AFP
AUSTRALIAN FEDERAL POLICE

Independent National Security Legislation Monitor

Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018*

September 2019

Submission by the Australian Federal Police

Table of contents

Introduction

1. The Australian Federal Police (AFP) welcomes the opportunity to make a submission to the Independent National Security Legislation Monitor (INSLM) Review of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (TOLA Act).

2. The AFP is an operational agency, and this submission naturally directs towards providing the INSLM with insight into the operational policing matters arising from the Terms of Reference for this Review. The AFP's submission should be read in conjunction with the Department of Home Affairs submission, which provides a broader policy perspective and on which the AFP was consulted.

Overview of powers provided to the AFP under the TOLA Act

Schedule 1: Industry Assistance Framework

3. The industry assistance provisions provide a technologically neutral industry assistance framework, comprising:

   - **Technical Assistance Requests** (TARs), which facilitate the AFP to seek designated communications providers to provide voluntary assistance.

   - **Technical Assistance Notices** (TANs), which allow the AFP to require designated communications providers to provide assistance they are capable of providing.

   - **Technical Capability Notices** (TCNs), which allow the AFP to require communications providers to build a new capability.

   Assistance to law enforcement from telecommunications industry providers has been available under section 313 of the *Telecommunications Act 1997 (Cth)* for over 20 years. While the AFP has successfully used the provisions of s313 since its enactment, the drafting of these provisions gave rise to differing interpretations, leading to inconsistency of responses from providers on their requirement to assist. The effectiveness of the provisions was also reduced due to technological advances in telecommunication services. Schedule 1 provides clarity (and subsequently more explicit and limited application) to the telecommunications industry assistance arrangements, and expands to providers and services not contemplated when the Telecommunications Act was drafted.

Schedule 2: Computer Access Warrants

4. The Computer Access Warrant (CAW) provisions provide the AFP with a covert investigative tool to obtain a warrant to physically or remotely search electronic devices and access all data on those devices. These provisions create a new capability and expand on what is permitted under a warrant issued under the *Surveillance Devices Act 2004 (Cth)*, in particular the limitation that a data surveillance device did not permit a search of electronic devices but only the monitoring of inputs and outputs to that device. The CAW provisions acknowledge that whilst large volumes of communications are now encrypted in transit, they are not always encrypted when at rest, thereby providing an alternative point of accessing otherwise unintelligible information. It also acknowledges that anonymising technology means that accessing end-point devices may attribute criminality and identify persons involved that is otherwise unattributable.

Schedule 3: Law Enforcement Search Powers

5. Amendments to the search warrant provisions in the *Crimes Act 1914* (Crimes Act) improve the operation of electronic evidence gathering processes under overt search warrants

issued under section 3E including increasing penalties for non-compliance with a compulsion assistance order for serious offences to incentivise persons connected with a device to provide reasonable assistance. There is also clarity around the types of actions that are required to be commonly employed on electronic devices to access, identify and preserve evidence that is prescribed within the search warrant.

6. In particular, the expanded powers:

- **Modernise Crimes Act Search Warrants**
  - The AFP now has 30 days to examine devices relocated for forensic processing under section 3K.
- **Increase penalties for non-compliance**
  - The maximum penalty for failing to comply with a section 3LA order is now 5 years and/or 300 penalty units, or, for a serious offence or serious terrorism offence, 10 years and/or 600 penalty units.
- **Allow access to Account-based Data**
  - Section 3F was amended to expand the types of actions that may be authorised by a search warrant to include:
    - using electronic equipment to access 'relevant data' that is held in a computer or data storage device found in the course of a search.
    - using electronic equipment to access 'relevant account-based data' (i.e.: cloud hosted data) in relation to a person who is (or was) an owner, lessee or user of a computer found in the course of a search, and
    - adding, copying, deleting or altering other data, if necessary to obtain access to the relevant data or account-based data.
  - We note the recent public attention relating to the power to 'add, copy, delete or alter other data'. This is an action used solely to obtain access to relevant data, or relevant account-based data, held on a computer system. This amendment is not directed at authorising officers executing a search warrant to destroy or modify the contents of documents on electronic devices. It acknowledges that to access data, modifications may be required to be made to data on the device which could include – adding software and copying data from the device to enable it to be searched and deleting or altering data such as a password to bypass electronic security. These are all inevitable activities in accessing, searching and preserving electronic data with modern technology.

