Production Order (IPO) process, and operational case studies.

Questions taken on Notice

Asked

Question Submitted by: *Senator Kristina Keneally*

Senator KENEALLY: Can I return to those 44 requests. What I'm trying to do is understand the types of information you're seeking now—the type and volume and how that volume and type may or may not change under this framework—because that will assist us to understand the usefulness of this framework. It will also assist us to understand the appropriate oversight that needs to be in place. Could you tell me, in relation to the 44 requests, about the types of information that you are requesting now and how that might change under an IPO regime in terms of both anticipated volume and anticipated content.

Mr Kent: Currently, the data that we provided in the opening statement around 44 requests in 2019 goes to a mix of requests that relate to other evidential materials and also communications data. I don't have those figures in front of me, but we could provide a breakdown of that data. We can certainly provide the committee with a breakdown of that data over the last five years, to characterise that more fully for the committee.

Senator KENEALLY: That would be useful.

Answer:

This response has been prepared with assistance from the Attorney-General's Department who hold data relating to the number of Mutual Assistance Requests (MARs) made to and from Australia.

Between 1 July 2014 to 30 June 2019, a total of 209 MARs were made to the United States (US) seeking evidence to assist AFP investigations. Of those, 98 MARs specifically sought communications data from US-based communications service providers.

Of these 98 MARs:

- 91 MARs sought both content internet data and non-content internet data (such as subscriber information and traffic data) and
- 6 MARs sought non-content internet data only, and
- 1 MAR sought subscriber data relating to telephone records.

While the type of assistance sought under an MAR is not categorised in the same way as the IPO Bill (ie. interception, stored communications data or telecommunications data) the above MARs would be categorised under the IPO regime as either 'stored communications data' or 'telecommunications data'. None of those requests related to interception.

Offence types

Of the 98 MARs made to the US for communications data to assist AFP investigations:

- 29 related to drug offences;
- 26 related to terrorism offences;
- 24 related to child sex offences;
- 11 related to money laundering offences;
- 4 related to foreign bribery offences;

- 3 related to human trafficking offences; and
- 1 related to a range of serious (unspecified) offences.

We note that MARs are made to assist investigations into serious criminal offending, which may include multiple offence types. In addition, a single MAR may seek data held by multiple US-based communication providers.

Asked

Question Submitted by: Senator Kristina Keneally

Senator KENEALLY: Thank you. My last set of questions goes to current investigations on foot. Are there any current investigations where you are waiting for the passage of this legislation and the CLOUD Act before taking the next steps?

Mr Kent: There are current investigations where we are currently utilising the MAR process as it stands. If new legislation were introduced, there are current investigations where we would move to utilise the changes in the legislation to greater effect.

Senator KENEALLY: Are you able to tell me whether that is the case in the investigations relating to either Sam Clark and Dan Oakes, with the Afghan file matters, or Annika Smethurst, in relation to the ASD matter?

Mr Kent: I'm not in a position today to provide that information, no.

Senator KENEALLY: Can I put that on notice.

Mr Kent: Yes.

Answer:

The AFP will not comment on ongoing investigations.

Asked

Question Submitted by: Mr Anthony Byrne

Mr BYRNE: It's good to talk to you. I just want to emphasise to you both that, in terms of the submission, it could help us as well if we could have—it sort of ties in with what Senator Stoker said—some case studies on how you might use it. It's not a criticism; it will just be useful. I think when we were having a discussion about metadata when Michael Phelan was there, as one of the deputy commissioners or assistant commissioners, he took us through how the metadata might be used, particularly given, if this bill is passed, we'll see a capacity for the AFP to get real-time information, which is related to what Senator Stoker was saying about child exploitation matters, terrorism matters or foreign interference matters. If we could just have from an AFP perspective some examples of how you might use that power, that would be very useful.

Mr McCartney: Yes, absolutely.

Answer

Please refer to the attached document outlining AFP understanding of the current MAR process, as well as operational case studies.

Asked

Question Submitted by: Mr Mark Dreyfus

Mr DREYFUS: I wasn't here for the past 20 minutes, because I had to go to the Federation Chamber. But I'm back, and sorry if I duplicate something that's already been done. I wanted to ask some questions just since you're here about the committee's other inquiry into press freedom. In particular I wanted to know whether it was still possible that Sam Clark, the journalist, will still be charged in relation to the Afghan files matter.

Mr Kent: We've certainly taken that question on notice in relation to that request.

CHAIR: I'm going to have to go down to the chamber, so over to you, Mr Byrne, to chair this.

Mr DREYFUS: Well, I'll ask about the other journalist: is it still possible that the ABC journalist Dan Oakes will be charged in relation to the Afghan files matter?

