Australian Government
Department of Home Affairs

Parliamentary Joint Committee on Intelligence and Security

Review of the mandatory data retention regime

Home Affairs Portfolio submission

Contents

Glossary of abbreviations

ACCC	Australian Competition and Consumer Commission
ACIC	Australian Criminal Intelligence Commission
ACLEI	Australian Commission for Law Enforcement Integrity
AFP	Australian Federal Police
ASIC	Australian Securities and Investments Commission
ASIO	Australian Security Intelligence Organisation
CCRs	Call charge records
Criminal Code	*Criminal Code Act 1995*
IGIS	Inspector-General of Intelligence and Security
LECC	Law Enforcement Conduct Commission
NSWCC	New South Wales Crime Commission
NSWICAC	New South Wales Independent Commission Against Corruption
NSWPol	New South Wales Police
POI	Person of interest
QCCC	Queensland Crime and Corruption Commission
QPol	Queensland Police
SAICAC	South Australia Independent Commissioner Against Corruption
TasPol	Tasmania Police
Telco Act	*Telecommunications Act 1997*
TIA Act	*Telecommunications (Interception and Access) Act 1979*
TSSR	Telecommunications Sector Security Reforms
VicIBAC	Victoria Independent Broad-based Anti-corruption Commission
VicPol	Victoria Police
VLR	Visitor Location Register
WACCC	Western Australia Corruption and Crime Commission
WA Police Force	Western Australia Police Force

Introduction

1. Section 187N of the *Telecommunications (Interception and Access) Act 1979* (Cth) (the TIA Act) stipulates that the Parliamentary Joint Committee on Intelligence and Security (the PJCIS) review the operation of amendments made by the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth) (the Data Retention Act) two years after the end of the implementation phase of this Act.

2. Since 2015, policy responsibility for this legislation has been transferred from the Attorney-General's Department to the Department of Home Affairs, as part of broader machinery-of-government changes. The Home Affairs Portfolio has prepared this unclassified submission, with input provided by each of the agencies able to access telecommunications data under the TIA Act.[1] The Australian Security Intelligence Organisation (ASIO) will also provide a separate, classified submission to the inquiry. The Australian Criminal Intelligence Commission (ACIC) and several other agencies will also provide separate unclassified submissions.

3. In administering the Data Retention Act, the Home Affairs Portfolio has found that the current two year retention period, combined with the oversight mechanisms, safeguards and data security guarantees within the legislation, provides Australian agencies with reliable and consistent access to telecommunications data, a longstanding investigative resource.

4. This submission outlines the role of data retention in Australia's national security and law enforcement framework, noting the investigative value of telecommunications data and describing how access to this information interacts with the privacy of Australians. It then discusses the Terms of Reference as set out by the PJCIS in detail.

Overview

Access to telecommunications data in Australia

5. Lawful access to communications in Australia is governed by the TIA Act. Introduced in 1979, the primary object of this Act is to protect the privacy of Australians by prohibiting access to live and stored communications. While limited exceptions to this prohibition exist, including where access occurs under the authority of a warrant, the structure of the legislation elevates the privacy of personal communications and subjects the use of intrusive powers to stringent thresholds.

6. The TIA Act also regulates access to a separate form of information and the object of data retention: telecommunications data. Telecommunications data is information about a communication, excluding the substance of the communication itself. It includes information such as the source, destination, date, time, duration, or type communication, as well as associated subscriber details. Importantly, access to this information does not allow investigations to view what has actually been communicated, but it does capture logistical details of a call, short message service (SMS) or other form of communication.

[1] *Telecommunications (Interception and Access) Act* (Cth), s 110A ('TIA Act').

7. While telecommunications data can be obtained under warrant, discrete and isolated access to this information was first introduced into the TIA Act through amendments made by the *Telecommunications (Interception and Access) Amendment Act 2007* (Cth). This Act established the provisions that permitted Australia's law enforcement and intelligence agencies to internally authorise the disclosure of telecommunications data from Australian carriers and carriage service providers. While agencies' access to this information has been regulated by the TIA Act since the commencement of the 2007 amendments, these same agencies could access telecommunications data through the then sections 282 and 283 of the *Telecommunications Act 1997* (Cth) (Telco Act) since 1 July 1997.

8. While the authority to authorise the disclosure of telecommunications data was transferred by the 2007 amendments from the Telco Act to the TIA Act, the legislative prohibition against its disclosure remains in sections 276, 277 and 278 of the Telco Act. These sections prevent a carrier and carriage service provider from disclosing information or documents that relate to the subscriber and logistical details of a communication (i.e. telecommunications data).

9. Chapter 4 of the TIA Act now hosts a number of limited exceptions to this prohibition in the Telco Act, including where a disclosure of telecommunications data is authorised by one of Australia's 21 key law enforcement or intelligence agencies and is reasonably necessary for:

    - the enforcement of the criminal law, or
    - the enforcement of a law imposing a pecuniary penalty or protection of the public revenue.

10. In the case of ASIO, a disclosure may be made if it would be in connection with the performance of ASIO's functions. The Office of the Commonwealth Ombudsman (or the Office of the Inspector-General of Intelligence and Security (IGIS) in the case of ASIO) oversights access to telecommunications data under this regime, including by conducting regular inspections and tabling reports to Parliament.

11. Requests for disclosures are made to carriers and carriage service providers, which include internet service providers (ISPs), who operate and deliver telecommunications throughout Australia and hold this data for a host of commercial and regulatory reasons. These businesses have always retained data for commercial purposes (in some cases for beyond two years) but inconsistent practices across industry impeded ready and reliable access to this information.

12. The Data Retention Act commenced in 2015 to address this issue. It did this by mandating that service providers retain certain types of telecommunications data for at least two years, thus providing additional guidance for industry and ensuring agencies have consistent access to a longstanding source of intelligence and evidence. However, the Act also established an enhanced framework around access to telecommunications data: restricting the number of agencies authorised to access telecommunications data under Chapter 4 of the TIA Act, creating a dedicated oversight regime, and introducing additional thresholds for data disclosures (including additional protections for journalist sources).

The value of telecommunications data

13. Access to telecommunications data is a critical investigative and intelligence gathering tool. It is used in almost all investigations into criminal activity, serious civil infringements and of intelligence matters. While this submission discusses the investigative value of telecommunications data throughout, a number of key benefits are noted by way of introduction.

14. Telecommunications data can be vital in all stages of an investigation but is particularly valuable in the early stages. For example, it may be used to:

    - identify suspects, associates and criminal networks,
    - identify patterns of illegal behaviour, and
    - provide the basis to apply for warrants for the use of additional powers, such as search or interception powers.

15. It can also yield intelligence or evidence of the movements of persons of interest (POIs) and the nature of events immediately before and after a crime. Importantly, telecommunications data is often used to exclude people from suspicion in the early stages of investigation. A person's telecommunications data may establish that they have had no contact with a criminal syndicate, or was in a different location at the time a crime was committed. The exculpatory nature of telecommunications data ensures that innocent parties are not subject to more privacy intrusive methods.

16. The use of data at the early stages of an investigation also allows agencies to refine and target the use of other, more intrusive, powers at a later stage. Not only does this help agencies plan investigations in a more effective and efficient manner, it assists with prioritisation of investigative resources. In the absence of data, telecommunications interception, digital surveillance or access to the content of communications themselves may be necessary to create a picture of a suspect and their network of criminal associates.

17. The importance of this data is underscored by the continually increasing threat environment Australia faces. The time from planning to action for criminal activity and national security threats can now be almost immediate, reducing the margin for error in law enforcement and national security investigations. So-called 'lone wolf' attacks exemplify this – such persons have limited contact with other known extremists or persons who have actively radicalised the individual. As such, any missed opportunity to identify the source of radicalisation or instances of contact with other known extremists represents a significant risk.

The original impetus for data retention

18. Given its investigative value, it is important that Australia's law enforcement and security agencies continue to have reliable access to telecommunications data. The data retention scheme guarantees that this critical investigative resource is consistently available across industry for a period of two years. As noted above, prior to the implementation of the scheme the inconsistent retention practices of industry, driven by commercial decisions, substantially degraded access to this investigative resource. Some examples illustrate:

19. In June 2014 for example, the Australian Federal Police (AFP) received information from Interpol about a suspect with an Australian IP address who had

made a statement online that they intended to sexually assault a baby. As the carrier only retained data for a limited period of time, no results were available and the suspect was unable to be identified.

- In mid-2013, a major Australian ISP reduced the retention period for IP address allocation records from a number of years to three months. This impacted a number of national security and law enforcement investigations, as there was a lack of information to identify and trace criminal activity facilitated by internet communications.
- A system upgrade in 2013 of a major Australian carrier deleted its entire holdings of a type of telecommunications data, leaving agencies unable to reliably identify suspects, or execute interception warrants on the carrier's network.[2]

20. As highlighted above, the original need for a data retention scheme was based on:

- the importance of access to telecommunications data,
- the decline in the availability of lawfully accessed telecommunications data, and
- an increasingly high-risk operational environment.

21. These factors have not changed in the intervening years and the rapid integration of digital technology into everyday life has made the need for reliable access to telecommunications data more pronounced. This year, the Australian Communications and Media Authority (ACMA) reported that 74 per cent of Australians accessed the internet three or more times a day, and 40 per cent of Australians have accounts with five or more communications services.[3] These statistics highlight the fact that, as Australians spend more of their lives online, pertinent details about offences or national security threats will increasingly be found in the logistics of communications. Current technical trends only underscore the investigative value of robust and accessible data sets.

Continuing technological challenges

22. Although Australians are generating more telecommunications data than ever before, shifts in industry practice, driven by technological change, threaten to reduce the amount of telecommunications data available to law enforcement and intelligence agencies. As technology has moved towards internet-enabled devices and communications, telecommunications providers increasingly bill customers based on overall data upload and downloads rather than billing on a 'per telephone call' basis. As a consequence, telecommunications companies began moving away from retaining data relating to individual calls (A-party, B-party, date/time, duration), thus risking the availability of data to law enforcement and intelligence agencies. Without the minimum standards set by the mandatory data retention framework, law enforcement and intelligence agencies would be at the mercy of market forces and telecommunications providers: bodies who do not share in the responsibility for citizens' safety and security.

---

[2] Further issues about access to telecommunications data prior to the passage of the Data Retention Act can be found in the Attorney-General's Department Submission to the Committee's 2015 *Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014.*

[3] Australian Communications and Media Authority, *Communications Report 2017-2018* <https://www.acma.gov.au/-/media/Research-and-Analysis/Report/pdf/Communications-report-2017-18-pdf.pdf?la=en>.

23. Other technological trends also reinforce the importance of consistent and accessible data sets. The proliferation of encrypted communications, for instance, has significantly eroded the effectiveness of traditional interception powers and it is estimated that by 2020 all electronic communications of investigative value will be encrypted. Encryption conceals the content of communications rendering intercepted material unintelligible to law enforcement and security agencies. While telecommunications data itself may be encrypted, it remains a key element of modern communications that is interpretable for investigative purposes. These challenges have increased reliance on retained telecommunications data as the utility of content interception is eroded by encryption.

24. Recent amendments in the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Cth) (the Assistance and Access Act) modernised agencies powers in response to technological trends, including the prevalence of encrypted communications. However, noting the cybersecurity value of robust encryption, these amendments did not provide agencies with the power to fatally undermine encryption schemes, or even access encrypted content where that access would create a wider risk to information security. Given the need to place limitations on the ability of law enforcement and security agencies to access encrypted content, those laws were also designed to complement the use of telecommunications data in addressing the challenges of encryption. For example, where an encrypted communication makes an interception warrant an ineffective tool, the industry assistance measures introduced by the Assistance and Access Act can be used to provide targeted access to telecommunications data at the point at which it is unencrypted.

Protection of privacy

25. The Australian public has strong reservations about sharing their personal information. Of those surveyed in the Office of the Australian Information Commissioner's (OAIC) 2017 *Australian Community Attitudes to Privacy Survey*, less than half (46 per cent) were comfortable with providing personal information to government, and even fewer with providing personal information to technology companies (34 per cent) or social media companies (12 per cent).[4] No organisation, whether government or industry, can afford to be complacent in appropriately managing Australians' data. The Home Affairs Portfolio acknowledges this and is committed to ensuring the Data Retention Act remains proportionate, only impacting the privacy of Australians where necessary for legitimate law enforcement and national security purposes. Privacy protections in Australian law and the current authorisation framework for telecommunications data already establish robust privacy protections.

26. Data retained by telecommunications providers under the regime is classified as personal information and is protected by the *Privacy Act 1988* (Cth) (the Privacy Act). Consistent with this statute, the Data Retention Act was drafted to comply with the Australian Privacy Principles (APPs). The Privacy Commissioner maintains oversight of this information, assessing the compliance of telecommunications providers with the APPs in relation to retained data as well as monitoring the non-disclosure obligations of industry under the Telco Act.

[4] Office of the Australian Information Commissioner, *Australian Community Attitudes to Privacy Survey 2017* <https://www.oaic.gov.au/resources/engage-with-us/community-attitudes/acaps-2017/acaps-2017-report.pdf>.

Applicable thresholds

27. Establishing appropriate thresholds for access to data was another key consideration in the design of this legislation. During the 2015 PJCIS inquiry, questions were raised about the appropriateness of the post-access oversight mechanisms for access to telecommunications data given the privacy concerns. Some commentators asserted that, on grounds of privacy, it would be more appropriate for there to be independent oversight of agencies' access to telecommunications data, such as by requiring agencies to obtain a warrant from a judicial officer or a member of the Administrative Appeals Tribunal before accessing telecommunications data.

