



AUSTRALIAN CRIME COMMISSION

Submission to

Inquiry into the *Comprehensive revision of the
Telecommunications (Interception and Access) Act 1979*



UNCLASSIFIED

UNCLASSIFIED

Table of Contents

Summary	3
Role of the Australian Crime Commission	6
ACC and the <i>Telecommunications (Interception and Access) Act 1979</i>	7
What does the ACC use the TIA Act for?	7
How effective is TIA Act material for the ACC?	8
What authority does the ACC require to use the TIA Act?	9
Balancing the dual objectives of the TIA Act	10
Australian Law Reform Commission report	12
Inquiry into the potential reforms of Australia's National Security Legislation	14
Recommendations by the Parliamentary Joint Committee on Intelligence and Security	14
ACC proposed reforms to the TIA Act	14
Assistance from telecommunications service providers	15
Telecommunications data retention	15
Use of TIA Act material for ACC functions	17
Revised TIA Act information sharing provisions	18
Redrafting of the TIA Act	20
ACC Board Position	20
Conclusion	20
Attachment A – ACC response to PJCIS recommendations	21

UNCLASSIFIED

**Inquiry into the
Comprehensive revision of the Telecommunications (Interception and Access) Act 1979
Australian Crime Commission (ACC) Submission
March 2014**

1. The Australian Crime Commission (ACC) welcomes the opportunity to make a submission to the Standing Committee on Legal and Constitutional Affairs Inquiry into the *Comprehensive revision of the Telecommunications (Interception and Access) Act 1979* (TIA Act).
2. This submission is unclassified and may be published in the public domain. It addresses both terms of reference for this Inquiry:

Comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the Act), with regard to:

- a) the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2; and
- b) recommendations relating to the Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation* report, dated May 2013.

Summary

3. The criminal environment has changed significantly since the enactment of the TIA Act. Organised criminals no longer rely on domestic telephone communications to organise and support their activities. Complex networks stretch across continents to support illicit activities that range from drug importation to identity fraud, cybercrime to high-level offshore tax evasion, counterfeit goods to money laundering, and even environmental crime. Those networks are supported by sophisticated and resilient communication methods which are continually changing and adapting to take advantage of the latest technology and security developments. ACC investigations are now often faced with instances where only partial discovery of information is possible. This has effectively diminished the authority initially issued by Parliament in 1979 in relation to interception.

Evolution of Telecommunications

In 1979, when the TIA Act was enacted, a warrant could be expected to capture the entirety of a person of interest's telecommunications; a home phone, a business phone, and a public telephone favoured by a criminal. Today, consumers and criminals have an almost unlimited choice of telecommunications service providers, access points to connect to the internet, devices that can be used to communicate and applications to facilitate communication. Changes in the way communications technology is delivered and used means that the capability to intercept the full range of communications, devices and applications used by criminals continues to decline.

EVOLUTION OF TELECOMMUNICATIONS

Commencement of the
*Telecommunications
(Interception and Access)
Act 1979*



1980

DEVICES

HOME PHONE, BUSINESS PHONE, FAX

TELECOMMUNICATIONS SERVICE PROVIDERS

TELECOM



1995

ACCESS POINTS

DIAL UP, ADSL

DEVICES

HOME PHONE, BUSINESS PHONE, FAX, MOBILE PHONE, DESKTOP COMPUTER

TELECOMMUNICATIONS SERVICE PROVIDERS

TELECOM, OPTUS



2010

ACCESS POINTS

WIFI, HOTSPOTS, ADSL, NBN, 3G, 4G, LTE, INTERNET CAFÉ, HOTEL, AIRPORT

DEVICES

HOME PHONE, BUSINESS PHONE, FAX, SMART PHONE, DESKTOP COMPUTER, LAPTOP, TABLET, GAMING CONSOLE

TELECOMMUNICATIONS SERVICE PROVIDERS

TELSTRA, OPTUS, VODAFONE, iiNET, INTERNODE, ETC.

ANCILLARY PRODUCTS

SMART PHONE APPLICATIONS, VOIP (VIBER ETC.), IM, EMAIL

ANCILLARY PROVIDERS

APPLE, GOOGLE, MICROSOFT, BLACKBERRY, INDEPENDENT DEVELOPERS



2025

ACCESS POINTS

WIFI, HOTSPOTS, ADSL, NBN, 3G, 4G, LTE, INTERNET CAFÉ, HOTEL, AIRPORT

DEVICES

HOME PHONE, BUSINESS PHONE, FAX, SMART PHONE, DESKTOP COMPUTER, LAPTOP, TABLET, GAMING CONSOLE

TELECOMMUNICATIONS SERVICE PROVIDERS

TELSTRA, OPTUS, VODAFONE, iiNET, INTERNODE, ETC.