Mr Kent: We would take that question on notice.

Senator KENEALLY: If I might just clarify for Mr Dreyfus's benefit: I actually did not ask the question he's asking. You took a different question on notice. My question was whether or not you were waiting for this particular IPO regime to come into place before proceeding with those investigations. He's asking a different question, so, Mr Dreyfus, that might assist you to understand what was asked and taken on notice.

Mr DREYFUS: I'm indebted to Senator Keneally, and this is a different question than that. I'll ask it again: is it still possible that the ABC journalist Sam Clark will be charged in relation to the Afghan files matter?

Answer

The AFP will not comment on ongoing investigations.

AFP UNDERSTANDING OF THE MAR vs IPO PROCESS

Mutual Assistance Requests (MARs)

An **offence is committed against Australian law** and evidence is identified overseas. The **AFP** determines an MAR is required.

The **AFP** completes a Mutual Assistance Request questionnaire and sends it to **AGD** (in consultation with CDPP if it is required for prosecution or relates to a CT matter).

AGD drafts the MAR, and then sends back to **AFP** for comment. *Repeat until terms are agreed.*

AGD considers the request in the context of Australia's relationship with the foreign country, what the request asks for, Australia's domestic law and that of the foreign country.

AGD provides comments and suggests amendments.

AFP revises the draft adding any further information.

Repeat until AGD agrees with the MAR.

Attorney-General (or delegate) approves the request

AGD sends the request to the **Foreign Central Authority (FCA)** (after translation, if required), and then coordinates liaison between the AFP and FCA, including providing updates with respect to timeframes for required evidence.

FAC considers Australian MAR in accordance with its laws processes and priorities.

Three possible outcomes

1. **Foreign country sends the requested material or information to AGD.** AGD considers requirements under the *Foreign Evidence Act,* and if appropriate, will *seal* the material and provide it to AFP or other agency.
2. **Foreign country requests further information before it can complete the request** - AGD will liaise with CDPP and AFP for further information. *Repeat until foreign country has all the required information.*
3. **Foreign country notifies AGD it cannot comply with the**

International Production Orders (IPOs)

An **offence is committed against Australian law** and evidence is identified overseas. The AFP determines an IPO is required to access data held overseas.

The **AFP** drafts an IPO application, with supporting affidavit to establish grounds (threshold of "reasonably suspects")

AFP sends application and affidavit to the **issuing authority** (Judge or approved AAT member).

Issuing authority considers the Application against the legislative criteria; and if appropriate *issues* the IPO

The AFP must give the IPO, or a certified copy, to AGD *as soon as practicable* after it is issued.

- AGD **must** consider whether the order complies with the designated international agreement nominated in the order.
- If *satisfied* that the order complies, AGD must give the order, or a certified copy directly to the designated communications provider (DCP) based in the foreign country *as soon as practicable* after becoming so satisfied. The order comes into force when it is given to the DCP.

(note, if AGD is not satisfied that the orders complies, then AGD **must** cancel the order, return it to the AFP and give the AFP advice in relation to the compliance).

Absent any objection, the DCP **must** produce the relevant content in accordance with the order:

- **Interception or Telecommunications IPO:** Disclose any such interception or telecommunications content or data to the AFP;
- **Stored Communications:** The Issuing authority will specify that the content be provided directly to either AGD or the AFP.

Operational Case Studies

The AFP has prepared a number of case studies based on current and previous investigations. The examples are based on real AFP operations, however they have been de-identified and de-classified. The case studies highlight the challenges and limitations experienced by the AFP under the current MAR process. They demonstrate how the International Productions Orders Bill will create a more streamlined and time efficient framework to obtain electronic evidence located offshore to progress criminal investigations.

The Bill also allows for interception, meaning that a designated communications provider obliged to comply with an International Production Order may be required to provide a specific communication to a single destination in real-time access to the AFP to that communication.

Case Study One – Child exploitation investigation

Technical obstacles and delays in the MAR process

Investigation Summary

The AFP commenced an investigation after receiving intelligence from foreign counterparts that a child within that jurisdiction was being groomed by an Australian individual.

The AFP investigation identified that child abuse material (CAM) was contained on the individual's devices, however specific content and data was not visible to law enforcement on the devices themselves as it was stored on the servers of carriage service providers in the United States and United Kingdom.

MAR Challenges

The AFP initiated the MAR process with the Australian Central Authority and requests were made to both the US and the UK to obtain evidence in an admissible form.

Throughout the investigation and in conducting reviews of material, the AFP identified a number of fake personas and a significant number of potential other victims both within Australia and overseas.