28. While all investigative techniques involve some degree of intrusion, the use of telecommunications data is one of the least intrusive. Telecommunications data, as opposed to content, does not divulge what has been communicated and the substance of a private conversation. This distinction has been recognised by Parliament in the tiered threshold for investigative powers within the TIA Act – all powers which access communications content have external approval and higher offence thresholds, whilst access to the logistics of a communication is internally authorised (although still subject to robust decision-making criteria and independent oversight).

29. Raising thresholds for access to telecommunications data would require agencies to potentially rely on more intrusive powers, such as physical surveillance and search powers, while also constraining their ability to obtain the preliminary information to apply for these powers. Indeed, the six categories of subscriber and traffic data set out in the legislation were chosen to provide the most benefit to law enforcement and intelligence agencies, while not unduly interfering with individuals' privacy.

30. As a further check on access to retained telecommunications data the TIA Act specifically sets out the thresholds that must be established before an authorisation is made. The TIA Act provides that agencies are only able to access telecommunications data if it is "reasonably necessary" for the enforcement of the criminal law, enforcement of a law imposing a pecuniary penalty or for the protection of the public revenue. Additionally, section 180F provides that, before making an authorisation, the authorising officer in a law enforcement agency must be satisfied on reasonable grounds that any interference with privacy that may result from the disclosure is justifiable and proportionate having regard to: the gravity of the conduct in relation to which the authorisation is sought; the likely relevance and usefulness of the information; and the reasons why the disclosure is proposed to be authorised. This requirement reinforces privacy safeguards by ensuring agencies weigh the proportionality of the intrusion into privacy against the value of the evidence and the assistance to be provided to the investigation.

31. Authorisations by ASIO are subject to strict privacy and proportionality obligations under the Attorney-General's Guidelines, made under paragraph 8A(1)(a) of the *Australian Security Intelligence Organisation Act 1979* (Cth), which require that:

    - any means used for obtaining information must be proportionate to the gravity of the threat posed and the probability of its occurrence,

- inquiries and investigations into individuals and groups should be undertaken using as little intrusion into individual privacy as is possible, consistent with the performance of ASIO's functions, and
- wherever possible, the least intrusive techniques of information collection should be used before more intrusive techniques.

32. In addition to establishing these thresholds, the Data Retention Act also provides that records indicating that the authorisation was properly made must be kept.[5] The Oversight section of this submission will provide further detail about how oversight mechanisms are used to ensure compliance with these thresholds.

33. Ultimately, the effect of additional layers of approval would considerably reduce the ability of agencies to obtain telecommunications data and significantly hamper their capacity to investigate crime and protect Australians. Noting the need to balance the expectations of the Australian public on privacy with the public's expectation that criminal violations be effectively investigated and enforced, and that national security threats be summarily addressed, the Home Affairs Portfolio considers the thresholds in the Data Retention Act are appropriately set.

Terms of Reference

The appropriateness of the dataset and retention period

34. Prior to the implementation the Data Retention Act telecommunications providers already retained user and communication records for commercial purposes. While in some cases data was retained for longer than the two years set in the legislation, the availability of telecommunications data varied greatly between telecommunications providers. This meant that the efficiency and, in some cases, success of investigations was dependant on the provider used by the POI.

35. In its unclassified submission to the PJCIS Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014, ASIO noted the inconsistency in the data sets and retention periods of the telecommunications data held by providers, with the following table:

Historical communications data	**Range of retention**
Subscriber information – name and address	7 years or longer
Telephone numbers called/received	6 weeks to 7 years
Telephone numbers associated with an SMS	60 days to 7 years
Mobile handset and Subscriber Identity Module (SIM) data	Up to 7 years
Internet Protocol (IP) account, device and address information	90 days to 3 years
Addresses associated with email and other IP communications	45 days to 3 years

36. As the table demonstrates, providers stored subscriber and traffic data for their own purposes, for varying lengths of time. A December 2014 investigation by the New South Wales Police (NSWPol) is illustrative of the issues this prompted. The agency investigated a series of armed robberies, and requested access to existing telecommunications data records from a carrier. At that time, that carrier only retained data for 42 days. Four offenders were charged, though it was suspected that other offenders were involved. When the case went to court, two of the

[5] TIA Act, s 186A(1)(a)(i).

accused provided a version of events incriminating another individual in one of the robberies. This individual denied involvement. Had cell tower locations, or other telecommunications data, been available to corroborate or disprove this new allegation, the case could have been resolved more effectively.

37. The 2015 amendments standardised provider retention practices. In recognition of the need to strike a balance between privacy concerns about a 'blanket' retention framework, and the need for law enforcement and intelligence agencies to access this critical data in their investigations, the retention regime limited the datasets that were required to be retained. The retention period was also fixed at two years.

Datasets retained

38. Under Schedule 1 of the Data Retention Act, the datasets required to be retained for two years are:

- **subscriber or account holder of the telecommunications service** – such as customer identifying details (name and address), contact details (phone number and email address), billing and payment information, and details about services attached to an account, such as the unique identifying number attached to a mobile phone, or the IP address allocated to an internet access account.
- **the source of a communication** – such as the phone number, international mobile subscriber identity (IMSI) or international mobile equipment identity (IMEI) from which a call or SMS was made, identifying details (username, address, number) of the account or device used, and the IP address and port number.
- **the destination of a communication** – such as the phone number that received the call or SMS, identifying details of the account or device which receives the communication, the IP address allocated to the receiving device, or any other service or device identifier that uniquely identifies the destination of the communication.
- **the time and duration of a communication** – such as the time a call started and ended, or when a device or account was connected to a data network.
- **the type of communication** – such as voice call, internet usage, SMS or Multimedia Messaging Service (MMS).
- **location of equipment used in the communication** – the location of a device at the start and end of a communication, such as a phone call or SMS, the address associated with an asymmetric digital subscriber line (ADSL) service, or which cell tower, wi-fi hotspot or base station a device was connected to at the start and end of communication.[6]

39. The legislation requires providers to retain the details of a communication, without capturing its content. In addition to content data, other datasets are explicitly ruled out of the regime, such as a subscriber's web browsing history.

40. Further, telecommunications providers were not required to keep visitor location register (VLR) data, which tracks the location of devices as they transit through cell-tower range or wi-fi zones, even when the phone is not communicating. This

[6] TIA Act, s 187A(2).

limitation ensures that the location records kept by providers do not allow continuous monitoring or tracking of devices.

41. Communications shared through 'over the top' providers (such as social media platforms and messaging applications) were also deliberately exempted from telecommunications data retention. Access to this type of data was left to other regimes, although the fact that many of these providers are based offshore continues to create challenges for Australian law enforcement and intelligence agencies.

Application of existing data types

42. The types of data retained under the Data Retention Act each play a different, and important, role in investigations.

Subscriber data

43. Subscriber data identifies the user of a communication device or service. It is critical in establishing which carrier holds the relevant data and is often key to collecting further intelligence and evidence on a suspect.

44. For example, during an illicit tobacco smuggling operation, the Australian Border Force (ABF) used telecommunications data to establish a connection between a POI and a known tobacco importer. **Subscriber data** proved the POI was using a telephone number acquired under fake identification, in an effort to conceal the tobacco importer's identity. Telecommunications data showed that the telephone number was used in the vicinity of the POI's house. Later evidence linked the POI to the false identification used to acquire the telephone.

Source and destination data

45. Telecommunications data can help determine the nature of contact between individuals, and rule out potential suspects without the need for more intrusive investigative measures.

46. In 2018, Western Australia Police (WA Police Force) conducted an operation which consolidated several investigations into alleged sexual misconduct by a male suspect. The request for telecommunications data was submitted following a report that the suspect was contacting potential victims (including parents of potential child victims) after the suspect was made aware of a pending police investigation. Through analysis of **source and destination data** of the suspect's phone calls investigators identified telephone contact between the suspect and the victims and identified additional potential victims unaware of the police investigation. The suspect was charged with 14 offences.

Time and duration of a communication

47. Investigators can use the time and duration of a communication to link that communication with associated events.

48. In a recent matter, telecommunications data helped the Australian Securities and Investments Commission (ASIC) identify that a POI misled ASIC during an examination. The POI asserted that they were not in contact with other persons of interest whilst overseas. However, the **time of communications**, coupled with the POI's travel records, demonstrated that this was false.

Type of communication

49. Data which identifies the type of communication is necessary for understanding what telecommunications service has been used to send the communication. Identifying the **type of communication** allows law enforcement and intelligence agencies to follow up with subsequent requests for information to refine their investigation.

Location data

50. Location data identifies the location of a device at the time of a communication, potentially linking the presence of a device to an event. Frequently, it is used to exclude a person from further inquiry where the data has placed a suspect in a different location at the time of offence.

51. Due to the historical nature of serious criminal matters, such as unsolved murders, **location data** can be crucial in the further investigation of known offenders and also the victim's movements at the time that they went missing. Crime Stoppers is a known hotline where persons can report criminal activity. If a person is nominated as a POI for a homicide, leads can quickly be obtained as to their location at the time of a victim going missing. A location trail can then be analysed.

52. In 2017, the Queensland Crime and Corruption Commission (QCCC) investigated allegations that an elected public official had corrupt associations with directors of property development companies. The investigation focused on allegations that the elected official had secured the approval developments in return for campaign donations and other financial benefits from the property developers. Location data, in conjunction with historical CCR data, provided evidence of contact between the elected official and other POIs around specific events of interest to the investigation. This assisted in locating evidence of corrupt activity.

53. Location data can also be crucial in locating a crime scene and further advancing investigations.

The case for expanding datasets

54. Some agencies have suggested the PJCIS consider expanding the datasets retained under the legislation. Such expansion could address emerging trends in technology, such as 5G and embedded Subscriber Identity Module (eSIMS). For example, including media access control (MAC) addresses and devices which identify serials would provide better information as to which device was being used at the time of an offence. MAC data is not currently retained under the Data Retention Act, but is a form of data that will become increasingly important to law enforcement and intelligence agencies. Where providers do retain this information, it is a significant investigative tool. In a recent case in Victoria, a mobile phone containing pictures of a terminally ill child was stolen at a shopping centre. Victoria Police (VicPol) were able to use the shopping centre's security infrastructure to track MAC addresses in order to obtain surveillance footage of possible offenders. Charges have since been laid.

55. Similarly, including IP addresses and port numbers to attribute data accessed on mobile phones, would allow agencies to make better use of mobile phone data.

Retention period

56. The two year retention period set in the Data Retention Act was based on experience of similar legislation in the European Union and was agreed by law enforcement and intelligence agencies. While the majority of telecommunications data disclosed to law enforcement and intelligence agencies is less than six months old, older data also plays an important part in many serious investigations. The PJCIS established that retaining telecommunications data for two years was an appropriate balance between supporting critical investigative purposes and minimising privacy impacts. In its 2015 *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, the PJCIS noted:

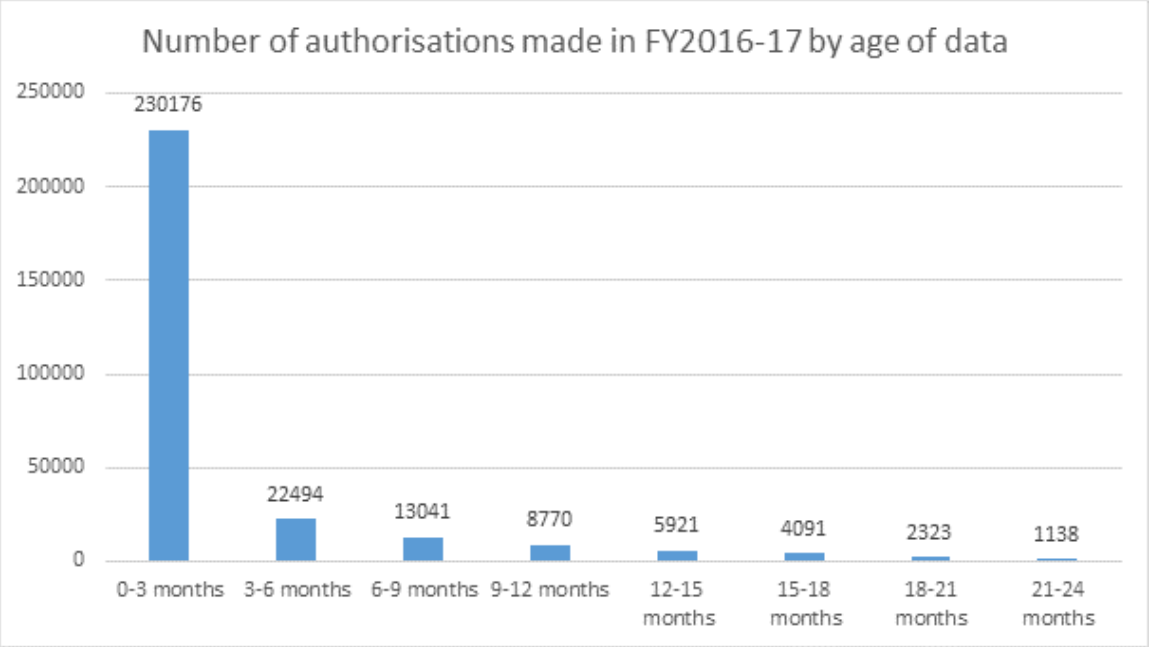
> "On the basis of the evidence provided, the Committee considers that a two-year retention period is necessary and proportionate… The Committee notes that longer retention periods may aid particular investigations. However, the effective conduct of serious national security and criminal investigations must be balanced against the degree to which a two-year retention period could interfere with the privacy, freedom of expression and other rights of ordinary Australians. For many service providers, a two-year retention period will not represent a substantial change to existing retention practices."[7]

57. The Home Affairs Portfolio notes that an increased retention period would further assist agencies with managing investigations. However, when these considerations are weighed against changes in public attitudes towards privacy and the need for strong privacy protections, the most appropriate way forward would be to retain the existing scope the legislation.