ANCILLARY PRODUCTS

SMART PHONE APPLICATIONS, VOIP (VIBER ETC.), IM, EMAIL

ANCILLARY PROVIDERS

APPLE, GOOGLE, MICROSOFT, BLACKBERRY, INDEPENDENT DEVELOPERS

EXPANSION OF TECHNOLOGY

BIOMETRICS, SMART DEVICES (WATCHES & GLASSES), CLOUD, UNKNOWN?



UNCLASSIFIED

4. Both the Australian Law Reform Commission (ALRC) in its 2008 *For Your Information: Australian Privacy Law and Practice* report and the Parliamentary Joint Committee on Intelligence and Security 2012 Inquiry (PJCIS) noted that revision or a review of the TIA Act was required and suggested a series of amendments. The ACC supports reform of the TIA Act in so far as it facilitates recognition of the technology revolution that has occurred since 1979, supports the ACC's work combating serious and organised crime and enables the agency to lawfully respond to the contemporary and emerging threats impacting the Australian community, while at the same time adequately protecting individual privacy.
5. This submission aligns with the ACC's earlier submission to the PJCIS *Inquiry on Potential Reforms to National Security Legislation* in 2012. Key areas for reform of the existing legislation to be addressed in this submission include:
 - the inclusion of a general provision outlining the scope of obligations imposed on telecommunication service providers and ancillary service providers¹ to assist law enforcement and national security agencies
 - the explicit use of telecommunications data and content obtained under the TIA Act for ACC functions (as defined in the ACC Act), and enhanced powers to lawfully intercept content related to serious and organised crime
 - the development of a uniform standard for telecommunications data retention
 - the amendment of the information sharing provisions of the TIA Act to ensure that telecommunications data and content obtained under the Act can be shared where necessary, and
 - the TIA Act be comprehensively revised with the aim of reducing legislative complexity, maintaining investigative capabilities and ensuring privacy cognisant of the evolving telecommunications environment.
6. The ACC considers that the existing arrangements in the TIA Act, whereby there is a strong mechanism to protect individual privacy, ensure agency accountability and transparency while at the same time enabling interception and access to communications when necessary to support serious crime investigations, should continue.
7. The ACC considers its TIA Act compliance regime to be robust and to provide appropriate safeguards regarding the use of interception powers. This has been supported by the findings of the Ombudsman in recent reviews in which no adverse recommendations have been made to the ACC regarding its treatment of TIA Act material. The ACC has another level of oversight arising from the ACC Board and the establishment of Determinations.

¹ Ancillary service providers refer to providers of technologies and applications used to conduct or facilitate telecommunications. This includes but is not limited to mobile phone manufacturers and smartphone application developers.

UNCLASSIFIED

8. The ACC sees a compelling need to modernise the TIA Act to ensure provisions keep pace with changes in technology. The TIA Act must be capable of overcoming technological advances which are deliberately used to prevent law enforcement from lawfully intercepting and accessing communications.
9. The existing TIA Act negatively impacts upon the ACC's ability to satisfy its legislative mandate. Because of changes in technology, the ACC is hindered in its investigation of serious and organised crime due to the restrictions on its ability to collect and share material obtained under the TIA Act. The loss of data due to the absence of a standard mandatory data retention scheme also has a detrimental impact on ACC investigations, in terms of availability of data and certainty as to the period it will be retained. These issues will increasingly impact the ability of the ACC to fulfil its functions without reform.

Role of the Australian Crime Commission

10. The ACC is Australia's national criminal intelligence agency with a specialised investigative remit and capabilities. The ACC is governed by the ACC Board, and works in partnership with Board member agencies, international law enforcement agencies, as well as other Australian Public Service agencies under task force, joint operations and intelligence-sharing arrangements, to gather intelligence and investigate serious criminal activity.
11. The ACC maintains national criminal intelligence holdings, produces strategic intelligence assessments, and coordinates national operational responses to disrupt, deter, degrade and prevent organised crime impacting on Australia.
12. To undertake its work, the ACC employs combinations of coercive powers and traditional law enforcement techniques such as telephone interception, physical and technical surveillance, controlled operations and covert human intelligence sources (informants) as a composite approach to the gathering of criminal intelligence. It uses these capabilities to support partner agencies and to provide government with an independent assessment of the risk, threat and impact of serious and organised crime on the community and national interests.