1. Appropriateness of Safeguards

General Comments

7. The powers provided to the AFP in the TOLA Act are supported by strong safeguards and oversight measures that protect the privacy of Australians citizens as well as the security of the digital environment, and ensures the powers are exercised effectively and responsibly.

8. Schedule 1 (Industry Assistance Framework) does not permit the access, collection or provision of personal or communications data without an accompanying appropriate warrant issued by an independent authorised judicial officer, or internal authorisation from a specified delegate. The AFP has reserved delegation for the issuing of TAR and TANs to

the Commissioner or Deputy Commissioners, being the two most senior sworn roles in the AFP.

9. Schedule 2 requires a warrant to be issued by an eligible judge or AAT member, and

10. Schedule 3 similarly requires a warrant to be issued by a person employed by a court who is authorised to issue warrants, such as a judicial officer.

11. The AFP considers a key safeguard is the extensive authorisation and accountability framework surrounding the management, collection and storage of personal information, particularly where that information is obtained through intrusive means.

12. As well as complying with legislative requirements, discussed below, the AFP also has a comprehensive internal governance framework as well as a Professional Standards Unit which maintains, promotes and enhances integrity in the AFP through a proactive integrity framework and prevention strategies and conducts investigations and review of exercise of powers.

13. In terms of external oversight, the AFP is subject to the scrutiny of the Commonwealth Ombudsman, the Australian Commission for Law Enforcement Integrity, the Senate Standing Committee on Legal and Constitutional Affairs, the Parliamentary Joint Committee on Law Enforcement, the Parliamentary Joint Committee on Intelligence and Security, and the Information Commissioner.

14. Finally, the use of powers by the AFP is also tested whenever information derived from those powers is led as evidence in court.

Privacy Protections

15. The *Privacy Act 1988 (Cth)*, Part 13 of the Telecommunications Act (protection of communications), the *Telecommunications (Interception and Access) Act 1979 (Cth)* (TIA Act) and Australian Privacy Principles (APPs) (particularly APP 11.2 which requires entities to destroy personal information when it is no longer required for legitimate purposes) regulate the use, disclosure and destruction of personal and communications-related information by the telecommunications industry.

16. The Privacy Act currently requires regulated entities to adopt a risk-based approach to protecting personal information in their possession from misuse, interference or loss, as well as from unauthorised access, modification or disclosure. The guidelines to the APPs issued by the Australian Information Commissioner, explain that entities must consider a range of factors when determining how to protect information they hold, including the amount and sensitivity of the personal information, and the possible adverse consequences for an individual. In particular, the guidelines state that '[m]ore rigorous steps may be required as the quantity of personal information increases'.

17. Under section 309 of the Telecommunications Act, the Information Commissioner oversees compliance by telecommunications providers with Part 13 of that Act. This includes monitoring the record-keeping of service providers and ensuring that the grounds for disclosures under Part 13 are recorded by service providers and authorised by the Telecommunications Act and the TIA Act.

18. Service providers also voluntarily comply with industry codes and standards that apply over-and-above legislative measures.

External Oversight

19. The TIA Act, the Surveillance Devices Act and the Crimes Act have safeguards and prohibitions in place in relation to search warrants, surveillance device warrants and

controlled operations, to ensure the careful management of any information obtained through the use of an intrusive method. For example, any information obtained is to be kept in a secure place with access restricted to only those who are entitled to deal with it.

20. The Commonwealth Ombudsman is empowered to inspect the exercise of these powers and activities conducted under these regimes and the industry assistance regime, in connection with warrants or authorisations granted by legislation. The Commonwealth Ombudsman may inspect the records of a law enforcement agency to determine compliance with these notification requirements and provide a written report on the results of inspections to the Minister for Home Affairs.