Use of data: recent vs older data

58. When considering the appropriateness of the retention period, it is important to understand how agencies use retained telecommunications data. This can be understood by reviewing the statistics on authorisations reported in the TIA Act Annual Report. As shown in the following graph, these statistics record authorisations by age of data.

[7] Parliamentary Joint Committee on Intelligence and Security, *Advisory report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, 2015, pg 146.



59. The data in this graph includes telecommunications data retained under Chapter 4 of the TIA Act as well as data retained for other purposes. Authorisations for 'point in time' information without an identifiable age, such as current subscriber information and current information held in the Integrated Public Number Database (IPND)[8], are treated as '0' months old and comprise a large portion of the telecommunications data requested by agencies within the 0-3 month category , significantly exaggerating the figures in this column. Checks against the IPND are commonly made at the onset of an investigative to confirm that status of a phone number and associated subscriber information. As this information is continually maintained it is in effect 'ageless'.

60. The majority of telecommunications data requests, leaving aside the IPND requests, are for 'recent' data (data aged between 0-12 months). This is attributable to the increasing use of telecommunications technology and the growing role telecommunications data plays in investigations, the type of data retained, and the types of crimes it is used to investigate. For instance, certain crimes are reported within a short space of time following the offence resulting in recent data being the most relevant.

61. While slightly older telecommunications data (data retained for 12 months or longer) is used less frequently than recent data, it plays a significant role in the investigations in which it is used. Authorisations for older data are often used to investigate serious, complex crimes which can take a long time to come to light and involve a range of sophisticated actors.

62. For example, in 2017 VicPol took over a case from the Queensland Police. The investigation examined offending which took place over a number of years, during which the suspect set up fake online profiles (including one impersonating a well-known television identity) to stalk and harass numerous victims. The suspect used multiple methods such as email, Facebook, Instagram, Viber, WhatsApp and

[8] The IPND is an industry-wide database, managed by Telstra, containing all listed and unlisted public telephone numbers.

Skype. One of the profiles was used to befriend the victims and others were used to harass, intimidate and threaten them. One victim ultimately took their own life. At the time VicPol took over the investigation, additional victims were identified. VicPol investigators were unable to obtain relevant historical telecommunications data from Optus, such as incoming call records dating back to 2011. Similarly, SMS records were unavailable. Historical IPND checks only provide detail on the previous four subscribers which created further issues in trying to identify who the number was registered to at the time of offending.

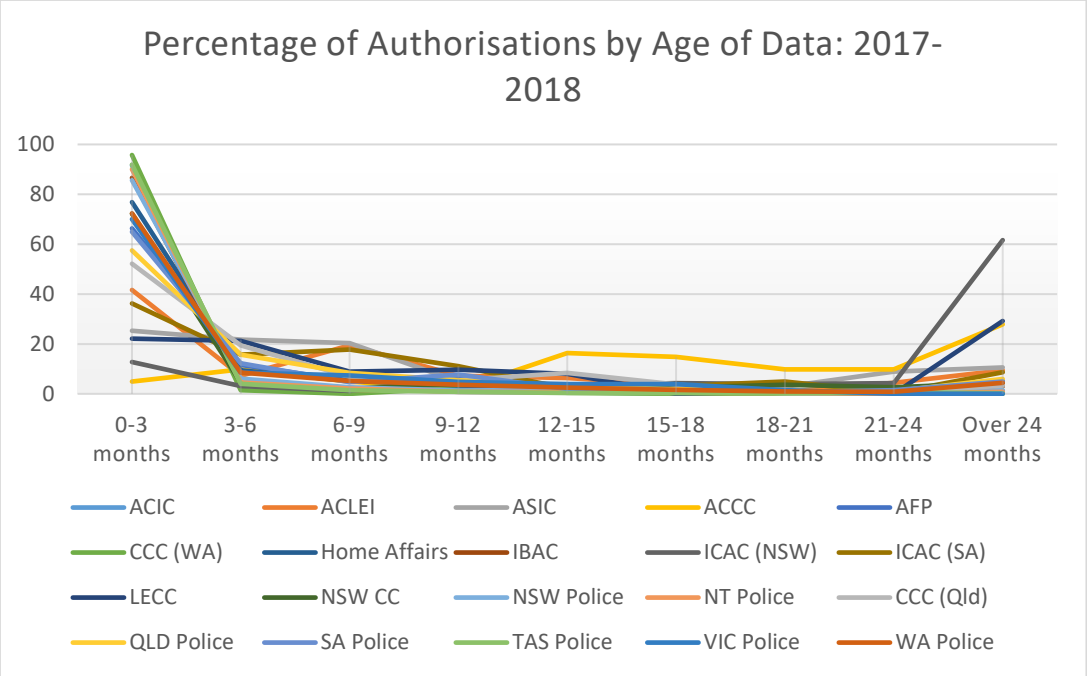
63. The suspect was charged with stalking seven people. Available telecommunications data played an important role in securing findings of guilt for the stalking of six people. The absence of older telecommunications data contributed to one charge not being able to be proven beyond a reasonable doubt.

Value of older data

64. Enforcement agencies have cited the need for lengthier telecommunications datasets to test evidence brought to light late in an investigation, or during a trial, as a common use of data up to and beyond two years old. It is not uncommon for trials to take longer than two years to be heard, particularly in the case of homicides and child sex offences. This older data is critical to police due to the length of time between a crime being committed and a case reaching the courts.

65. In the case of corruption and integrity agencies, many cases hinge on the investigators' ability to demonstrate connections and communications between persons. Once criminality is suspected, or a crime committed, older telecommunications data allows this investigation to take place in a covert, and judicially credible manner. The Australian Competition and Consumer Commission (ACCC) saw a similar usage pattern: between October 2015 and February 2019, 63 per cent of its telecommunications data requests were for data over 12 months old, and 30 per cent were for data more than two years old.

66. This can also be illustrated by reviewing the percentage of telecommunication data requests made by each agency by the age of the data, as in the following graph.



67. It is clear that while older data is requested less frequently, it plays a more critical role in investigations where agencies cannot rely on other forms of evidence as easily. Feedback from Australia's law enforcement and intelligence agencies is that data held for 12 months or more tends to be more necessary in complex and organised group-type of investigations where knowledge of criminal methods and the links, relationships and associations are more difficult to immediately discern, or in matters of corruption where the behaviours might not be immediately identified or reported.

68. Intelligence agencies, such as ASIO, regularly investigate individuals whose connection to Australians, or residence in Australia is historical. Australians engaged in threats to national security, including acts of espionage and terrorism in Australia and overseas, invariably have contacts and associations which go back many years. Many of these associations are only revealed through assessment of historical telecommunications data, and can be critical to both progressing investigations and identifying ongoing threats.

69. Due to the nature of some intelligence investigations, lead information may not become available to agencies until long after an investigable event, such as a cyber-attack, initial contact from a foreign state actor or the initial stages of radicalisation of an individual. Data older than 12-24 months is often required to investigate activities at the time of these events and is crucial to gaining an understanding of the residual threat. Often in these cases, a level of communications security has been applied by the POIs, meaning that relevant activities are not discoverable in more recent telecommunications data.

70. In investigating older incidents, it is often the case that other forms of evidence have been degraded or lost (such as physical evidence, including fingerprints). In these circumstances, reliable access to retained telecommunications data is crucial.

The case for extending periods

71. Several agencies who access telecommunication data under the TIA Act have suggested that the retention period be extended beyond the current two year period. These agencies point to cases where their inability to access historical data has hindered their effectiveness, as well as examples of investigations where data held by providers for longer than two years has been instrumental to securing a conviction.

72. For example, in 2018 the Victoria Independent Broad-based Anti-corruption Commission (VicIBAC) investigated claims a police officer had connections to a registered sex offender and was using this association to facilitate sex trafficking. Analysis of call charge records going back two years established a connection between the two individuals over that period, however call records beyond that period were unavailable. The statutory declaration signed by the police officer declaring no associations was dated 2015, and as the VicIBAC were unable to obtain telecommunications data evidencing a connection prior to the date of this declaration, perjury could not be proven.

73. In 2011, the New South Wales Crime Commission (NSWCC) began investigating a murder committed in 2010. The NSWCC's investigation continued into 2012. By this time, the NSWCC had identified a number of suspects and POIs, together with telecommunications services suspected to have been used by those persons around the time of the murder. When those individuals and services were

identified, some telecommunications records critical to any homicide investigation, chiefly those relating to incoming calls, messages and location information for outgoing and incoming calls, were no longer available. This lacuna made it very difficult to track the movements of the persons of interest around the time of the murder or place them in the vicinity of the crime, and hindered the reconstruction of communication events at relevant times. While this example predates the introduction of the data retention requirements, it illustrates the inadequate preservation of telecommunications data can impact homicide investigations.

74. Conversely, in late 2014, the NSWCC began investigating a murder that was committed in 2013. By early 2016, after extensive investigation, almost all lines of inquiry had been exhausted. However, in late 2016 credible information was received concerning the circumstances of the murder, and identifying suspects not previously investigated. Relevant telecommunications records were obtained, the analysis of which led to the identification of services used by suspects for the murder, the reconstruction of their communications and physical movements, and, crucially, the corroboration of the information received. Murder charges have now been laid in this investigation. The telecommunications records obtained during the investigation, most of which were obtained at least three years after the offence, formed a vital part of the brief of evidence.

75. Similarly, in the case NSWPol case of P v Holdom[9], telecommunications data beyond the two year retention period (in this case, dating back seven years) led to a conviction for two murders more than ten years after the crimes were committed. Investigators believe the telecommunications data was critical in this prosecution. Given the length of time that had elapsed since the crimes occurred, physical evidence was no longer available to investigators. Had telecommunications data not been available as evidence, it is likely the offender would have escaped justice.

76. In 2015, South Australia Independent Commissioner Against Corruption (ICAC SA) commenced an investigation into the conduct of a public officer accused of deception and abuse of public office. The majority of the evidence surrounding the allegations concerned the location of the suspect at specified times between 2009 and 2015. Requests were submitted to Telstra for available telecommunication data records of the service used by the suspect at that time. In this case, Telstra were able to provide ICAC SA with the historical records from 2009, although some of these records took a while to be processed and came at higher than normal cost. These records formed a critical part of the brief of evidence in the case.

77. ASIO considers the existing retention period of at least two years as a minimum requirement, balancing the competing needs of privacy, business needs and security and law enforcement. However, in ASIO's experience in dealing with both counter-espionage and counter-terrorism investigations, an increased retention period would increase their ability to manage such threats.

78. The Home Affairs Portfolio notes that any expansion of the retention period would require greater consideration, including an examination of privacy implications, and that there have been no changes in the investigative environment to warrant such consideration at this time. However, the case studies above demonstrate that

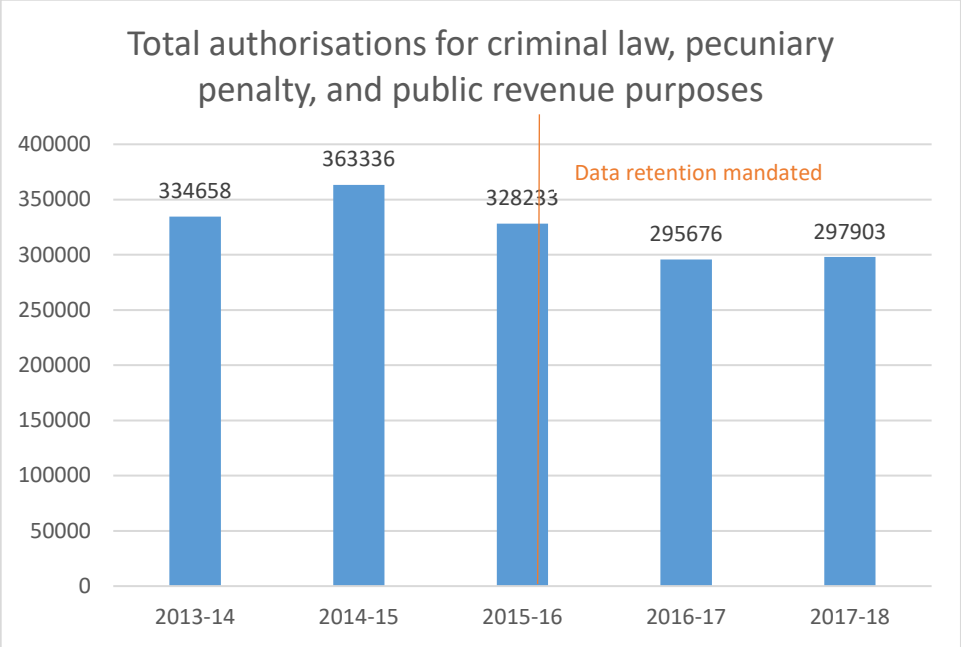
[9] *P v Holdom* [2018] NSWSC 1677.

data held by commercial entities for longer periods can prove critical to prolonged investigations.

The effectiveness of the scheme

Frequency of use

79. The statistics provided by agencies to the TIA Act Annual Reports[10] provide evidence of the overall use of telecommunications data before and since the introduction of the mandatory data retention regime.



80. The slight decrease of authorisations issued for telecommunications data at the introduction of the Data Retention Act correlates closely to the number of requests previously made by local councils as well as state and territory organisations (3172 requests in 2013-14[11], and 3313 requests in 2014-15[12]).