Australian Crime Commission Board

The ACC Board consists of representatives of Australian's law enforcement and key national security and regulatory agencies, comprising all Australian Police Commissioners, the Secretary of the Attorney-General's Department, Commissioner of Taxation, the Chairman of the Australian Securities and Investment Commission, the Chief Executive Officer of Australian Customs and Border Protection Service, and the Director-General of the Australia Security Intelligence Organisation.

UNCLASSIFIED

ACC and the *Telecommunications (Interception and Access) Act 1979*

What does the ACC use the TIA Act for?

13. The TIA Act provides the ACC with the ability, under lawful authority, to collect the following in support of its investigations:²

- live communications passing over a network
- stored telecommunications held by a carrier, and
- telecommunications data.³

Key Definitions

What is interception?

- Interception refers to the capturing of the content of a communication in its passage across a network. That content is currently captured by a carrier or carriage service provider exercising a technical capability called 'interception capability'.
- The word 'access' was introduced to refer to obtaining a stored communication from a provider, but can also be used to refer to obtaining telecommunications data from a provider. If a single word is used to mean both 'interception' of live communications and 'access' to stored communications, the preferred word is 'access'.

What content can be intercepted?

- Under the TIA Act, the ACC can intercept the content of calls and/or internet activity on a mobile, fixed line, internet, or e-mail service when authorised under warrant. This includes for example the content of an SMS message and the content of a phone call.

What are stored telecommunications?

- Stored telecommunication means a communication like an SMS or e-mail while it is held by a telecommunications service provider (not on a user's computer or phone). That is, a communication that has passed over a network and is being held by a provider.

What is telecommunications data?

- Telecommunications data is also known as metadata, communications data and communications associated data.
- It is not defined explicitly in the TIA Act, but is accepted to mean information about a communication that does not include content or substance of that communication, such as:
 - Subscriber information, for example the name and address of the user
 - The service identifier used to send a communication, for example the customer's email address, phone number or Voice-over-IP number (internet telephone number)
 - The date, time and duration of a communication
 - Information about the location of the parties involved in a communication, for example mobile phone cell tower location

² Note that the ACC may conduct an investigation as part of ACC Board authorised investigations or intelligence operations, which the ACC Board may determine to be Special Investigations or Special Operations.

³ Access to this data may also be authorised if it is reasonably necessary for the enforcement of the criminal law or a law imposing a pecuniary penalty or protection of the public revenue.

UNCLASSIFIED

How effective is TIA Act material for the ACC?

14. TIA Act material is a necessary tool for the ACC and directly contributes to the investigation and prosecution of serious and organised crime. In 2012–13 the ACC reported that 62 arrests were made directly on the basis of lawfully intercepted information. In that year there were also 10 prosecutions for serious drug offences in which lawfully intercepted information was used in evidence.
15. More broadly, TIA Act material consistently provides an efficient method of obtaining information, in an evidentiary form, compared with other traditional law enforcement tools such as physical surveillance. Intercepted material can support a range of outcomes under ACC investigations and operations⁴ and is critical to the Commission being able to meet its mandate of disrupting, deterring and preventing organised crime impacting on Australia.

Effective use of TIA Act material

To respond to the threat of exploitation of the alternative remittance sector, the Board of the Australian Crime Commission established the Eligo National Task Force in December 2012 to deter and disrupt criminal groups and to work with industry to professionalise the sector and harden the environment to future threats. This Task Force is made up of participants from the ACC, Australian Federal Police (AFP), Australian Transaction Reports and Analysis Centre (AUSTRAC), key Commonwealth agencies and State and Territory law enforcement.

Since its commencement, the Eligo National Task Force has achieved:

- the seizure of more than \$27 million in cash
- the seizure of illicit drugs with a combined estimated street value of more than \$540 million
- the restraint of more than \$30 million worth of assets
- the disruption of 22 serious and organised criminal groups/networks
- the identification of more than 156 targets previously unknown to law enforcement
- the arrests of 115 people on 222 charges

The Task Force has also led to the shut down of three commercial amphetamine laboratories, including one of the largest and most sophisticated clandestine laboratories discovered by Victoria Police, and shut down one of the largest urban hydroponic cannabis operations discovered by the NSW Police Force.

The use of material obtained under the TIA Act has been a key contributor to the results of the Task Force. It has enabled the discovery of methodologies, groups and targets previously unknown to law enforcement (including groups and targets with links to offshore drug cartels and terrorism financing activities).