The process of victim identification is complex and time-consuming requiring specialist analysis. This was exacerbated by a significant amount of content required to be obtained from overseas through the MAR process – causing delays.

The AFP ultimately received working copies of the evidence sought from one country after approximately 9 months. It was nearly 2 years before the AFP received information from the other country, and when received the data was provided in a format, which required extensive in-house resources and analysis.

In total, it took almost 3 years from the date of initiating the MAR process to receive working copies of the relevant material, with a further 18 months until receipt of the formally sealed MAR material.

The delays faced in using the current MAR processes not only frustrate the investigative process, but provide an opportunity for suspects to continue offending throughout that time, potentially resulting in further victims, and prolonging the trauma experienced by current known victims.

This was evident in this case, where victims continued to be impacted while awaiting the MAR material so that the AFP could progress the investigation.

This is not an uncommon scenario in child exploitation cases.

Alternative Impact if an IPO was available

An IPO would have allowed the request to be quickly directed to the relevant provider, who would then be in a position to provide the content or data directly back to Australian authorities, likely within a much shorter timeframe.

This would have assisted to address the real issue of continued offending and trauma to new and current victims in these types of cases.

Potential use of Interception IPO

As the offences under investigation (5 offences under division 474 of the *Criminal Code Act 1995 (Cth))* attracted a penalty of more than 7 years imprisonment, the AFP could apply for an Interception IPO if other criteria was met.

An Interception IPO would have been provided to a social media platform/messaging service, to facilitate real-time interception monitoring of that service as communications are occurring. This would support investigations allowing rapid identification of child abuse networks, victims and perpetrators. This would allow law enforcement to swiftly respond to protect this vulnerable demographic, avoid continued offending and trauma to identified and future victims, identify and further investigate additional perpetrators.

Case Study Two – Child exploitation investigation

Delays on behalf of overseas jurisdiction

Investigation Summary

The AFP was investigating an individual who was blackmailing a juvenile to produce child abuse material (CAM). The AFP identified content held by a carriage service provider located in a foreign country, which was crucial to prove elements of the offence. Accordingly, the AFP initiated an MAR with the Australian Central Authority.

MAR Challenges

In this case, there were significant delays with the foreign Central Authority progressing the MAR and seeking the material from the provider.

The AFP received the material 9 months after initiating the MAR process. In the meantime, the offender continued to produce CAM and was distributing it to contacts, resulting in ongoing offending and harm to the victim.

The material obtained via MAR was fundamental for investigators to be able to link the offender to the production of the CAM.

As a consequence of this delay over a 9 month period, the offender was also able to actively use another online forum, potentially to groom further victims.

Alternative Impact if an IPO was available

An IPO would have allowed the request to be quickly directed to the relevant foreign provider, who would then be in a position to provide the content or data directly back to Australian authorities, likely within much shorter timeframes.

Any reduction in timeframes in this matter would have significantly hindered the offender in being able to continue using forums to identify and target other victims, while reducing the overall length of the investigation (including reducing strain on AFP resources) and initiation of a more timely justice process.

Case Study Three – Cybercrime investigation

Difficulty meeting foreign thresholds for evidence via MAR – causing delay and enabling crime to continue

Investigation Summary

The AFP was investigating an Australian individual who developed, advertised and sold malware, specifically a Remote Access Trojan (RAT), using a domain and related services. While similar to legitimate RAT software used by ICT helpdesks to service remote clients, the RAT differed in that it contained non-legitimate features such as covert deployment, covert webcam operation and keylogging.

MAR challenges

The AFP first approached the Australian Central Authority to make an MAR in this matter in November 2018. As at April 2020, the request remains ongoing and ***no*** *material has been received to date.*

The AFP faced practical difficulties in meeting foreign evidentiary thresholds to obtain relevant data. For example in order to preserve content while the MAR process is pending, the AFP must meet the foreign country threshold of 'probable cause' that the data is:

a. located with the overseas provider and

b. that it is content and not merely subscriber details.

The AFP was advised the foreign provider would not provide email content unless we were able to demonstrate that the specific emails we were seeking directly related to the offending. This in effect required the AFP to obtain the evidence it required from the foreign provider, before we could meet the evidentiary threshold for that information to be released pursuant to an MAR.

The telecommunication company concerned will only keep data for 360 days before that data is destroyed. Under current MAR arrangements this may be insufficient time for the data to be secured.