81. While the rate of use of telecommunications data has not significantly altered since the introduction of the Data Retention Act, the consistent volume of use demonstrates that this data remains a highly valued tool for law enforcement and intelligence agencies in their efforts to provide a safe and secure environment.

Use of telecommunications data in investigations

82. The application of telecommunications data differs depending on the nature of the investigation. Agencies have developed their investigative techniques in response to the modus operandi of their targets and the investigative methods available. This is reflected in the following examples provided by law enforcement agencies:

- The NSWCC, which predominantly investigates serious crimes involving drugs, homicide and money laundering, advised that in the 2017-18 period telecommunications data was used in 90 per cent of that year's investigations.

[10] TIA Act, s 187P.
[11] *Telecommunications (Interception and Access) Act 1979*, Annual Report 2013-2014.
[12] *Telecommunications (Interception and Access) Act 1979*, Annual Report 2014-2015.

- The ACCC noted that telecommunications data is increasingly used as an important source of intelligence for covertly corroborating case theory, and supporting lines of inquiry, particularly for criminal cartel investigations. This is especially the case given the ACCC is not an interception agency for the purposes of telecommunications interception, and is unable to access similar evidence through other means.
- Statistics provided by the NSWICAC show that more than 85 per cent of its investigations rely on telecommunications data.
- Accessing, and analysing telecommunications data is vital to successful outcomes in ASIC's investigations of technology-enabled offences. ASIC's investigative techniques have evolved to keep up with the technological advancements employed by those contravening the law. This may lead to an increasing reliance on telecommunications data in the future.
- The ACIC works to identify new and emerging serious and organised crime threats and criminal trends; to create a national strategic intelligence picture across the spectrum of crime; to fill intelligence and knowledge gaps; and to share information and intelligence holdings to inform national and international responses to crime. Noting the targeted nature of the ACIC's work, dramatic changes to the agency's investigative methodologies have not been seen in the relatively short time since the introduction of the regime. However, in the last year the ACIC substantially increased its access to telecommunications data retained for a period between six and nine months and notes the importance of the data retention regime.
- Telecommunications data is used in approximately 90 per cent of the Law Enforcement Conduct Commission's (LECC) investigations. Investigation teams at the LECC analyse the telecommunications data that arises from communications between targets to assist in developing POI profiles. Two patterns that are often examined from this telecommunications data include frequency of contact with particular individuals and location frequency, to infer lifestyle and behavioural trends. The analysis of this data then allows for the LECC to deploy targeted surveillance in order to produce high value intelligence.

83. Further case studies demonstrating the ways in which telecommunications data is used to aid investigations can be found at Appendix B.

Transnational, serious and organised crime

84. Access to retained telecommunications data is particularly useful to understand the activities of organised criminal groups. These groups use traditional telecommunication and emerging methods to plan and carry out offences; this in turn produces an array of telecommunications data for enforcement agencies to obtain and investigate. The establishment of behavioural patterns and criminal networks can assist in both investigating crime, and preventing future criminal activity.

85. For example, in 2017, the AFP used telecommunications data retained within the regime to investigate an individual suspected of planning to import narcotics into Australia. Investigators accessed call charge records (CCRs) and subscriber checks on a regular basis for two years as the target of the investigation continually changed phones to contact other POIs. This data supported suspicions

that the suspect was involved in criminal activities. Using further investigative tools, the target was linked to a narcotics importation, resulting in seizures in late 2018 and early 2019. Had the material obtained from the subscriber checks and CCRs not been available, police would have had little evidence that the target was involved in serious criminal activities.

86. The AFP advised that this example is consistent with a large percentage of its successful investigations of organised crime networks.

Corruption

87. Integrity and anti-corruption agencies use telecommunications data in the majority of their criminal investigations, primarily as a source of evidence in the investigation of serious misconduct and other serious criminal offences. In more complex and prolonged investigations, telecommunications data is used to build a picture of suspected offences by identifying POIs, and establishing relationship networks and levels of contact. This data has also been used to eliminate suspicion without having to resort to more intrusive, costly, and, in some cases, dangerous investigative measures.

88. In many instances, corruption offences result from a pattern of behaviour detected over a period of time. It is common for these agencies to require access to data spanning a period of years to establish connections at the time the corruption began.

89. In a 2017 investigation by the West Australian Corruption and Crime Commission (WACCC) into a public officer engaging in serious misconduct and corruption within the West Australian Department of Transport, telecommunications data was used to significant effect. The POI in the investigation was conducting practical driving assessments for heavy vehicles on a fee-for-service basis, but not enforcing the regulations. A number of telecommunications data requests ranging from 0-3 months in age, were used to identify all parties impacted, and to validate the use of further investigation methods. As a result, the agency was able to establish the period over which the offences occurred, which resulted in 678 heavy vehicle licenses being reviewed. Over half of those reviewed failed upon re-testing. In this case, the use of telecommunications data eliminated a significant risk to community safety by identifying and preventing incompetent drivers from taking to the road under fraudulent documents.

Violent Extremism and Terrorism

90. For many years now, terrorist organisations have used sophisticated technology-based strategies to recruit followers and incite them to violence. ISIL has increasingly encouraged its followers to carry out ‘lone wolf’ attacks in their own countries – the internet is the new battleground for this campaign. Likewise, right-wing extremists have also used the internet and other methods of communication to share and promote their ideological views. Information is shared between sympathisers on how to finance, plan and execute attacks. Being able to trace connections between networks, analyse patterns of behaviour, and gather evidence to justify more intrusive investigative methods remain key tools in staying ahead of terrorists, and preventing attacks being carried out in Australia or by Australians.

91. The planning of terrorist attacks may span several years. In some cases, it can take an offender years to develop an attack capability, including acquiring the skills, knowledge and resources, as well as target selection and reconnaissance

before attack mobilisation. Analysis of CCRs to identify associates could assist in the identification of potential witnesses and/or associates who may require further investigation to prevent future attacks. Additionally, analysis of CCRs may identify locations of interest, such as the whereabouts of group meetings or possible sites to target. In responding to the recent Christchurch attack, for example, historical CCRs were obtained by the NSWCC, a member agency of the Joint Counter Terrorism Team in NSW, and proved valuable in understanding the offender's domestic and international movements.

92. Telecommunications data has also been accessed in relation to a 2018 investigation concerning past terrorist conduct. The investigation related to a group of young Australian males allegedly planning to travel to Syria to engage in hostile activity. The AFP used historical CCRs from 2016 to identify the frequency of contact between a person of interest while they were making their preparations for travel, including calls to Australian-based chemical companies and the Australian passport office. These records were used in the brief of evidence for this matter. Witness statements later alleged that the person of interest was calling chemical companies in an attempt to learn how to make explosive devices. The defendant is currently before the court charged with multiple Commonwealth terrorism offences.

Complex crime

93. Complex crimes (such as financial crimes, corruption, and the types of terrorist activities outlined above) often occur over a long period of time, or between numerous individuals. These crimes can take a number of years to come to light, requiring law enforcement officers to rely on all available historical data to build their cases. In this time, many forms of evidence (such as physical evidence, including fingerprints and other elements of a crime scene) degrade or are completely lost due to age.

94. Analysis of telecommunications data has been an essential tool for identifying and understanding linkages across complex criminal networks. It assists law enforcement to identify persons in enabling roles (that is, professional facilitators such as accountants, lawyers and encrypted telecommunications vendors) providing services to multiple criminal networks.

95. During a 2015 investigation into suspected market manipulation of an ASX listed company, ASIC's investigation revealed that the principal person of interest used over 43 accounts with a dozen stockbroking firms to dominate the market for the listed company. These accounts were in various names, including that of the POI, those of their personal companies, and the names of third parties. By obtaining telecommunications data ranging from 12 to 24 months in age, ASIC was able to reconcile the time when orders were placed with stockbrokers against the call charge information and IP addresses to identify that a significant volume of orders and trading came from the POI. In this case, the telecommunications data confirmed that the 43 accounts were connected to the same person. Charges have been laid and an arrest warrant issued for the person of interest and two co-conspirators.

Protecting the public revenue

96. Agencies have long been able to access telecommunications data for the purposes of protecting public revenue. While the number of agencies able to use telecommunications data under the TIA Act for these purposes was significantly

reduced by the Data Retention Act to 21 key law enforcement and intelligence agencies, data remains an effective tool to investigate these matters.

97. A contemporary example of this is the Illicit Tobacco Task Force, established on 1 July 2018 to protect Commonwealth revenue by proactively targeting, disrupting and dismantling serious actors and organised crime syndicates that deal in illicit tobacco.[13] This Task Force is expected to see significant revenue saved or potentially collected. Participating enforcement agencies such as the ACIC and the ABF (formerly the Department of Immigration and Border Protection) will be able to access telecommunications data to facilitate their investigations in respect of offending under the *Customs Act 1901* (Cth).

Imposing pecuniary penalties

98. A number of agencies have also reported their use of telecommunications data in investigating offences which attract both criminal sanctions and civil or pecuniary penalties. Agencies have applied these provisions to a range of activities, varying in relation to their specific focus:

- The ASIC have used the provisions to investigate insider trading offences, market manipulation, and a number of offences under Chapter 7 of the *Corporations Act 2001* (Cth) (for example, telecommunications data was integral in identifying relevant witnesses who could provide evidence against a corporate defendant).
- The ACCC have used the provisions to investigate harassment and coercion in the supply or provision of goods and services (using data used to confirm excessive contact from a business to a consumer); unconscionable conduct (data used to confirm communications and sales practices of a business engaging in systemic unsolicited sales and misleading conduct); and companies making false and misleading representations (using data to establish that an overseas entity was carrying on business within Australia).
- Policing agencies, including NSWPol, the WA Police Force and the Tasmania Police, have reported using the provisions to prove traffic infringements (using telecommunications data to establish whether or not a person had used their phone while driving); to investigate into dealings in the proceeds of crime, and property damage and environment pollution (using location data in suspected cases of illegal dumping).

National security outcomes

99. Telecommunications data has provided valuable intelligence for intelligence agencies both before and after the implementation of the data retention regime. The data retention regime ensured that access to such data was maintained as telecommunications technology shifted towards internet-enabled devices and communications, enabling ASIO, and other intelligence agencies, to continue using longstanding and critical investigative techniques.

100. Due to the classified nature of ASIO's activities, this submission does not provide specific examples of how ASIO has used telecommunications data in its activities. ASIO will provide a separate, classified submission to the inquiry containing

[13] Australian Criminal Intelligence Commission, *Illicit Tobacco Taskforce* <https://www.acic.gov.au/about-crime/task-forces/illicit-tobacco-taskforce>.

several examples of significant national security outcomes based on the use of telecommunications data. General observations are made below.

Industry compliance with the legislation

101. Based on the experience of enforcement agencies to date, service providers have demonstrated a high degree of compliance with the data retention regime. Ensuring law enforcement agencies are able to draw on a consistent store of information, regardless of the provider used by persons involved in an investigation, has increased the reliability of data being available to investigators within the two year retention period. It also prevents criminals from exploiting the disparity between providers' retention policies.

102. Outside legislated data retention obligations, many service providers pool data from across their operational and business support systems in order to evaluate the usage by their customers of its network components. The service providers' use of this data goes far beyond the traditional storage of communications records for customer billing purposes; data on customers' use of products, services, content and applications is used to establish patterns of usage and understand their customer's behaviour.[14]

103. This data is monetised by providers, allowing them to match the tastes of individual customers in a timely manner, in order to increase sales.[15] The aggregation of their data also allows them to respond in real-time to market demand and threats, by targeting customer interactions in order to maximise cross-sell and up-sell.[16] Industry reports demonstrate this data is one of the major sources of income for the telecommunications carriers.[17]

104. The introduction of the mandatory data retention regime reserved a portion of this data, without diminishing providers' use of it. This ensures it is available to enforcement and intelligence agencies for a defined period of time, even if the data should lose its commercial value to industry.

105. It is not known whether providers lengthened or decreased their own retention policies in the years since the mandatory data retention regime was introduced. The Department of Home Affairs has not made any estimates of this category in relation to total requests for telecommunications data made annually.

Ongoing effectiveness of telecommunications data

106. As noted in the overview to this submission, the technological landscape has continued to evolve since the introduction of the legislation in 2015. The increasing use of 'over the top' applications and encrypted communications has had an impact on the reliance on traditional communication methods, such as phone calls and SMS.

107. While the New South Wales Independent Commission Against Corruption (NSWICAC) notes a decline in both SMS and call traffic due to third party instant messaging applications and wi-fi calling, it still sees substantial benefit in

---

[14] IBM Telecommunications Data Warehouse General Information Manual <ftp://public.dhe.ibm.com/software/data/sw-library/industry-models/brochures/IBM_telco_data_warehouse_GIM.pdf> ('IBM General Information Manual').
[15] NEC Technical Journal, *Special Issue on Telecom Carrier Solutions for New Value Creation*, Vol 10 No. 3 (July 2016).
[16] IBM General Information Manual.
[17] NEC Technical Journal, *Special Issue on Telecom Carrier Solutions for New Value Creation*, Vol 10 No. 3 (July 2016).

accessing telecommunications data. The use of telecommunications data is far less intrusive to individuals' privacy, but still significantly influences officers' decisions by confirming or ruling out avenues of investigation. Without access to this data, more intrusive covert techniques, including telephone interception, surveillance devices and physical surveillance, would be required more frequently.

108. The emerging technology change related to the rollout of 5G is expected to have an impact on retained data and may present challenges to both agencies and providers, in particular the carriers' ability to collect and retain data that may not be routed via centralised systems, as they currently are within 3G and 4G networks. However, by no means is this impact expected to result in a decreased demand for, or decreased utility, of the data.