⁴ under s67 and the definition of *permitted purpose* in s5 TIA Act, the ACC may (amongst other things) use and communicate *lawfully intercepted information* and *interception warrant information* for a purpose connected with any ACC operation or investigation, a report to the ACC Board, and reports on its operations and investigations.

UNCLASSIFIED

What authority does the ACC require to use the TIA Act?

16. In practice, for the ACC to access telecommunications data and intercepted content under the TIA Act, the ACC Board must firstly authorise an ACC special investigation. An ACC special operation can acquire telecommunications data and intercepted content in more restricted circumstances, and where it contains an investigative component.

Special Operation vs. Special Investigation

The ACC Board may determine an ACC investigation or operation to be a Special Investigation or Special Operation, in which case ACC coercive powers are available to be applied for. An ACC Special Investigation is focussed on the disruption and deterrence of identified criminal groups and activities through collecting admissible evidence of criminal activity and typically results in arrests and/or seizures of illegally obtained assets.

An ACC Special Operation is primarily conducted towards scoping out and understanding the nature of serious criminal activity, particularly in key markets and sectors in the economy (primarily through the collection, correlation, analysis and dissemination of criminal information and intelligence relating to serious offences) and in providing assessments to governments and a range of government, and private sector bodies in accordance with the disclosure regime in the ACC legislation.

ACC Board authorised investigations are only approved on the basis that the Board has considered whether ordinary police methods of investigation are likely to be ineffective, and intelligence operations are authorised only after the Board has considered whether methods of collecting criminal information and intelligence that do not involve the use of coercive powers have been effective. The ACC Board may only authorise investigations and intelligence operations in relation to federally relevant criminal activity (specified serious and organised crime offending punishable by imprisonment for 3 years or more, or indigenous violence or child abuse).

Currently, the ACC Board has authorised a series of 2 x Special Investigations, 2 x State Special Investigations and 6 x Special Operations.

17. In addition to ACC Board authorisation of an investigation or operation, the ACC must seek a warrant to intercept telecommunications or access stored telecommunications from an independent Judge or nominated AAT member. In urgent circumstances, an oral application can be made for a warrant. Once an interception warrant is issued and executed, the ACC can use and communicate *lawfully intercepted information* (LII) and *interception warrant information* (IWI) in accordance with the provisions of the TIA Act.⁵ Similarly, once an access warrant is issued and executed, the ACC can record, use and communicate *lawfully accessed information* (LAI), *preservation notice information* and *stored communications warrant information* in accordance with the Act.⁶

⁵ Section 67 or 68 of the TIA Act.

⁶ Sections 139 and 139A of the TIA Act.

UNCLASSIFIED

18. To obtain access to telecommunications data, authorisation from an appropriate executive level ACC delegate is required. Pursuant to the TIA Act,⁷ the authorising officer must be satisfied that the disclosure of the information is reasonably necessary for the investigation of a serious offence or an offence carrying a minimum imprisonment period of three years.⁸ Pursuant to s180F the authorised officer must have regard to whether any interference with the privacy of any person(s) that may result from the disclosure or use of the information is justifiable.

Balancing the dual objectives of the TIA Act

19. The ACC supports the dual objectives of the TIA Act – protecting the privacy of communications while at the same time enabling interception and access when required in order to facilitate the investigation of serious crime and threats to national security.
20. The ACC considers that whilst the privacy of personal conversations and communication between individuals should be protected, serious and organised crime groups, both domestic and international, represent a significant threat to the privacy and civil liberties of Australian citizens and their international associates.
21. The ACC can assure the Committee that the ACC undertakes targeted collection of telecommunications data in support of its remit. It already has its targets or suspects identified. ACC uses specific telecommunications data to build a foundation for further investigative measures, including applications for interception and access warrants.
22. The ACC has very stringent oversight and accountability arrangements that govern the access, storage and use of material obtained under the TIA Act as well as the approval of ACC investigations. The ACC is accountable to a number of well-established external scrutiny mechanisms, including the:
- Commonwealth Ombudsman
 - ACC Board
 - Parliamentary Joint Committee on Law Enforcement
 - Inter-Governmental Committee on the ACC, chaired by the Commonwealth Minister for Justice and consisting of the Police Ministers from each state and territory
 - Australian Commission for Law Enforcement Integrity, and
 - Australian National Audit Office.
23. Ultimately, the ACC is also accountable to the courts where telecommunications evidence is presented and either rejected or admitted into evidence in court proceedings following scrutiny of its lawfulness and appropriateness.