Alternative impact - if an IPO was available

The AFP is confident there were 'reasonable grounds to suspect' the US provider had content relevant to the entire spectrum of the alleged offender's conduct. If the AFP had been able to obtain an IPO from an Australian issuing authority, it would allow a request to the Australian Central Authority and then directly to the foreign service provider much more quickly, so that relevant content data could be provided to further the investigation with less time for the risk of the individual moving infrastructure to obstruct law enforcement efforts. Obtaining the evidence faster would also allow the AFP to arrest alleged offenders, confident that the foreign evidence required for prosecution would be available in time for the AFP to submit briefs to court.

Potential use of Interception IPO

As the offence under investigation involved unauthorised modification of data held in a computer (under section 477.2 of the *Criminal Code Act 1995)* and is a Commonwealth offence involving the misuse of a computer or electronic communications (under section 11.2 Criminal Code), it attracted a penalty of up to 10 years imprisonment. This means the AFP could apply for an Interception IPO if other criteria was met. Such an order would have allowed real-time monitoring of email communications to establish fault elements of offending and identification of additional malicious actors and their victims for further investigations.

Case Study Four – Cybercrime investigation

Timeliness of obtaining evidence via MAR – causing potential court difficulties and delays or inability to admit critical evidence

Investigation Summary

In a similar matter involving interference with a software product by Australian individuals, the AFP approached the Australian Central Authority to make an MAR in April 2017 to obtain evidence in admissible form to support prosecution.

At the time the prosecution commenced in March 2019 (nearly 2 years later), no material had been received via the MAR. The alleged offenders subsequently entered guilty pleas and the Australian Central Authority wrote to the foreign Central Authority in June 2019, to advise that the assistance sought under the MAR was no longer required.

MAR challenges

If the defendant had pleaded not guilty the matter would likely have proceeded to trial. The significant delays in not receiving the MAR material would have resulted in either:

a. the court not having the opportunity to consider critical evidence to support the prosecution case, or

b. the trial could have been delayed to await the MAR material- leading to delays in the justice process.

There are so many factors that impact timing, and so many experiences with delay in the MAR process, that the AFP generally progresses cybercrime matters via summons rather than arrest. This is due to concerns that should individuals be arrested, the AFP may not be able to adhere to evidence brief timing requirements, usually due to the need for evidence held by foreign providers, which needs to be obtained via MAR.

Alternative impact - if an IPO was available

The AFP is confident there were 'reasonable grounds to suspect' the foreign provider had content relevant to the entire spectrum of the alleged offender's conduct.

If the AFP had been able to obtain an IPO from an Australian issuing authority, it would allow a request to the Australian Central Authority and then directly to the foreign service provider much more quickly, so that relevant content data could be available in an admissible form to support prosecution.

In addition, where we are confident admissible evidence would be available more quickly, the AFP may be more inclined to arrest alleged offenders and ensure they cannot continue criminality while awaiting prosecution.

Case Study Five – Counter terrorism investigation

Delays obtaining evidence via MAR – resulting in ongoing national security risks while sufficient evidence is sought to make an arrest

Investigation Summary

The Queensland JCTT conducted an investigation into three Australians suspected of committing terrorism offences. A number of MARs to foreign countries were required to progress the investigation, including for social media content and related evidence held with foreign providers.

MAR Challenges

The key challenge was obtaining this evidence in a reasonable timeframe. Following lengthy delays, some material was obtained from one country, but only as a result of Australian authorities travelling to that country to assist authorities to obtain the evidence.

Material sought from the other countries remains outstanding 12 months later.

This is not uncommon in counter terrorism investigations. Delays and difficulties in obtaining useful evidence in admissible form from overseas jurisdictions frustrates these already complex investigations, and in many cases may pose a genuine national security risk.

Alternative Impact if an IPO was available

The time critical nature of responding to potential terror threats, and the necessity to be able to rapidly obtain crucial evidence (particularly in an admissible form), often from multiple jurisdictions simultaneously, highlights the need for IPOs.

An IPO obtained domestically would have allowed the request to be quickly directed to the relevant provider, who would then be in a position to provide the content or data directly back to Australian authorities, likely within much shorter timeframes.

Potential use of Interception IPO in counter-terrorism investigations

As terrorism offences attract a penalty of more than 7 years imprisonment, the AFP could apply for an Interception IPO if other criteria was met. In certain circumstances (for example, where the AFP is investigating a terrorist group at the attack planning stage), an Interception IPO could assist to monitor the communications of suspects in real-time, and allow police to act, before the planned attack presents an imminent threat to life.

Although there are other avenues for the AFP to obtain information in life-threatening situations (for example, via police-to-police assistance with a foreign counterparts), interception could present an opportunity for the AFP to obtain real-time actionable evidence for a more timely response, prior to the situation escalating to an imminent threat.