Oversight of access to telecommunications data

109. The Data Retention Act improved oversight of access to telecommunications data. Prior to the commencement of Chapter 4, access to telecommunications data by law enforcement agencies was not subject to legislated oversight. Schedule 3 inserted new provisions into the TIA Act to facilitate the oversight of law enforcement agencies' records by the Commonwealth Ombudsman. Section 186B, introduced by the Data Retention Act, requires that the Ombudsman inspect records of an enforcement agency to determine the extent of compliance with Chapter 4 by the agency and its officers.[18]

110. The Office of the IGIS provides oversight of ASIO's access to telecommunications data.

Inspections

111. The Ombudsman is now able to use consistent and systematic inspection methodologies to inspect the records of designated agencies[19] that have access to telecommunications data (excluding ASIO). The Ombudsman focuses on areas of high risk and considers the impact of non-compliance, for example where there is unnecessary intrusion on privacy. [20]

112. Following the introduction of the Data Retention Act, the Ombudsman reported that the agencies were generally exercising their powers to access telecommunications data appropriately.[21] Reports for the period 1 July 2016 to 30 June 2017 and the report 1 July 2017 to 30 June 2018 noted that agencies had frameworks in place to ensure appropriate access to intrusive powers and these frameworks appeared to be working as intended. Agencies also demonstrated a commitment to compliance and responded appropriately to compliance issues.'[22] In addition, the most recent Ombudsman report highlighted that the number of issues being identified by the Ombudsman had been reduced, which indicates the

[18] TIA Act, s 186B(1)(a).
[19] TIA Act, s 110A.
[20] Commonwealth Ombudsman, *A Report on the Commonwealth Ombudsman's Monitoring of Agency Access to Stored Communications and Telecommunications Data under Chapters 3 and 4 of the Telecommunications (Interception and Access) Act 1979* (2016-2017) pg 4 ('Ombudsman Report').
[21] In 2015-16 the Ombudsman conducted a 'health check' at each agency, analysing its policies and procedures for accessing telecommunications data. The results of the 'health checks' were presented in a report to the Commonwealth Attorney-General (the Minister), and these results were used to inform the records-based inspections in 2016-17.
[22] Ombudsman Report (2016-2017) pg 1, Ombudsman Report (2017-2018) pg 1-2.

effectiveness of both the remedial actions and the oversight regime of the agencies.[23]

113. However, the Ombudsman inspection reports have identified a number of compliance concerns, including:

- adherence to journalist information warrant provisions,
- authorisations that were improperly made,
- inability to sufficiently demonstrate required privacy considerations,
- access to unauthorised telecommunications data,
- statistical issues, and
- record-keeping.[24]

114. As are result of this finding, the AFP implemented mandatory training for authorised officers and introduced additional guidance for requesting officers when filling in the authorisation request form.

115. Overall, the introduction of oversight can be viewed positively as it has encouraged the AFP to review governance and best practice on accessing telecommunications data and make improvements along the way, such as introducing measures to improve the quality of requests.

116. ASIO's access to telecommunications data is subject to inspections by the Office of the IGIS. IGIS staff review ASIO's access to prospective and historical telecommunications data as part of the regular inspection of ASIO investigative activities. IGIS staff also check that ASIO's access to telecommunications data is in connection with the performance by ASIO of its functions.

117. These reports have assessed that authorisations for telecommunications data under the TIA Act were approved at the appropriate level, had regard to the Attorney-General's Guidelines and were undertaken in connection with ASIO's functions.[25] Further, consecutive IGIS annual reports have not identified concerns with ASIO's access to historical data under the TIA Act.

118. A few key instances of non-compliance with the legislation, either self-disclosed or reported by independent oversight bodies are discussed below.

Non-compliance - Data accessed without proper authority

119. Instances of non-compliance with the correct procedures for obtaining an authorisation are rare. In such instances, agencies often self-report to the appropriate oversight body.

120. The AFP disclosed that between 13 and 26 October 2015, 116 authorisations within ACT Policing were made by an officer who was not authorised under section 5AB(1) of the TIA Act. The AFP advised that this was due to administrative oversight. Upon identifying the error, the AFP updated the Commissioners written authorisations on 26 October to appoint the relevant position within ACT policing

[23] Ombudsman Report (2017-2018) pg 2.
[24] Ombudsman Report (2016-2017) pg 2, Ombudsman Report (2017-2018) pg 2.
[25] Inspector General of Intelligence and Security, *Annual Report* (2015-2016) pg 19-20 ('IGIS Annual Report'), IGIS Annual Report (2016-2017) pg 18, IGIS Annual Report (2017-2018) pg 22.

as an authorised officer.[26] The AFP has quarantined the data, in line with the Commonwealth Ombudsman's recommendation. AFP advised that it was seeking legal advice regarding the use of the affected data.

Access to data outside authorised parameters

121. Both Ombudsman and IGIS inspections[27] have found instances where providers have disclosed data beyond the scope of an authorisation. Such access arises for any number of reasons, including human error or changes in a provider's system. In some instances, providers have disclosed telecommunications data beyond the datasets specified in the Data Retention Act. The PJCIS could consider whether amendments should be made to oversight measures to address access to data outside the scope of an authorisation, such as data stored by telecommunications providers being given to agencies as part of their telecommunications data requests.

Journalist Information Warrants

122. As part of the Data Retention Act, additional safeguards were developed in relation to accessing telecommunications data for the purpose of identifying a journalist's source. One of the requirements relevant to the issue of a journalist information warrant is that the public interest in issuing the warrant outweighs the public interest in protecting the confidentiality of the identity of the journalist's source.[28] Telecommunications data relating to journalists that may lead to the identification of journalists' sources is afforded greater protections.

123. Since the introduction of this scheme there has been only one breach of the legislation, which was reported by the AFP in April 2017. The AFP disclosed that it had accessed telecommunication data of a journalist without obtaining a journalist information warrant. Subsequent investigations by the Commonwealth Ombudsman found that this was a failure of administrative process and not an attempt to evade the oversight protections.

124. The timely and transparent investigation of this matter demonstrates that the considerations and oversight mechanisms governing the oversight of journalist information are effective.

Oversight of carriers

125. By virtue of section 187LA of the TIA Act, the Privacy Act applies in relation to a service provider, as if the service provider were an organisation within the meaning of the Privacy Act, to the extent that the activities of the service provider relate to retained data. This ensures that all the protections to personal information afforded by the Privacy Act unambiguously apply to entities, like carriers, who hold retained data.

126. The OAIC continues to have oversight of service providers' collection and retention of personal information under legislation where service providers are subject to the Privacy Act, including the ability to conduct assessments to ensure compliance with the APPs.

127. In July 2015, the OAIC issued Privacy Business Resource 11, titled *Telecommunications service providers' obligations arising under the Privacy Act*

[26] Ombudsman Report (2016-2017) pg 10.
[27] Inspector General of Intelligence and Security, *Annual Report* (2016-2017) pg 18
[28] TIA Act, s 180L and s 180T.

1988 as a result of Part 5-1A of the Telecommunications (Interception and Access) Act 1979 to assist providers of telecommunications services in Australia who are required to comply with the data retention provisions.

128. In accordance with a recommendation from the PJCIS review of the data retention legislation, the national data breach scheme came into effect from 22 February 2018. This scheme, established by the passage of the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth), creates an obligation to notify individuals whose personal information is involved in a data that is likely to result in serious harm, and recommend remedies. It applies to entities with existing personal information security obligations under the Privacy Act, including telecommunications operators and government agencies. Certain instances of unauthorised access to retained telecommunications data are captured by this scheme and it functions as an added layer of transparency and data security to complement the Data Retention Act. The OAIC's quarterly reports have not included any breaches of telecommunications data.

129. Further, sections 306 and 306A of the Telco Act require carriers and carriage service providers to record disclosures of telecommunications data. The Privacy Commissioner has the function of monitoring compliance with these record-keeping requirements.

130. Noting the operation of the robust and independent oversight mechanisms contained within TIA Act, the Telco Act and the Privacy Act, the Home Affairs Portfolio considers that safeguards for the Data Retention Scheme are working effectively.

The regulations and determinations made

131. While the Data Retention Act has now been fully implemented for over two years, the framework is not rigid. The TIA Act outlines two aspects of the regime which may be further defined through regulations:

- section 180X(3): outlining the role of a Public Interest Advocate in relation to the issuing of Journalist Information Warrants, and
- section 187C(2): varying the retention period for subscriber information to make it consistent with the retention period for traffic data (not exceeding two years after the information came into existence).

132. The TIA Act also provides that the Communications Access Coordinator (CAC) may make a decision in relation to a specified service provider to remove or vary the data retention obligations, or reduce the data retention period, either generally or in relation to data that relates to a particular kind of relevant service.[29] This allows for a conversation to be had between the CAC and those providers whose business needs require special circumstances or individual consideration.

133. Additionally, the TIA Act allows a number of ministerial declarations to be made relating to the nature of data sets and the status of enforcement agencies. Of particular note are:

[29] TIA Act, s 187(K).

- as per subsection 187AA(2), a ministerial declaration modifying the datasets outlined in the table in section 187AA of the Act, and
- the capacity of the Minister to declare an agency a 'criminal-law enforcement agency' or an 'enforcement agency' under sections 110A or 176A of the Act, respectively.

134. Since the introduction of the Data Retention Act, no regulations or determinations have been made. However, a number of agencies have sought to be determined as law enforcement agencies, with others likely to do so in the future.

Requests for additional enforcement agencies

135. Operational needs and investigatory mandates can shift as criminals and crime types evolve. Accordingly, Commonwealth, state or territory authorities who do not currently have access to telecommunications data may require access at a later stage, either temporarily for a specific operation or on a permanent basis as their investigatory requirements change.

136. Under the TIA Act, an agency that seeks to be added as an 'enforcement agency' must submit a case to the Minister for consideration. The submission should clearly identify whether the agency is seeking a temporary declaration as an enforcement agency or permanent listing as an enforcement agency (permanent listing can only be achieved through an amendment to the TIA Act).

137. The Department of Home Affairs has developed a set of criteria to assist the Minister in evaluating requests from agencies. These criteria seek to address the mandatory requirements that are found in the TIA Act.[30] This includes:

- the need for direct access to telecommunications data, including necessity rather than usefulness;
- privacy safeguards implemented by the requesting agency;
- the viability of the agency gaining adequate access via a joint operation with a law enforcement agency;
- the agency's ability to comply with the obligations of the TIA Act;
- whether the declaration is in the public interest; and
- other relevant matters such as consistency across jurisdictions.

138. Pursuant to subsection 176A(11) of the TIA Act, any legislative amendment (once declared) to what constitutes an 'enforcement agency' also requires referral to the PJCIS for review. Subsection 176A(10) of the TIA Act provides that where the Minister declares an authority or body to be an enforcement agency, that declaration is effective for no longer than 40 sitting days of the Parliament following the commencement of the declaration. Permanent changes to the meaning of enforcement agency would require an amendment to the Act and a referral to the PJCIS.[31]

139. Additional agencies with significant criminal, intelligence or revenue-related functions may seek to be considered under this framework in the future.

[30] TIA Act, s 176A.
[31] TIA Act, s 176A(11).

Department of Home Affairs' use of telecommunications data

140. The Department of Home Affairs[32] is a 'criminal law enforcement agency' under section 110A of the TIA Act. However, the Department's status as an enforcement agency to telecommunications data is restricted to listed purposes, namely investigations of contraventions of:

- the *Customs Act 1901* (Cth),
- the *Crimes Act 1914* (Cth),
- the *Criminal Code Act 1995* (Cth),
- the *Environment Protection and Biodiversity Conservation Act 1999* (Cth),
- Part 6 of the *Australian Border Force Act 2015* (Cth), or
- Acts or provisions of Acts prescribed in a legislative instrument. [33]

141. This does not include the use of telecommunications data for the purpose of investigations under the *Migration Act 1958* (Cth) (the Migration Act).

142. The investigation of compliance with the Migration Act forms a key function of the Home Affairs Portfolio. Due to the non-inclusion of Migration Act functions, the Department of Home Affairs is unable to authorise requests for telecommunications data through the Data Retention Act for these purposes.

Costs

Data Retention Implementation Grants Program

143. At the time the data retention provisions were designed, the PJCIS recommended that "the Government make a substantial contribution to the upfront capital costs of service providers implementing their data retention obligations."[34]

144. This manifested in the Government agreeing to pay a "reasonable portion" of industry's implementation costs, and establishing a demand-driven data retention implementation grants program (DRIGP) to fund 50 per cent of the mid-point of an estimate of industry's capital cost of implementing a mandatory data retention scheme that included stringent security controls.

145. This program was intended to make a one-off contribution towards existing service providers' costs in adjusting to meet the new obligations. A grants scheme of $128.4 million was agreed. New entrants to the market were expected to be compliant and, as such, ongoing funding was not considered necessary. To date, a total of $127.9 million has been provided in grants, to a total of 175 Australian providers.

---

[32] The Department of Home Affairs is the Department administered by the Minister administering Part XII of the *Customs Act 1901*, within the meaning of the 'Immigration and Border Protection Department' in subsection 5(1) of the TIA Act.

[33] TIA Act, s 110A.

[34] Parliamentary Joint Committee on Intelligence and Security, *Advisory Report on the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014*, pg xvi <https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/Data_Retention/Report>.