⁷ Section 180 of the TIA Act.

⁸ See footnote 2.

UNCLASSIFIED

24. The ACC does not request, obtain or hold telecommunications data or seek to intercept or access telecommunications content for every investigation. Each request is carefully considered. The request must include the reason and must be related to the ACC's mandate in countering serious and organised crime.
25. The ACC has received no adverse recommendations from the Commonwealth Ombudsman over the past five years on its compliance with the TIA Act. The Ombudsman has remarked favourably on the strong mechanisms in place for ensuring compliance by the ACC. The ACC has a strong 'excellence in compliance' regime. The agency has a '*no training - no access*' policy, for TIA Act material. All staff who apply for warrants and/or have access to information obtained through warrants and/or authorisations must attend training on the provisions of the TIA Act on a regular basis.
26. Inspection by the Commonwealth Ombudsman is thorough and provides avenues for complaints and for addressing natural justice concerns as well as adoption of best practice for recording, using and communication of TIA Act material. The Ombudsman has an own motion power to inspect any administrative process of the ACC. The number of requests (intercept warrants and authorisations or requests for telecommunications data) made by the ACC are reported to Parliament in the Attorney-General's Annual Report on the TIA Act, which is publically available.
27. The ACC is of the view that the existing authorisation arrangements under the TIA Act establishes lawful access to telecommunications data and provides the appropriate balance between protection of privacy and the ability of the agency to conduct its investigations effectively. The agency accountability and oversight mechanisms provide assurance that the access and use of telecommunications material is in the public interest.

UNCLASSIFIED

Australian Law Reform Commission report

Recommendation 71.2

The Australian Government should initiate a review to consider whether the *Telecommunications Act 1997* (Cth) and the *Telecommunications (Interception and Access) Act 1979* (Cth) continue to be effective in light of technological developments (including technological convergence), changes in the structure of communication industries and changing community perceptions and expectations about communication technologies. In particular, the review should consider:

- (a) whether the Acts continue to regulate effectively communication technologies and the individuals and organisations that supply communication technologies and communication services;
- (b) how these two Acts interact with each other and with other legislation;
- (c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation;
- (d) the roles and functions of the various bodies currently involved in the regulation of the telecommunications industry, including the Australian Communications and Media Authority, the Attorney-General's Department, the Office of the Privacy Commissioner, the Telecommunications Industry Ombudsman, and Communications Alliance; and
- (e) whether the *Telecommunications (Interception and Access) Act* should be amended to provide for the role of a public interest monitor.

28. The ALRC, in its *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, made a series of recommendations. Recommendation 71.2, included in the terms of reference to this Inquiry, related to the *Telecommunications Act 1997* (Cth) and the TIA Act.

29. There have been significant changes to both the criminal and telecommunications environments since the drafting of the TIA Act. While the TIA Act originally contemplated the interception of traditional telephone lines, the array of communications methods and devices has expanded exponentially since that time. The criminal environment has also radically changed from one where the use of telecommunications was primarily to facilitate domestic criminal activities, to one where global criminal networks exploit communications technology to advance and disguise their multi-million dollar criminal enterprises. The change in technology and reach of communications necessitates an appropriately updated response which enables lawful interception of all communications consistent with the aims of the TIA Act in 1979, and allows for the lawful communication of relevant information to appropriate agencies, both Australian and international, balanced with appropriate oversight and privacy considerations.

30. The TIA Act, as it is currently drafted,⁹ restricts the powers for the ACC to effectively communicate lawfully intercepted information and telecommunications data with numerous domestic law

⁹ Refer to the limited scope of communication permitted under s67 and s68 of the TIA Act.

UNCLASSIFIED

enforcement, policy and regulatory agencies as well as international agencies. The ACC is supportive of recommendations made by the ALRC to amend the TIA Act as it relates to the disclosure of information where there is reason to suspect that unlawful activity has been, is being, or may be engaged in, and uses or discloses the personal information as a necessary part of its investigation of the matter or in reporting its concerns to relevant authorities.

31. The ACC supports recommendations to impose an obligation on all telecommunication service providers to assist law enforcement. The ACC also supports an extension of the Act to regulate ancillary service providers in addition to telecommunication service providers. The Act as currently drafted does not oblige ancillary service providers to supply decrypted information to law enforcement, or assist with decryption.
32. The TIA Act sets out no provisions compelling the retention of telecommunications data, which potentially jeopardises the effectiveness of law enforcement investigations and creates uncertainty as to what information will be available and when.
33. The ACC is not supportive of the introduction of a Public Interest Monitor. As outlined earlier in this submission, the ACC is subject to extensive accountability and oversight arrangements, and considers that there are sufficient safeguards and accountability mechanisms in place to obtain, protect and lawfully disclose information under the TIA Act.