21. The Commonwealth Ombudsman is exempted from the unauthorised disclosure provisions in the TOLA Act, which protect industry assistance request and notice information. As such, these officials may disclose this information as necessary in the course of performing their oversight duties. These disclosures may include giving information to a State or Territory inspecting authority charged with overseeing an interception agency based in that jurisdiction.

22. The AFP's Telecommunications Interception Division continues to support the office of the Commonwealth Ombudsman's oversight and inspection duties under the TIA Act, Surveillance Devices Act and Crimes Act. From February 2018 to present, the Commonwealth Ombudsman has conducted seven (7) inspections under the various pieces of legislation. The AFP was found to be compliant during these inspections.

23. In the AFP's view, the combination of internal and external accountability and oversight within which the AFP must comply, including specific legislative regimes which contain penalties for misuse of information, provides sufficiently robust safeguards. While the AFP would of course comply with any additional oversight measures considered necessary and appropriate, we would be concerned if any such measures were duplicative, excessively onerous, or otherwise impeded the ability of law enforcement agencies to exercise, or provide support for, legitimate law enforcement, intelligence and related functions.

Schedule 1: Industry Assistance Framework

24. The AFP has developed a positive and consultative working relationship with Carriers and Carriage Service Providers in relation to the mandatory assistance requirements under section 313 of the Telecommunications Act and we have continued to utilise this relationship model in relation to engagement with designated communications providers under Schedule 1.

25. The AFP's preference is for assistance to be provided voluntarily but we acknowledge it must be guided by the preferences and input of the provider in assessing whether a TAR, TAN or TCN offers the most appropriate conduit to the provision of the assistance. In determining the most appropriate request or notice, invariably the provider needs to be consulted to establish whether the assistance will be provided voluntarily, as to whether it is something they are already capable of providing, and in considering whether the assistance is practicable and technically feasible. Early and ongoing engagement between the AFP and our industry counterparts is helpful in facilitating these requests.

26. In particular, the advice, expertise and knowledge of the providers in their eligible services is invaluable to the Commissioner (or delegate) in satisfying themselves that the assistance is proportionate, reasonable, practicable and technically feasible before issuing any request or notice for assistance.

27. The legislation governs the extent to which the industry assistance framework can be used. Under section 317ZH, interception agencies cannot issue a request or notice in order to undertake activities that require a warrant or authorisation. For example, an assistance notice cannot require the provider to intercept, retain or provide personal, subscriber or

communications data. An assistance notice may, however, require a provider to convert data collected pursuant to a warrant or authorisation into an intelligible format, or to divert a communication subject to a warrant entitling the AFP to access these communications.

28. Further, while the AFP does not have a mechanism to obtain a warrant extraterritorially to intercept or request communication providers data, section 317ZH providers an additional safeguard against this by expressly preventing such assistance, even if voluntary.

29. Interception agencies are required to notify the Ombudsman of their use of the industry assistance powers. Specifically the Ombudsman must be notified within 7 days that a request had been given, varied, revoked or extended. This requirement applies to all industry assistance measures. The Ombudsman may also inspect the records of the AFP to determine compliance with these notification requirements and may make a written report on the results of these inspections for the Minister of Home Affairs.

30. It is the AFP's view that the above measures provide sufficient safeguards that balance protection of individual's privacy and the AFPs lawful use of these powers to progress serious criminal investigations.

Technical Capability Notices

31. In addition to the above measures, the TOLA Act contains additional safeguards specifically for TCNs, requiring that they must be approved by both the Attorney-General and Minister for Communications.

32. The TOLA Act also expressly prohibits the building of 'back-doors', or building a systemic weakness or vulnerability into a form of electronic protection, and cannot cause providers to jeopardise the information security of general users by making encryption less effective. TCNs cannot be issued to remove a form of electronic protection and cannot prevent a provider from fixing a vulnerability or weakness.

33. Further, the TOLA Act includes a review process for TCNs, where a provider can refer a TCN for review by both an independent technical assessor and legal assessor, who will assess whether the TCN is unduly intrusive.

34. These measures recognise the additional impact of TCNs on providers. In the AFP's view, these additional measures are sufficient to safeguard privacy and ensure TCNs are not used when there is a less intrusive and more appropriate method available.