ANAO Report

146. The design and implementation of the grants scheme was the subject of an ANAO review, the findings of which were released in a report dated 21 August 2018.[35] While the ANAO was critical of some aspects of the grants scheme, the purpose of assisting roughly half of the affected providers in making the necessary arrangements to retain the required data in a reliable and secure manner was achieved. The report found that overall, the grants scheme had come in under cost, with very few cases of misallocation or fraud uncovered.

147. The report also found that industry consistently and significantly overestimated the costs when estimating the financial impacts of compliance with the Data Retention Act. The process of acquitting grant applications against actual reported implementation costs also provided some evidence that the level of financial impost on many providers was lower than had initially been expected.[36]

148. In determining the effectiveness of the implementation assistance, it should be considered that, at this stage, no request for telecommunications data made by an enforcement agency to any of the providers that received a grant has been declined due to a lack of capability. Similarly, there have been no reported security breaches of data stored by industry for the purpose of the scheme. This indicates that the money granted to providers to make the necessary implementation arrangements, and the scrutiny of providers' planned security arrangements, represented reasonable value for money.

149. The long-term value of this investment can only by realised by maintaining this scheme. With the grants issued to bring industry up to standard, any move to remove or substantively lower the retention obligations would erode the overall value for money.

Industry charging model

150. Beyond the initial implementation outlay, there are now opportunities to increase the overall value of the scheme. It was agreed by Government that the ongoing costs associated with the provision of telecommunications data should continue to be met by agencies under the 'no profit-no loss' obligation for industry as outlined in the Telco Act.

151. Agencies have reported that, contrary to expectations, the unit cost of information within the now mandatorily retained data sets has not dropped since the conclusion of the grants program. They further expressed concern that though data retention has increased the availability of information, the agencies harbour concern that the high cost of some datasets (especially data over 12 months old) may adversely impact agency demand for them.

152. Agencies also remarked that the data disclosed by service providers lacks clarity and consistency, with some providers charging more than others for comparable datasets. An example of price disparity can be shown as follows:

[35] Australian National Audit Office, *Administration of the Data Retention Industry Grants Program* <https://www.anao.gov.au/work/performance-audit/administration-data-retention-industry-grants-program>.
[36] Ibid.

OPTUS	1 day	1 week	1 month*	2 months*
CCR	$100	$100	$200	$256
SMS	$100	$100	$100	$100
Data	$100	$100	$200	$400
Total	$300	$300	$500	$756

*1 month = 28 days, 2 months = 56 days

TELSTRA	1 day	1 week	1 month*	2 months*
CCR				
SMS				
Data				
Total	$30	$210	$900	$930

*1 month = 30 days, 2 months = 60 days

VODAFONE	1 day	1 week	1 month*	2 months*
CCR				
SMS				
Data				
Total	$28	$28	$112	$224

*1 month = 28 days, 2 months = 56 days

153. Further to this, providers also charge significantly more for data requests examining a longer period, and as such are often required to establish patterns of communications between persons of interest over a number of weeks or months. The WACCC noted that the amount charged by providers for requests of retained data with extended durations has become increasingly expensive to the point where they may not be pursued due to the associated costs.

154. Further, agencies noted the lack of clarity between themselves and providers often led to confusion over the correct template or method through which to provide a request. In such cases, a provider will charge an agency simply for responding to a request with a notification advising of a new template.

155. The National Criminal Intelligence Capability Committee (NCICC) have discussed the inconsistency in costs charged by telecommunications carriers and lack of oversight on this. NCICC would welcome a Commonwealth regulatory body to act as an interface in future dealings between agencies and providers. Such a body could influence the provision of data in a standardised format and ensure that it is delivered in a consistent and secure manner at an equitable cost.

156. With request and disclosure methods becoming increasingly automated, it could be timely for a review of the charging and request frameworks between agencies and providers. Regulating the requesting scheme between agencies and providers would create time efficiencies for investigators, and may reduce overall costs.

Security requirements

157. The Home Affairs Portfolio notes the critical importance that retained data be protected and subject to sufficient cybersecurity measures to guard against the unauthorised use of personal information. The ability of providers and agencies to enact adequate security measures was key to assuring the public that the retained datasets would only be used for the purposes specified in the legislation.

158. Issues of privacy and security were highlighted through extensive outreach and collaboration with industry stakeholders.

Industry perspectives

159. There have been no reports of increased instances of data being hacked or lost as a result of the Data Retention Act. Similarly, the lack of any notifiable data breaches found by the OAIC in carrying out its oversight functions attests to the suitability of the security measures put in place to protect retained telecommunications data.

160. Under the Data Retention Act, providers were required to create systems to store, process and dispatch telecommunications data upon request to law enforcement and intelligence agencies. The attractiveness and scale of the data pools retained by the larger providers was an important consideration in the drafting of the legislation.

161. The creation of centralised platforms to retain data was foreshadowed by some in industry as a 'honey pot', or target for criminal or other nefarious actors. Major carriers raised concerns that mandatorily retained telecommunications data would give a hacker 'the pot of gold' to aim for, as opposed to their having to work through their multitude of systems in order to extract the same data.[37]

162. However, risks to customers' privacy existed prior to the implementation of this legislation. Providers already had in place sophisticated security frameworks to protect the customer data retained for commercial purposes. Given this, it did not follow that the proposed data retention scheme presented an unmanageable level of risk to customer privacy. The evidence to date supports that the existing data security arrangement have been effective.

Security assessment of Data Retention Implementation Plans

163. Data retention introduced a virtual graduation from basic security to defence-level mechanisms to prevent, detect, and respond to threats to this information. Implemented systems used integrated and layered security controls such as encryption, privileged access management, multi-factor authentication, and logging and auditing.

164. The government-managed DRIGP established the security framework governing telecommunications providers' storage of data retained under Chapter 4 of the TIA Act, to ensure user's privacy was protected. Each telecommunications provider was required to outline its existing retention policies (including what was retained and for how long). Providers were also required to detail a series of milestones to be undertaken throughout the implementation period to achieve the sufficient security standards for the data. In the case of many larger providers, existing security measures were deemed to be adequate.

165. Industry stakeholders were directed to existing Government guidance materials on information security and encryption, including:

- the OAIC Guide to securing personal information, which contains detailed information on how to protect personal information,

[37] Mr Mike Burgess, Chief Information Security Officer, Telstra, *Committee Hansard*, Canberra (29 January 2015) pg 9.

- the Australian Signals Directorate *Top 4 Mitigation Strategies and* Strategies *to Mitigate Targeted Cyber Intrusions*, and
- the Australian Government Evaluated Products List. [38]

166. Altogether, the Data Retention Act's information security and privacy controls have created a marked improvement to former security measures, in terms of protecting customer privacy information.

Telecommunications Sector Security Reforms

167. The Explanatory Memorandum for the Data Retention Act anticipated that the Telecommunications Sector Security Reforms (TSSR) would complement the introduction of the Data Retention Act by creating an additional layer of security regulation for Australia's critical infrastructure. Increased industry security standards have improved the overall protection of telecommunications data stored under Chapter 4 of the TIA Act.[39]

168. The TSSR impose a security obligation on carriers, carriage service providers and carriage service intermediaries within the meaning of the Telco Act requiring them to "do their best" to protect telecommunications networks and facilities from unauthorised interference and unauthorised access. Providers must also maintain competent supervision of, and effective control over, telecommunications networks and facilities they own or operate.

169. The TSSR information gathering power permits the Secretary of the Department of Home Affairs to obtain information or documents from regulated entities to assess their compliance with the security obligation.

170. The PJCIS is required to review the operation of the TSSR. The review must start on or before 18 September 2020 and must conclude on or before 18 September 2021.

Access by agencies under the *Telecommunications Act 1997*

171. While Schedule 2 of the Data Retention Act introduced improvements to privacy protections, restricting access to telecommunications data under the TIA Act to 21 agencies, telecommunications data can also be accessed under the Telco Act. The Telco Act is administered by the Department of Communications and the Arts.

172. Section 280 of the Telco Act provides an exemption to the general prohibition on the disclosure of telecommunications within sections 276, 277 and 278 of that Act, allowing agencies outside of the data retention scheme to use their own powers to seek access to this "if the disclosure if required or authorised under law". Requests under section 280(1)(b) are facilitated by industry obligations under section 313(3) of the Telco Act, which requires carriers and carriage service providers to give authorities "such help as is reasonable necessary". This is a licencing condition for all carriers.

173. Many Commonwealth, state and territory organisations have their own 'notice to produce' powers, set out in their own enabling statute. As a result, these bodies

[38] Attorney-General's Department, *Data Retention Frequently Asked Questions for Industry* <https://www.homeaffairs.gov.au/nat-security/files/data-retention-industry-faqs.pdf>.
[39] *Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014* (Cth), Explanatory Memorandum, pg 13.

can lawfully access telecommunications data under section 280, provided the request falls within their legislated powers. The Home Affairs Portfolio understands that section 280 is being used regularly to request telecommunications data.

174. While the OAIC has oversight responsibility for the Telco Act, the disclosure of data under section 280 is largely regulated by industry. Further, there is currently no legislative requirement for carriers and carriage service providers to report which agencies they disclose this data to, as had previously been released through the TIA Act annual reports.

Scope of access under the Telco Act

175. During last year's PJCIS review of the Assistance and Access Act, the Communications Alliance raised the issue of agencies not listed in the TIA Act accessing telecommunications data. Addressing the PJCIS, Communications Alliance noted that around 80 entities (including Commonwealth, state and territory government departments) had made requests for retained data under sections 280(1)(b) or 313(3) since the Data Retention Act was passed.[40] In its annual report, ACMA noted that in 2017-18, providers made 11,976 disclosures under section 280 of the Telco Act.

176. There are many lawful purposes for which government agencies request telecommunications data under the Telco Act. A range of government agencies not designated as 'enforcement agencies' for the purpose of the Data Retention Act investigate criminal activity or protect public revenue. Examples of this include coroners' courts, state justice departments, state revenue offices, Australia Post and the Australian Taxation Office.

177. It is important to note that section 280 itself does not authorise the disclosure of data. Rather, the section works in connection with existing laws, passed by Commonwealth or State and Territory legislative bodies, which set out their own thresholds and safeguards for access to personal information by relevant authorities. Section 280 enables these underlying laws to function as intended by relaxing the prohibition against disclosing telecommunications data if it is in response to a lawful request. Removing this exception would have serious implications to a range of entities across Australia.

178. Access through section 280 may appear inconsistent with the intention of the Data Retention Act: to increase the reliability of telecommunications data for selected agencies, within an appropriate framework of reporting and oversight. However, section 280 does not augment the range of agencies with access to mandatorily retained data. Subsection 280(1B)(b) specifically notes that the exception does not apply to the disclosure of any data kept solely for the purposes of the Data Retention Act to an entity not designated in the TIA Act. This means that agencies outside the TIA Act regime who use their own powers to access telecommunications data can only access data which a carrier or carriage service provider would have retained in the course of their usual business, absent obligations within the Data Retention Act.

[40] Mr John Stanton, Chief Executive Officer, Communications Alliance, *Committee Hansard*, Canberra (16 November 2018) pg 34.

International environment

179. Australia was not alone in recognising the importance of telecommunications data to criminal and national security related investigations, nor in mandating its retention through legislation.

180. The design of international data retention frameworks has not been without strong debate, and legal misstep. A year before Australia's Data Retention Act was enacted, the European Union Data Retention Directive was found invalid by the Court of Justice of the European Union (CJEU) on the grounds that the general and indefinite retention of various categories of data "exceeds the limits of what is strictly necessary and cannot be considered to be justified".[41]

181. The years since the passage of Australia's provisions have seen many countries implement their own legislation to govern the collection of telecommunications data for the purposes of law enforcement and national security. In doing so, each country has sought an appropriate balance between its citizens' expectations of privacy and the requirements of law enforcement and intelligence agencies.

182. It is necessary to maintain awareness of similar frameworks across the world. The table at Appendix A shows a contemporary outline of data retention legislation in other countries.

European Union context

183. In the case of *Tele2 Sverige*, the CJEU concluded that member states of the EU could not impose a general obligation on providers of electronic telecommunications services to retain data. However, the court's ruling did not ban data retention altogether, and such practice remains lawful where it is considered proportional to the seriousness of the types of crime targeted.

United Kingdom

184. Despite numerous challenges to its data retention legislation, the United Kingdom (UK) has persisted in efforts to maintained access to communications data given its critical role in law enforcement and national security investigations.[42]

185. On 8 April 2014, the CJEU ruled against the UK's voluntary data regime on the basis that it exceeded the limits created by the Charter of Fundamental Rights of the European Union. In response, the UK introduced the *Investigatory Powers Act 2016* (the IP Act) which provides an updated framework for security and intelligence agencies, law enforcement and other public authorities to obtain communications and telecommunications data.[43]

186. Under the IP Act, the Secretary of State can issue a 'retention notice' requiring a telecommunications operator to retain relevant data for up to 12 months.[44] The notice may be issued in the interests of criminal law enforcement, national security, the economic well-being of the UK, or public safety. The decision to issue a retention notice must be approved by a Judicial Commissioner.

---

[41] European Union: ECJ Invalidates Data Retention Directive, <https://www.loc.gov/law/help/eu-data-retention-directive/eu.php>.
[42] Ibid.
[43] *Investigatory Powers Act 2016* (UK) Overview ('Investigatory Powers Act').
[44] Investigatory Powers Act, s 87(3).

187. In 2018, the UK Government made further amendments to the IP Act to make the legislation consistent with EU law.[45] These amendments introduced independent administrative or judicial authorisation for most communications data applications, and restricted requests in criminal matters to the investigation of serious crime.[46]

Italy

188. According to the general resolution issued by the Italian Data Protection Authority on 'Secure Retention of Telephone and Internet Traffic Data', operators providing electronic communications services available in Italy are required to keep both telephone and internet traffic data for justice-related purposes.[47] The public prosecutor may access such data by means of a reasoned decree in compliance with the provisions of the Italian Criminal Procedure Code.