UNCLASSIFIED

Inquiry into the potential reforms of Australia's National Security Legislation

Recommendations by the Parliamentary Joint Committee on Intelligence and Security

34. In 2012, the ACC provided a submission to the PJCIS regarding potential reforms to Australia's national security legislation, specifically the TIA Act. The PJCIS report made a number of recommendations relevant to the ACC and its use of the TIA Act:

- Inclusion of an objectives clause in the TIA Act which expresses the dual objectives of the legislation (protection of privacy and enabling interception and access)
- A mandatory data retention scheme (noting that the report left this matter for Government to decide)
- Review of information sharing provisions
- Development of a single warrant regime
- Industry assistance obligations and the requirement to assist law enforcement in decrypting communications
- Comprehensive revision of the TIA Act

35. The ACC considers it imperative that existing investigative capabilities are maintained under a revised TIA Act and that the administrative requirements and thresholds to seek access to telecommunications data and intercepted material are not increased.

36. The ACC is broadly supportive of the PJCIS recommendations relating to the inclusion of a specific objectives clause in the TIA Act, revised information sharing provisions, a single warrant regime, and the requirement for industry to assist law enforcement. The ACC's comments regarding each recommendation may be found at **Attachment A**.

ACC proposed reforms to the TIA Act

37. The ACC proposes a number of reforms to the TIA Act, as were outlined in its submission to the PJCIS, that would assist discovering, understanding and responding to serious and organised crime. The proposals included:

- Obligation imposed on telecommunications service providers to assist law enforcement, including with the decryption of communications
- The mandatory and uniform retention of telecommunications data
- Clarification regarding the use of TIA Act information for ACC purposes
- Revision of the TIA Act information sharing and destruction provisions

UNCLASSIFIED

38. The reforms sought by the ACC are to ensure the agency is best equipped to target serious and organised crime while at the same time maintaining a strong accountability framework where access to TIA Act material is only obtained through meeting serious offence thresholds and being appropriately authorised and externally reviewed.

Assistance from telecommunications service providers

39. There has been a significant change in the technological environment since the drafting of the TIA Act. Serious and organised criminal groups deliberately pursue means to prevent detection, using devices with complex security measures. The evolution of technology and the ability of serious and organised criminals to evade detection present a considerable challenge and risk for Australia.
40. The ACC is supportive of measures which require telecommunication service providers, including ancillary service providers, to assist law enforcement with accessing communications where authorised, including offences for not assisting with decrypting communications, as was recommended by the PJCIS.

Telecommunications data retention

41. Access to telecommunications data is a critical investigative tool for the ACC. A large number of serious crime investigations by law enforcement agencies are assisted by some form of telecommunications data. Such data generally enables agencies to establish the time, general location and subscriber details of those involved in telecommunications activity. It is particularly important at the early stages of an investigation where it is used to identify and obtain basic information about persons of interest, and to provide key evidence in support of warrant applications.
42. Telecommunications data provides an alternative source of information that allows agencies to understand the threat environment and the individuals involved, without requiring interception of the device concerned or access to the content of the communication. It is also used to discount innocent parties from investigations in a manner much less intrusive than using full telecommunications interception.
43. Retention of telecommunications data by service providers in Australia is variable and subject to the storage capacity of the service provider, the volume of telecommunications data that is being inputted and the type of telecommunications data being collected. Consequently, some service providers store the same type of telecommunications data for longer periods than others, and some less. The absence of a national standard results in uncertainty for law enforcement and can jeopardise the outcome of operations.
44. These differences in retention periods create difficulties for the ACC in its ability to undertake investigations into federally relevant criminal activity, as valuable telecommunications data is not always available when needed. When it comes to conducting ACC investigations on long-term federally relevant criminal activity, access to retrospective telecommunications data is critical for the ACC to understand the scope and nature of the threat.

UNCLASSIFIED

Case study 1 – Use of TIA Act data to protect innocent parties

An ACC money laundering project identified an active money laundering syndicate controlled from another country. The Australian member of this syndicate was told by his overseas controller to contact an Australian mobile number to collect criminal proceeds. However, the number provided by the overseas controller was incorrect. The Australian syndicate member made contact with the Australian phone number, and on initial examination the communication appear to be suspicious.