AFP Commissioners Approval of State/Territory Technical Assistance Notices

35. Recommendation 7 of the PJCIS Advisory Report recommended a tiered approval system for state and territory-initiated Technical Assistance Notices (TANs), under which TANs would be submitted for approval to the AFP Commissioner before issuing to the recipient. The recommendation was focused on ensuring consistency in decision-making and reporting across jurisdictions. It was also recommended that, to give effect to this intention, the AFP Commissioner would be required to apply the same statutory criteria, and go through the same decision-making process, as if the AFP were the original issuing authority.

36. The AFP expressed concern during earlier PJCIS inquiries about such a role on a number of bases, and in particular:

- It is not appropriate for the AFP to interfere (or be seen to be interfering) with the operational independence of state and territory law enforcement, by second-guessing the independent decision-making process of state and territory law enforcement counterparts.

- It is not feasible for the AFP Commissioner to be required to review potentially long-term and complicated state or territory cases in order to be in a sufficiently informed position to revisit the original decision.

- Review by the AFP Commissioner could create additional time delays, costs and logistical challenges. Consideration by the AFP Commissioner of state and territory TANs would need to be prioritised against other competing AFP priorities. This could result in delays in the AFP Commissioner's review and approval.

37. In response to the PJCIS recommendation, the TOLA Act was amended to require state and territory initiated TANs to be *approved* by the AFP Commissioner. The Supplementary Explanatory Memorandum clarifies that approval in this context means coordination to reduce duplication and support consistency. It does not require that the AFP Commissioner assess the TAN as if the AFP were the original issuing authority.

Schedule 2: Computer Access Warrants

38. The AFP acknowledges the intrusive nature of CAWs and is committed to ensuring we use the least intrusive means of obtaining likely evidence. As discussed in respect of Schedule 1 above, all AFP activity is subject to internal and external oversight, and must comply with AFP internal governance frameworks.

39. The Attorney-General has a discretion to authorise Mutual Legal Assistance Treaty assistance with a CAW under the Surveillance Devices Act and arrange access to data held on a computer for a foreign country law enforcement agency, where an investigation or proceeding relates to a criminal matter involving an offence against a law of a foreign country punishable by three years imprisonment. The CAW is still required to be obtained from an eligible AAT member or judge.

40. The legislation also provides specific safeguards with respect to Schedule 2. The TOLA Act includes a specific safeguard similar to those that apply to surveillance device warrants, whereby the applying law enforcement officer must suspect on reasonable grounds that a relevant offence (being a serious offence attracting a maximum penalty of imprisonment for three years or more) has been or will be committed, an investigation is or will be commenced and access to the data is necessary to obtain evidence of the offence of offenders.

41. Further, a CAW requires applications to specify what is to be authorised, and an eligible judge or AAT member to be satisfied of the grounds for an application before issuing.

42. The AFP considers this represents a reasonable and appropriate set of safeguards.

Schedule 3: Law Enforcement Search Powers

43. The AFP believes existing general measures and safeguards, combined with those specifically contained in the TOLA Act, are sufficiently robust to achieve the right balance between protection of Australians' privacy and civil liberties, and enabling the AFP and partner agencies to protect Australians in today's rapidly changing digital world.

Modernised Crimes Act Search Warrants

44. Amendments relate to pre-existing overt search warrants powers under section 3E Crimes Act. Section 3E's existing legislative safeguards extend to these amendments, specifically that:

- judicial approval is required for a s3E search warrant;

- the issuing officer must be satisfied on reasonable grounds for suspecting evidential material is or will be on the premises or person within 72 hours;

- there is a time limit of seven days for execution from the date of issue
- the person executing the warrant must provide details to the occupier;

45. Additionally, the amendments regarding 'add, delete or alter' as discussed above, specifically address the inevitable changes that occur when interacting with data, and the steps required for law enforcement to access data in a way that does not leave a trace. For example, this allows law enforcement to interact with data on computers found on the premises, or account based data to obtain access to relevant data, if it is likely to be effective and is reasonable in the circumstance.