189. At the time of introduction, operators were required to keep telephone traffic data for two years, and internet traffic data for one year. A 2017 amendment subsequently extended both retention periods to 6 years.[48] This does not include the content of communications, which lawfully must not be retained by the operators.

Sweden

190. After the EUCJ ruled against the European Data Retention Directive, an assessment by Sweden's Ministry of Justice found that Sweden's version of the data retention legislation did not contravene the European Convention on the Protection of Human Rights and Fundamental Freedoms. The assessor found that it was compliant.[49] In June 2014, the Swedish Post and Telecom Authority ordered Swedish internet service providers to retain users' telecommunications data.

191. Under Sweden's *Electronic Communications Act 2003*, providers are required to retain for six months the date, time and duration of a communication, the type and location of communication, and subscriber details associated with the source and destination of a communication.[50] After six months, providers must destroy the records.

192. Debate in Sweden continues over how best to implement these laws, without risking a challenge and rejection by the CJEU.

Denmark

193. Denmark's surveillance law is also a local extension of the European Union Data Retention Directive and requires all communication providers, including telephones and internet providers, to retain a similar dataset to what is required under Australia's Data Retention Act. Providers must retain: the subscriber information for both A, B and C parties, the receipt for receiving a message, time

---

[45] Data retention and Acquisition Regulations 2018 (UK) Explanatory Memorandum <http://www.legislation.gov.uk/ukdsi/2018/9780111170809/pdfs/ukdsiem_9780111170809_en.pdf>.
[46] Ibid.
[47] International Comparative Legal Guides, *Italy: Telecoms, Media & Internet 2019* <https://iclg.com/practice-areas/telecoms-media-and-internet-laws-and-regulations/italy>.
[48] Ibid.
[49] Swedish data retention back in full swing minus one ISP, <https://www.zdnet.com/article/swedish-data-retention-back-in-full-swing-minus-one-isp/>
[50] Electronic Communications Act 2003, <https://www.riksdagen.se/sv/dokument-lagar/dokument/svensk-forfattningssamling/lag-2003389-om-elektronisk-kommunikation_sfs-2003-389#K6>

and duration of communication, and equipment information such as IMSI and IMEI numbers.[51]

194. Denmark has a data retention period of one year, and authorisation for access to this data is provided through a legal court where the application meets the grounds of suspicion, necessity and proportionality.

195. The Danish Ministry of Justice has indicated it may seek to amend the data retention provisions in the future.[52]

United States

196. The United States (US) currently has no 'blanket' data retention law or scheme. However, the US government may obtain access to any communications or communications records stored by providers, under the *Stored Communications Act* (SC Act). The SC Act establishes that providers must preserve stored data for up to 180 days upon request by government.

197. Access to data can also occur where access is compelled by a court order. As there is no legislative guidance on what data needs to be retained by providers, the data available will vary between service providers.

Conclusions

198. The Data Retention Act is part of the Australian Government's ongoing commitment to modernise investigatory powers and maintain a strong, proportionate and reasonable law enforcement and national security framework. This legislative framework has effectively enhanced the criminal and national security investigations of the agencies able to access it, while also ensuring the administrative rigour and data security standards expected by the Australian public.

199. Any substantial reduction in either the length of the retention period or the scope of the dataset could significantly reduce the ability of law enforcement and security agencies to effectively investigate criminal matters and threats to national security.

200. Furthermore, to reduce the scope of this legislation now would leave Australian law enforcement and intelligence agencies beholden to the policies practices of domestic and international providers' whose primary concern is the provision of telecommunications to its customers rather than maintaining Australia's safety and security. Given international precedents in recent years, it is likely that this dataset would be materially degraded from the level of access it afforded in 2014.

201. Almost four years after the passage of this legislation, telecommunications data remains a vital investigative tool for Australian law enforcement and intelligence agencies. Retaining consistent and reliable access to this data is and will remain of critical importance to law enforcement and intelligence agencies.

202. The Data Retention Act achieves a balance between the right to privacy and access to consistent data. The oversight mechanism and the mandating of data sets and retention periods have proven effective. The data retention scheme

[51] The Logging Order, 24-Staffing, Security Approval and the EU Logging Directive, <http://logningsdirektivet.dk>

[52] Litigation against the Danish government over data retention, <https://edri.org/litigation-against-the-danish-government-over-data-retention/>

remains a necessary, reasonable and proportionate response to the Australian threat environment.

Appendix A

Data Retention Legislation – International Comparisons

Country	Data Retention Period	Authorisation required to access the data	Status Of Data Retention Regime
Australia	2 years	Authorisation from within designated enforcement agencies. Higher level of authorisation required for journalist information.	Implemented 2015.
Belgium	Between 1 year & 36 months for 'publically available' telephone services. No provision for internet-related data.	A magistrate or prosecutor must authorise the access.	Declared unconstitutional.
Bulgaria	1 year, Data can be accessed for 6 months more upon request.	Magistrate or prosecutor must authorise the access.	Declared unconstitutional in 2008, and again in 2015.
Cyprus	6 months	A prosecutor approval is needed to access the data if he might ask for evidence in the case of committing a stern crime. A judge can issue such an order if there is a rational suspicion of a major criminal offense and if the data is expected to be linked with it.	Declared unconstitutional due to the violation of privacy rights.
Denmark	1 year	Judicial authorisation required for gaining access. A court order may be granted where an access application meets the strict criteria for suspicion, necessity, and proportionality.	Had implemented the EU data retention directive. Session logging ceased 2014.
Estonia		Permission from preliminary investigation judge is required for access.	Implemented.
Finland	1 year	Without judicial authorisation, all competent authorities can access user data. A court order is needed for other data.	Under review.
Germany	4-10 weeks		Introduction of data retention suspended until

Country	Data Retention Period	Authorisation required to access the data	Status Of Data Retention Regime
			final decision of the Higher Administrative Court of North Rhine-Westphalia.
Greece	1 year	Access requires a judicial decision declaring that investigation by all other means is impossible or extremely difficult.	Implemented.
France	1 year	To access retained data Police must provide justification and authorisation from a person in the Ministry of the Interior designated by the 'Commission Nationale de contrôle des interceptions de sécurité'.	Implemented.
Spain	1 year	Judicial authorisation is required by all competent authorities to access retained data.	Under review.
Hungary	6 months for unsuccessful calls and 1 year for all other data.	Police and the National Tax and Customs Office need prosecutor's authentication. Prosecutor and national security agencies can access such data without a court order.	Preparing further constitutional challenge in opposition to the law.
Italy	Up to 72 months (6 years) for both telephone and internet traffic data (excluding the content of the communications). Prior to this, 2 years of fixed telephony and mobile telephony data, and 1 year of internet access, email and internet telephony data could be retained.	Public prosecutor may access such data by means of a reasoned decree in compliance with the provisions of the Italian Criminal Procedure Code.	Implemented.
Lithuania	6 months	Authorised public authorities must request	Implemented.

Country	Data Retention Period	Authorisation required to access the data	Status Of Data Retention Regime
		retained data in writing. Pre-trial investigations require a judicial warrant for accessing the data.	
Latvia	18 months	Authorised officers, public prosecutor's office, and courts are required to access 'adequacy and relevance' of the request, to record the request and ensure the security of data obtained.	Implemented.
Luxembourg	6 months	Judicial authorisation required.	Under review.
Malta	1 year for fixed, mobile and internet telephony data, 6 months of internet access and internet email data	Requests made by Malta Police Force; Security Service must be in writing.	Implemented.
Netherlands	1 year telephony, 6 months internet-related data	Order of a prosecutor or an investigating judge required.	On 11 March 2015, national law was suspended. The decision is a preliminary injunction rendering the obligation ineffective.
Russia	6 months. Providers required to store phone calls, text and email telecommunications data, as well as the actual voice recordings.		Implemented in 2016.
Poland	2 years	Requests must be in writing and in the case of police, border guards, and tax inspectors, authorised by the senior official in the organisation.	Under judicial challenge.
Portugal	1 year	Transmission of data requires judicial authorisation on grounds that access is crucial to uncover the truth or that evidence would be, in any other manner, impossible or	Implemented.

Country	Data Retention Period	Authorisation required to access the data	Status Of Data Retention Regime
		very difficult to obtain. The judicial authorisation is subject to necessity and proportional requirements.	
Slovenia	8 months for internet related and 14 months for telephony related data	Judicial authorisation required.	Declared unconstitutional and ordered the deletion of data collected under the data retention law.
Slovakia	1 year for Internet data	Written request required.	Retained data has been deleted and have stopped following the orders of the European Court of Justice.
Sweden	6 months		Expected to face judicial challenge.
Switzerland	6 months for mobile phone and email telecommunications data. Does not include content of the communication.		In 2016 the Swiss Federal Law about the Surveillance of the Post and Telecommunications entered into force. Current status unknown.
United Kingdom (UK)	Up to 12 months	Authorisations for obtaining communications data may be granted by a designated senior officer of a relevant public authority.	Investigatory Powers Act 2016 (UK). Amendments made under the Data Retention and Acquisition Regulations 2018.
Ireland	2 Years of fixed telephony and mobile telephony data, 1 year for internet access, internet email and internet telephony data	Requests to be in writing from police officer/military over specified rank & tax/customs official over the specific grade.	Under judicial challenge
United States of America	1 year for Internet telecommunications data, email, phone records	Various United States agencies leverage the (voluntary) data retention practiced by many U.S. commercial organisations like Amazon.	No mandatory data retention regime

Appendix B

Data Retention – Additional case studies

To assist the Committee in its consideration of the effectiveness of the *Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015* (Cth), the Home Affairs Portfolio has gathered some additional case studies which illustrate the ways in which telecommunications data is used to aid investigations.

Any additional detail on these case studies should be sought from the contributing agency.

Agency: Australian Border Force

Case 1

In a 2018 investigation into multiple importations of smuggled tobacco, telecommunications data was used to provide circumstantial evidence of suspects' movements, in relation to events of interest. The data was used in conjunction with other evidence, such as closed circuit television (CCTV) footage and eyewitness accounts, to establish a pattern of criminal behaviour.

This investigation led to the identification of many prior instances of tobacco smuggling. Historical telecommunications data assisted in building a more accurate and complete understanding of the extent of the offending.

Case 2

In an Australian Border Force investigation into illicit tobacco smuggling, CCR checks on a person of interest (POI) demonstrated their movements matched pattern of offending across multiple states. The POI was able to be linked to phone calls crucial to the case by matching CCRs with CCTV footage. This evidence proved critical to the case, which involved the smuggling of 5.88 million sticks of cigarettes.

Agency: Australian Competition and Consumer Commission

Case 1

The Australian Competition and Consumer Commission (ACCC) suspected two POIs were communicating with each other after being made aware of their investigation. CCRs confirmed that the two POIs communicated with each other in the lead up to, and after, the ACCC conducted separate and simultaneous interviews with each.

The CCRs also provided another lead, identifying three previously unknown mobile numbers which both POIs contacted during the relevant period of the alleged cartel conduct.

Case 2

The ACCC investigated the extent to which a POI was interacting with other witnesses. CCR results spanning a five year period allowed the investigation team to identify a pattern of telephone communication between the POI and another key witness, including a lengthy

phone conversation on the day the POI's employment was terminated. This allowed ACCC staff to identify and obtain an email (via ACCC powers not related to the mandatory data retention regime) which coincided with the lengthy phone call.

The CCRs also provided the ACCC with additional lines of inquiry in relation to other suspicious phone calls between the POI and other witnesses during the investigation period.

Case 3

In a cartel investigation, CCRs were used as a means to corroborate an informant's recollection and to confirm that two competitors were in contact with each other during the period of the alleged conduct. CCR results also helped identify a third potential POI, which would not have been possible without speaking with that person's employer (which would have resulted in taking an overt step in the investigation at a point in time where this was undesirable). The CCR results have also been used to map the locations of the POIs to identify potential meetings during the period, which also provided additional lines of inquiry.

Agency: Australian Federal Police

Case 1

In an investigation into a syndicate allegedly involved in large-scale taxation fraud, the Australian Federal Police (AFP) obtained historical telecommunications data, CCRs and reverse call charge records (RCCRs), for a phone belonging to the accused. The telecommunications data obtained by the AFP aided the defence at trial and proved the accused made a phone call that was central to the defence case. The AFP requested the telecommunication data 18 months after the call was made and may not have been retained by the provider prior to the data retention regime coming into place.

Case 2

In 2017, the AFP conducted an investigation into an alleged organised crime syndicate, which resulted in the second-largest drugs seizure in Australian history: 1.28 tonnes of cocaine, with a potential street value nearing half a billion dollars. The investigation made considerable use of CCRs, which indicated relationships between POIs and criminal associations including outlaw motorcycle gang (OMCG) links.

Agency: Australian Securities and Investments Commission

Case 1

The Australian Securities and Investments Commission (ASIC) commenced an investigation based on a suspicious matter report referral from an ASX market participant who had identified that a single IP address was regularly placing multiple orders for the same security from numerous, apparently unrelated, trading accounts. ASIC obtained telecommunications data which established that the POI was the individual that owned the various email addresses.

This data also established that the orders from the reported individual trading accounts were all in fact from the same IP address, which was being used by the POI at the time of security

purchases. Telecommunications data also confirmed that telephone calls made to various stock brokers purporting to be from various individual account holders, were in fact made by the same POI from their mobile phone.