A check on the subscriber of the Australian phone and collection of call associated data of the number provided by the overseas controller were conducted. The subscriber check showed that the Australian phone was subscribed to a real person with legitimate details who was not involved with drug distribution or money laundering suspects.

Based on this information, the ACC could identify that the user of this service was not likely to be involved in criminality and they were excluded from further enquiries in the investigation.

45. The ACC is requesting that telecommunications data be retained uniformly across the telecommunications industry for a minimum period of two years. This two year period would assist with protracted ACC investigations, which are currently authorised by the Board for up to three year periods. The concept of telecommunications data retention would need to be sufficiently flexible to ensure data from new, emerging or unknown future technologies that can assist investigations is also able to be retained. Without this flexibility, technology will continue to outpace the legal framework under which the ACC and its partner national security and law enforcement agencies operate.
46. The ACC is not supportive of amendment of the threshold for access to telecommunications data consistent with the Attorney-General's Department submission to the Senate Standing Committee on Legal and Constitutional Affairs inquiry into the *Telecommunications Amendment (Get a Warrant) Bill 2013*. Currently, such data is accessed following an internal application and authorisation process. The requirement for a warrant to be obtained for access to all data (not only content) will result in a major impact on the investigative capability of the ACC, and will significantly impinge on the resources available to conduct operational activities. Applications for telecommunications warrants rely on evidence obtained for telecommunications data, such as the subscriber name and evidence that the service is active. An inability to access what is threshold telecommunications data without a warrant will significantly impede ACC investigations and create consequential difficulties for ACC when applying for telecommunication interception warrants. ACC and its law enforcement partners will only remain effective in their efforts against serious and organised crime while they remain agile and prompt in response.
47. The interception of communications is an expensive and finite resource. Having access to telecommunications data means that interception can be applied selectively and most effectively in the interests of minimising intrusion and to optimise use of scarce resources.

UNCLASSIFIED

Case study 2 – EFTPOS skimming and telecommunications data retention

Between March and December 2010, the ACC led a coordinated task force targeting the activities of a transnational network of high threat, serious and organised criminal groups conducting EFTPOS card skimming activities across several jurisdictions. During the investigation the ACC arrested a key syndicate member who had acted as the principal offshore organiser of the syndicate prior to arrival in Australia.

While this person was known to the ACC under his real name, and was refused an Australia visa, he successfully obtained travel documents, including an Australian visa, in a false name.

While in Australia, he used this false identity to procure mobile telephones and communication services, which he used to coordinate the supply and installation of EFTPOS card skimming devices. The short telecommunications data retention period of his chosen telecommunications provider meant that it was not possible to retrospectively investigate and assess the extent of his criminal activity in Australia once his false identity was identified.

The use of false or stolen identities by persons of interest in any investigation may not be apparent at the commencement of a new project, and may only be recognised after lengthy intelligence collection, other warranted activity, and ACC examinations. This process can sometimes take years to undertake.

Short telecommunications data retention periods hinder, or even preclude, further retrospective intelligence collection and investigative action into these newly discovered false identities.

Case Study 3 – Illicit funds and telecommunications data retention

In February 2013, the ACC received information indicating Person A was processing illicit funds and potentially involved in money laundering. Enquiries revealed that Person A had not previously come to law enforcement attention.

In conducting a money laundering investigation, the ACC sought access to telecommunications data (subscriber details, not content) for Person A's mobile telephone number, which revealed that the phone account in fact belonged to Person B but used by Person A. Person B was suspected of arranging the importation and distribution of large quantities of illicit drugs. The ACC was then able to analyse relevant information based on the subscriber check and identify a relationship between Person A and Person B. The ACC assessed that illicit funds being managed by Person A were likely derived from illicit drug sales conducted by Person B. Intelligence regarding this matter was referred to a Task Force for further investigation.

Without the ability to conduct a subscriber check at the initial stage of the investigation, it is unlikely the ACC would have been able to detect and further investigate the relationship between Person A and Person B.

Use of TIA Act material for ACC functions

48. As noted earlier, a fundamental precondition to ACC applying for access to TIA Act material is that it is conducting an investigation of specified offences, and that this may occur under ACC Board

UNCLASSIFIED

authorised investigations or intelligence operations (which may include an investigation component). Intelligence processes (focussed collection, analysis and reporting) are routinely used to identify criminal targets and determine whether offences have been committed. The ability to acquire such information from lawfully intercepted communications and data obtained from service providers is critical for the intelligence component of an investigation. Equally, such intelligence processes can be applied to scope out the nature of the serious crime environment to enable a wider range of policy (prevention) and law enforcement (disruption) responses.