Increased Crime Act Assistance Order Penalties

46. These amendments relate to pre-existing powers under section 3LA assistance orders. Section 3LA's existing legislative safeguards extend to these amendments, specifically that:

- a magistrate must approve a s3LA assistance order,
- the Magistrate must be satisfied that there are reasonable grounds for suspecting that:

(i) evidential material exists,

(ii) the specified person is connected to the device and

(iii) the specified person has relevant knowledge and is able to access the device.

2. Proportionality to the threat environment

General Comments

47. The tempo and complexity of the criminal threat environment driving the operational urgency of the reforms in 2018 has not abated. The TOLA Act strengthens the AFP's ability to overcome technological impediments to our lawful access to digital content.

48. Communication technology and encryption underpins everyday modern communications and is advancing at an incredible rate and is contributing to the creation of ungovernable space, free from the rule of law.

- This includes communication devices with military grade encryption, remote wipe capabilities and secure cloud-based services.
- Additionally online platforms are increasingly being used to connect and store data for easy sharing, promotion and discussion or illicit material such as violent abhorrent material and child sexual exploitation.
- Anonymization combined with encryption technologies such as Virtual Private Networks and the TOR network provide relative anonymity and the ability to participate in criminality with relative impunity.
- The reach of modern technology means that criminals are no longer confined by jurisdictional borders and can be located in one country, with an online presence in another and reach thousands of victims in a third.

49. Serious criminals (including terrorists and child sex offenders) who have an understanding of law enforcement's technical impediments are known to deliberately use encryption

technologies to prevent police from lawfully accessing their criminal communications. This makes it increasingly difficult for the AFP to prevent, deter, disrupt and investigate criminal activity.

50. As such, the AFP has had to explore new capabilities and evolve to overcome these disruptive technologies. We need assistance to ensure existing powers do not become ineffective and that technology cannot be used to thwart the investigation of serious criminal offences and national security threats.

Operational Statistics and Examples

- The AFP has seen a continued increase in the volume of unintelligible encrypted intercepted communications. Encrypted communications are heavily used by both national security and organised crime targets.
- Since 2016, the AFP has prosecuted **20 individuals** for a range of terrorism-related offences where encrypted technology was used in an attempt to inhibit law enforcement investigation.
- In March 2018, the AFP in collaboration with the FBI (US) and RCMP (Canada) executed 25 warrants internationally (19 in Australia) relating to the sale and disruption of encrypted communications provider Phantom Secure, resulting in 5 individuals being indicted in the US on Racketeering charges.
    - In May 2019, the CEO was sentenced to 9 years jail and **US$80M in assets was seized** from Phantom Secure as the proceeds from knowingly supporting transnational criminal organisations through the provision of encrypted communications.
    - AFP analysis identified more than 10,000 handsets in Australia, all of which were immune to traditional lawful access technology.

3. Continuing necessity of the Powers

General Comments

Key Statistics

51. The below statistics demonstrate that these powers remain necessary to the furtherance and continued effectiveness of investigations and evidence gathering:

- **Currently**, over **90 percent of content** being lawfully intercepted by the AFP, uses some form of encryption. This impacts on the AFP's ability to investigate and prepare evidence for prosecutions.
- Encryption has directly impacted **around 200 operations** conducted by the AFP in the last 12 months, all of which related to the investigation of serious criminality and terrorism offences carrying a penalty of seven years or more.
- **By late 2020,** it is expected that **nearly all communications content** of investigative value will be encrypted.

52. The AFP understands the benefits of modern technology and the telecommunication industry's objective to provide a secure online environment for users. However this same technology is increasingly used by criminals to conceal illicit activities and evade investigative efforts. Criminal entities are astute to gravitating toward safe havens in which to undertake their criminality, whether these be defined by societal, legal or technical opportunities. While enhanced security and privacy should be the foundation on which all

technology and telecommunications are developed, these foundations also significantly enhance the opportunities for criminality to flourish without fear of detection and disruption by law enforcement.