The evidence from this data provided sufficient grounds to obtain a search warrant that ultimately identified other relevant and admissible evidence. In this case the telecommunications data was between 12 to 18 months old, and in some cases older, as information from 2017 data demonstrated the need to retrieve telecommunications from 2014.

Case 2

In a recent investigation ASIC obtained telecommunications data that resulted in the accused being charged with, and pleading guilty to, an offence under section 247A of the *Crimes Act 1958* (Vic).

ASIC's allegation was that the accused, without authority, altered data held on a computer. The data in question was voting records in elections for the director of a credit union. The accused had obtained the necessary personal information of credit union members that enabled him to vote numerous times in the election and thus alter the outcome. The accused claimed that he had telephoned all of the members on whose behalf he had voted (approximately 600 people) and obtained their authority to vote.

ASIC obtained call charge records that demonstrated that, at the relevant time, the accused had made hardly any telephone calls. This evidence was sufficient to disprove the claim that the accused had authority to vote prior to the commission of the offence and led to his plea of guilty. In this matter the telecommunications data was 20 months old.

Agency: Law Enforcement Conduct Commission

Case 1

The Law Enforcement Conduct Commission (LECC) investigated a police officer for allegations of money laundering, serious fraud and improper relationship spanning many years. The provider was able to provide CCRs for four years prior, which established contact between the suspected parties at the time the alleged fraud commenced. This data was invaluable in proving a long term relationship between the subject officer and another POI complicit in the activity. In addition, the data corroborated allegations of specific fraudulent activity conducted through financial institutions.

This data, when combined with other intelligence, also showed a pattern of behaviour around other corrupt conduct. The CCRs significantly contributed to a body of evidence indicating serious fraud, which enabled the LECC to apply for and be issued with telecommunications interception warrants. The investigation uncovered criminal and corrupt conduct, in relation to fraud and unauthorised release of confidential information.

During this operation, multiple requests for data exceeding four years were successfully retrieved by the carrier and assisted in the resulting prosecution.

Case 2

In the course of a LECC investigation, a target unexpectedly travelled twice by vehicle to a remote location, raising suspicion. The LECC then made use of geo-fencing technology configured to alert when the target's location data indicated travel towards this remote location. Following this, the LECC deployed physical surveillance to determine the purpose of this travel. This deployment resulted in effective intelligence being gathered that significantly contributed to the outcome of the investigation.

Agency: New South Wales Crime Commission

Case 1

In its homicide investigations, the New South Wales Crime Commission (NSWCC) regularly conducts coercive examinations with witnesses. It is a criminal offence in those hearings to give false or misleading evidence in a material particular. Occasionally witnesses are charged with providing misleading evidence or other offences against the *Crime Commission Act 2012* (NSW).

During a 2017 murder investigation, a hearing was held with a witness who was associated with a POI. The witness gave evidence concerning his and his associate's use of a telecommunications service; evidence which police allege was false and misleading. Telecommunications records were obtained, in several instances more than one year after the murder.

This telecommunications data was critical to the brief of evidence against the witness, who later pled guilty to the charges.

Case 2

In 2017, the NSWCC commenced investigating a shooting murder that was committed in 2016. By obtaining the forward and reverse call charge records for telecommunications services linked to numerous POIs (some of the records were from 13-14 months after the offence), investigators were able to chronologically reconstruct the pattern of phone contacts and cell site movements of the POIs in the lead up to the shooting incident.

As a direct result of these records, investigators have been able to confirm and eliminate suspects based on their cell site locations at the time of the shooting.

Agency: New South Wales Independent Commission Against Corruption

Case 1

The New South Wales Independent Commission Against Corruption (NSWICAC) investigated an allegation of corrupt conduct where a POI attended a meeting with other individuals. A number of these individuals denied that the meeting occurred despite one witness statement to the contrary.

Telecommunications data was sought for the individuals in the days before, during the meeting and afterwards. Analysis of the data showed that the meeting location was out of the ordinary for some of the individuals.

Corroborating evidence from telecommunications data analysis placed the individuals in the area, and contributed to the outcome of this investigation.

Case 2

In 2017-2018 NSWICAC investigated allegations of fraud in an investigation where a person claimed to have documents witnessed by an interstate Justice of the Peace more than six months earlier.

Telecommunications data indicated that the person was in NSW at the time they alleged they were interstate. Investigators sought other evidence, including banking records, which further proved the person was in NSW at the time.

The corroborating telecommunications data was a key part of the investigation.

Agency: Queensland Crime and Corruption Commission

Case 1

The Queensland Crime and Corruption Commission (QCCC) conducted a corruption investigation into allegations that police officers in a regional area were accessing a police database without authorisation, and providing confidential information to criminal associates. These police officers were also allegedly using and supplying dangerous drugs (steroids).

Historical CCR data (from two years prior to commencement of investigation) was obtained and used to verify, and in some instances refute, allegations that subject officers had long-standing social relationships with criminal associates. Telecommunications data was also used to demonstrate contact between some officers and criminal associates around the time of alleged unauthorised checks of the police database.

Many of the allegations related to events that were between 12 months and three years prior to the commencement of the investigation, therefore the historical data was essential.

Case 2

The QCCC conducted an organised crime investigation into a range of alleged fraud offences committed by solicitors from a law firm. Historical CCR data was obtained for a period in 2015 (three years prior to the investigation), for three subject officers. The data was used to corroborate allegations that the suspects met at a particular location at a particular time to discuss a matter subject to the allegations. Cell tower data from the CCRs was used to verify that the suspects were all in a similar proximity at the time of interest.

The data was then used in a closed hearing to refute claims made by the suspects that they had not met on that occasion.

Agency: Queensland Police

Case 1

In November 2018, a male person went missing in the Toowoomba area. Available information suggested one of two scenarios having occurred: that he was last seen walking

into a bushland on the Toowoomba Range, or that he had been murdered at Dalby, some 100 kilometres west of Toowoomba. An initial search of bushland failed to locate the missing person and investigations needed to be widened.

As a result of the analysis of telecommunications data obtained on the missing person's phone (0-3 months) the Dalby scenario was discounted, and it appeared that the bushland scenario was the most likely. Policing resources were then concentrated on two extensive land searches in rough terrain including the use of specialist personnel.

The remains of the missing person were located in dense bushland in March 2019, in an area that would not have been considered at that time if not for the reliability of the telecommunications data.

Case 2

In 2018, an investigation was commenced into multiple burglary offences being committed in the Brisbane area. Telecommunications data on a primary suspect placed the offender's mobile handset at multiple locations where burglaries had occurred.

This information led police to identify a hotel where the offender had been staying and they were able to obtain CCTV images from that hotel showing the offender leaving and returning from the hotel at relevant times wearing clothing matching low-quality home CCTV images obtained from various offence locations. This data also identified the existence and location of a storage shed where the offender had been storing stolen property.

Agency: South Australia Independent Commissioner Against Corruption

Case 1

Location data proved extremely important in a recent corruption investigation by the South Australia Independent Commissioner Against Corruption. The location data was obtained from the telecommunication data records and from additional data obtained from the carrier, in the form of global positioning system and cell tower data. Analysis of the location data associated with two services, along with other evidence, was able to show two suspects being together at a place and time of relevance to the case. The majority of the data requested for this investigation was aged between 12 and 24 months.

This evidence was a key aspect of the prosecution brief presented to the Director of Public Prosecutions. The accused was subsequently found guilty of 47 counts of deception.

Agency: Victoria Independent Broad-based Anti-corruption Commission

Case 1

A Victoria Independent Broad-based Anti-corruption Commission (VicIBAC) investigation identified an individual who was unlawfully accessing, altering and disclosing official records to known members of an OMCG. Call charge records (0-3 months and older than 12 months) were correlated with system logs to demonstrate collusion and connection between the individuals during periods of unlawful access and alteration.

The main person of interest subsequently pled guilty to a number of charges of misconduct in public office.

Case 2

In December 2015, VicIBAC commenced an investigation into the leaking of information concerning allegations of drug trafficking within multiple Victorian public service organisations. During the course of this investigation, a POI subverted the execution of a lawful search by VicIBAC by concealing the location of a mobile device. Call charge records (0-3 months) obtained following the search were instrumental in disproving the alibi provided by the POI.

Case 3

VicIBAC conducted an investigation in 2017 into corrupt activity by a drug rehabilitation officer, which led to the identification of an extensive network of individuals involved in drug trafficking and perverting the effective performance of the court system through misrepresentation in bail and community correction orders proceedings. A range of prospective and retained telecommunications data records (including CCRs for 0-3 months, 3-6 months and 6-9 months) were used to identify communications in key periods to substantiate interactions between POIs.

Over 20 individuals were subsequently charged with offences including trafficking a drug of dependence, perjury, perverting (and attempting to pervert) the course of justice.

Agency: Victoria Police

Case 1

In 2016, the Victoria Police investigated a series of related offences comprising trafficking drugs of dependence, firearms offences and conspiracies to engage in conduct endangering life. The majority of the syndicate were identified and charged with this offending. Those believed to be responsible for ordering and directing the offences to occur were not.

In 2018, a suspect believed to be one of those responsible for ordering and directing some of the offending was identified. As a result, telecommunications data requests including Integrated Public Number Database (IPND), incoming and outgoing call records and cell tower information were authorised. The telecommunications data showed communication between the new suspect and co-accused at specific times of offending and allowed the movements to be mapped to and from their addresses to offence locations before, during and after the offences. The availability of this data has led to fresh prosecutions.

Case 2

The Victoria Police investigated a serious assault committed by OMCG members in 2014. The offenders were subsequently charged and the matters were to proceed to trial in 2016. Prior to the trial, the first accused offered to plead guilty to significantly lesser charges. Prosecutors had concerns about the evidence in existence not conclusively confirming OMCG affiliation and the identity of both parties.

Investigators re-analysed the accused's mobile phone and obtained telecommunications data including IPND, incoming and outgoing call records and cell tower information. The requests for data were submitted two years after the offence.

This analysis and the records obtained comprehensively proved the issues beyond doubt. The first accused pleaded guilty to the more serious charges and received a high range sentence, upheld on appeal. This establishing significant case law in relation to offending on behalf of or in connection to an OMCG. The co-accused also elected to plead guilty rather than go to trial based on the new telecommunications data evidence.

Case 3

The Victoria Police conducted an investigation into firearms trafficking by an associate of an OMCG. Investigators obtained telecommunications data including incoming and outgoing call records to assist investigators to identify the suspect's associates, and discovered a pattern of attending a rural property. From this intelligence, investigators executed a search warrant at this property and the suspect's home address, seizing numerous illegal firearms.

Further analysis of historical data (aged approximately 12 months) identified the accused to have been in contact with a prominent OMCG figure, confirming the association. The data also assisted investigators with identifying an excavation business, chemical companies and another rural property owned by the suspect where numerous tunnels had been dug for the illegal storing of chemicals. Cell tower data was used to identify frequency of the accused attending this location and at unusual times of the day, strengthening investigators' case that the property was used for illegal activity.

Agency: Western Australia Corruption and Crime Commission

Case 1

The Western Australia Corruption and Crime Commission (WACCC) received a notification relating to the release of official information through the use of portable media devices. The information received led to the review of the use of a restricted computer system, with evidence obtained correlated with CCR data.

Overall, the operation resulted in a charge that a POI had unlawfully accessed a restricted-access computer system to gain a financial benefit. Without the use of retained historic data, the commission would have extended the duration of the investigation and potentially impacted the privacy of individuals in a way far greater than was otherwise needed.

Case 2

During an investigation to a breach of code of conduct, CCR data from a number of carriers was required to develop a timeline of events after the fact. The WACCC encountered limitations with the availability of carrier-provided data. A significant amount of additional investigation was required in order to compensate for the lack of telecommunications data records.

While the end result was of significant value to the investigation, and ultimately allowed the investigation to exclude POIs from the investigation, the resources required to ascertain this data was demanding. Had more RCCR data been available from the carriers, the investigation would have benefitted.

Agency: Western Australia Police Force

Case 1

Telecommunications data, specifically Visitor Location Register (VLR) and CCRs/RCCRs, were pivotal in establishing a prima facie case against three POIs accused in relation to a complex homicide investigation.

From the telecommunications data, Western Australia Police Force (the WA Police Force) investigators were able to establish a timeline of the deceased's movements and interactions leading up to his murder. More importantly, the data provided evidence of the contact between the co-accused, and their whereabouts before during and after the crime. Both the accused and the deceased were using numerous telecommunications services. Each of these services provided data relevant to the investigation.

The data helped establish vital avenues of inquiry, such as potential CCTV and additional witnesses, giving investigators irrefutable evidence to devise interview strategies and contradict the accused's alibi.

At the commencement of this investigation, the identity of the accused were not known. The assurance of telecommunications data being stored for a period of two years allowed investigators to request important data as it became relevant in the case and potential suspects emerged. Had this data not been available, it is likely that there wouldn't have been sufficient evidence to substantiate the charges against the accused in this matter.

Case 2

Following the discovery of a person's remains, suspects were identified in relation to the person's disappearance. Police were able to trace the suspects' movements using the mobile cell towers VLR, and place the suspects in the area at the time the victim's body was placed into the Swan River.

The evidence provided by telecommunications data was invaluable during the trial, as it was irrefutable evidence that the offenders were at the crime scene.

Case 3

A person's remains were located in mangroves in a regional West Australian town in August 2017. The last confirmed sighting of the deceased had been in early 2016. Telecommunications data was used to ascertain the last known movements of the deceased. Phone records assisted in establishing when the deceased had last used his mobile phone, which then narrowed down the possible time of death. This allowed the WA Police Force to explore further investigative opportunities.