53. While industry already plays a significant role in supporting investigations, the TOLA Act provisions remain necessary, to ensure that the assistance framework appropriately reflects a modern communications market characterised by a broader range of industry participants, enhanced information security and a shift from Carrier managed services to third party 'over-the-top' providers who have flourished in an unregulated and global market. The TOLA Act provisions provide an opportunity to re-calibrate the need to balance public security versus privacy. When contrasted with previous assistance requirements, the TOLA Act provides enhanced civil, criminal, operational, privacy and capability protections to both incentivise and support industry in meeting its public security obligations where an appropriate delegate has assessed these as necessary and proportionate.

54. The TOLA Act provisions provide necessary legal protections, confidence and clarity for both law enforcement and communications providers and ensure a broader range of communications providers are captured, such as overseas providers with end-users in Australia.

55. To date, these provisions have provided significant operational benefit to address a number of emerging and urgent operational issues and facilitated productive engagement on potential technical options. This has been, and continues to be, of significant value to the AFP's investigative effectiveness.

Schedule 2: Computer Access Warrants

56. As noted above, the AFP continues to ensure less intrusive options are fully explored prior to application for a CAW. This does not demonstrate that CAWs are unnecessary, rather that the AFP takes the application of such intrusive powers very seriously and with due consideration.

57. However, the ability to escalate to this level of access remains critical to ensure continued operational effectiveness and lawful access to content at an unencrypted point. CAWs are a necessary tool to allow law enforcement to effectively and efficiently search electronic devices and content on those devices.

58. The new powers address significant gaps in capabilities that apply under existing legislation. Most notably, in relation to data surveillance devices, while covert access is permitted, this is restricted to monitoring inputs and outputs, and does not enable access to historical evidential material stored on a computer. Other provisions are available, including delayed notification search warrants, which while covert, require the physical attendance at the warrant premises, to enable warrant execution thereby causing unnecessary physical intrusion and risk to AFP members where the warrant is only seeking access to data.

59. Communications can be accessed under stored communications warrants, however, these are only available in relation to information held by a Carrier, which poses substantial limitations as to the scope of material available under these powers. CAWs not only provide a more explicit warrant framework for covertly accessing computers, but also addresses the issue of data being encrypted in transit but not always at rest, allowing evidential material to be accessed and preserved before it is deliberately or incidentally destroyed, and allowing covert collection of evidence (including identifying proposed criminal activity and participants) to facilitate law enforcement intervention prior to the physical act being committed (e.g: drug importation or terrorist activity) thereby reducing the impact on victims and the broader public.

60. CAWs also allow law enforcement to intercept communications to facilitate access to relevant data, including access to premises (including third party premises), to remove a computer or device and the doing of anything reasonably necessary to conceal anything done under the warrant to protect the covert nature of computer access warrants and covert capabilities. This may include the deletion of access logs or software installed to facilitate the access and search for relevant data. This is essential to ensure that the persons that are the subject of the investigation are not prematurely alerted to the police investigation potentially resulting to the destruction or interference with evidence, counter measures being developed to identify police methodologies, alerting of other participants or fleeing prior to police intervention or criminal proceedings being instituted.

61. An AFP investigation into the use of a carriage service to make a threat of telephony style attacks against the Australian public and government telecommunications infrastructure. This was a parallel investigation to Victoria Police investigation of sabotage offences against Victoria Police stations and their Private Automatic Branch Exchange (PABX) telephony systems. Following the confirmation of a target computer suspected of enabling the commission of the offending, AFP obtained a CAW. The CAW enabled the AFP to covertly acquire the contents of multiple systems used by the offender in the commission of a variety of offences. Information obtained under this warrant informed various affidavits, identified multiple further avenues of Police enquiry and filled significant evidentiary gaps in relation to the alleged offending and better directed Police resources in relation to this investigation. Further a significant proportion of the material obtained under the CAW is relied on in a brief of evidence in relation to the accused.

Schedule 3: Law Enforcement Search Powers

Modernised Crimes Act Search Warrants

62. The AFP has utilised the search warrant provisions as amended by Schedule 3 of the TOLA Act to collect evidence from electronic devices found during search warrants since the amendments were passed. The majority of search warrants executed by the AFP identify and require the examination of electronic devices. Advances in technology such as smart phones, Chromebooks, cloud hosted storage including web-based email, backup storage, file sharing, office products and web based forums and social media platforms mean that it is increasingly difficult to pre-empt where digital evidence will be hosted. Increasing data volumes and security being applied to data (including encryption) means that accessing and identifying relevant data is taking longer, requiring the extension of movement powers from 14 to 30 days.

63. Amendments to allow officers to 'add, copy, delete or alter' data on a device during a search warrant is a necessary part of interaction with modern electronic devices such as smart phones which do not permit the removal of data storage to readily attach to a writeblocker as traditionally occurred with removable storage from desktop computers. As a result electronic devices are increasingly required to be powered on and specialist software installed to enable access and preservation of relevant data [thereby necessitating the need to add, copy, delete or alter data. Data such as passwords and other security features may be required to be altered or removed (ie reset or deleted), to enable access and identification of relevant data. The provisions to 'add, copy, delete or alter' data does not extend to other purposes such as deletion or altering of illegal possessed material (such as child exploitation or classified documents) or to mislead or prevent ongoing access by co-offenders.

64. The ability to overtly and remotely access data enables the use of higher speed equipment and larger bandwidth network connectivity to search and copy relevant data than may otherwise be available at the premises nominated in the warrant. Increasingly the AFP was being required to spend large periods of time onsite at warrants (e.g: including for periods longer than 12 hours) to access, search and copy relevant data prior to the amendment that permitted overt remote access. This was particularly disruptive to search warrants

being executed on commercial businesses and could cause undue attention and anxiety for families of suspects at private residences. Further the ability to perform such activity remotely without requiring to utilise equipment found at a premises can reduce the interaction with data on electronic devices located at premises which may alter and thereby compromise potential evidence located on these devices.

65. The hyper-connectivity of modern technology and increasing data volumes means that most modern devices will remotely store account based data, be it backups or primary data. Cloud based storage is both cheap and plentiful and provides an assurance to users that should they lose or damage their personal devices or change between devices that they can still access their data. This account based data can be a rich source of evidence and may include information that has subsequently been deleted and is therefore no longer accessible through examination or seizure of the device located at the premises or on persons the subject of the search warrant.

66. ***These provisions remain necessary to ensure the AFP can access intelligible communications needed for investigation and prosecution of serious crimes into a future where the way in which individuals (and businesses) store, use and engage with data has and is continues to be increasingly remotely hosted.***

Increased Crimes Act Assistance Orders Increased Penalties

67. The AFP provided two case studies in our public submission to the PJCIS (copied below) that demonstrate the necessity of non-compliance penalties. In both cases, the prospect of a significant penalty for non-compliance with a section 3LA order led to the person providing information which enabled devices to be unlocked, and access to encrypted digital evidence.

Case Studies to demonstrate necessity of the laws

AFP submission case study A: Investigation into the importation of illicit drugs

The AFP executed a section 3E search warrant on a premises following the suspected procurement and importation of illegal drugs with cryptocurrency via a dark web marketplace.

During the execution of the search warrant the accused was served a notice to assist in accordance with the updated section 3LA provisions. Following consideration of the order and being advised of the new penalties, the accused advised the AFP of the passwords to a number of devices as well as a number of cloud hosted accounts in which he had facilitated the importation. Through the provision of this assistance, the AFP was able to successfully access, identify and collect otherwise secure and encrypted communications and digital records as evidence of the alleged offending.

AFP submission case study B: Investigation into the distribution and possession of electronic child exploitation material

Following receipt of information relating to the distribution of child exploitation material the AFP executed a section 3E search warrant on a premises. The search resulted in the identification of several devices containing child exploitation material. However, a number of devices could not be accessed due to the application of encryption and electronic protections. Those devices that the AFP was unable to access the contents of at the premises were subsequently moved under section 3K for further examination, which did not prove successful.

The accused was issued a section 3LA order signed by a judicial authority to provide assistance. Following being advised of the conditions of the order and the penalties that can apply for non-compliance, the accused provided information to enable access to the contents of the locked devices, which identified further evidence.