49. Currently, the ACC can seek a warrant under the TIA Act in connection with a Board authorised Special Investigation.¹⁰ However, in applying for a warrant in support of an investigation component of a Board authorised Special Operation, this qualification is not available, and the application must meet other tests of what constitutes a serious offence in the Act.¹¹ The ACC requests that there be a standardised approach to applications for TIA Act warrants across Special Investigations and Special Operations in support of the ACC's functions.

Revised TIA Act information sharing provisions

50. The ACC is unable to share lawfully intercepted information and other information obtained under the TIA Act, such as telecommunications data, with other agencies beyond investigation of offences and other purposes of the specified agency. Currently the ACC can only communicate lawfully intercepted information for the investigation of offences by the agencies listed in s68 of the Act (largely police and integrity bodies). This has proved problematic for example, where the ACC has wanted to share information regarding criminal activity with agencies such as ASIC, AUSTRAC, the ATO and the Australian Border and Customs Protection Service.
51. The PJCIS report recommends that the TIA Act be reviewed to ensure information is shared where necessary to facilitate the functions of the ACC in combating serious and organised crime, or threats to national security. The ALRC report contained a similar recommendation. The ACC supports these recommendations, but also suggests the inclusion of additional policy, regulatory, and intelligence agencies as potential TIA Act material recipients where appropriate for prevention and disruption of serious and organised crime, as previously outlined.

Case study 4 – Information sharing and drug offences

In an ACC operation, the Commission lawfully collected intercepted information linked to a principal person of interest.

The intelligence developed from this information indicated that the person of interest was involved in serious offences against the Customs Act 1901 (Customs Act). The ACC sought to share the information with the Australian Customs and Border Protection Service (Customs) in order for them to take appropriate action, as the ACC was no longer continuing the investigation.

The ACC was unable to communicate the lawfully intercepted information to Customs under either s67 as it was not be for a permitted purpose, or under s68 as Customs is not an intercept

¹⁰ Taking advantage of the qualification in s5D(1)(f) of the TIA Act in meeting the precondition of serious offences.

¹¹ Section 5D TIA Act.

UNCLASSIFIED

agency. This inability to pass on the information frustrated the efforts of law enforcement to effectively address serious and organised crime.

Case study 5 – Information sharing and freezing orders

An ACC task force investigated the suspected narcotics supply, tax evasion and money laundering activities of an Australian based criminal syndicate. The syndicate was suspected to have laundered more than AUD 30 million in cash, including approximately AUD 25 million which was sent offshore.

During the course of the investigation, lawfully intercepted information collected by the ACC identified an offshore property development being undertaken by the syndicate. Due to restrictions on the disclosure of the intercepted information, the ACC was unable to advise the ATO of the existence of the offshore development.

Freezing orders were obtained in relation to taxation assessments of the principals of the syndicate. Although this was enough to cover the Australian assets of the syndicate, the potentially significant offshore assets were not sought by the ATO because they did not have access to lawfully intercepted information obtained by the ACC.

Case study 6 – Information sharing and money laundering offences

An ACC task force investigated the money laundering activity of an Alternate Money Remittance (AMR) business in Sydney. During the course of the investigation, lawfully intercepted information obtained by the ACC showed clearly that the operators of the AMR business were reporting false information to AUSTRAC, for example using false names for transaction reports, and requesting customers provide false identities to hide the true customer's details.

The ACC was unable to refer the lawfully intercepted information to AUSTRAC due to the restrictions under the current TIA Act, meaning that the ultimate referral to AUSTRAC contained considerably less information regarding the false reporting of the AMR than the ACC held. As a result, AUSTRAC had to rely on technical breaches of the Anti-Money Laundering/Counter-Terrorism Finance Act (AML/CTF), such as a failure to meet reporting requirements, to undertake enforcement action, rather than the information that was held by the ACC which showed clear breaches of the AML/CTF Act (for fraud).

Case study 7 – Information sharing and money laundering offences

As part of a task force, the ACC obtained lawfully intercepted information which revealed significant breaches of the *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) reporting requirements by an Alternate Money Remittance (AMR) business. In particular, the intercepted material showed that a money launderer under investigation was providing cash obtained from drug dealers to the principal of an AMR. Those funds were not

UNCLASSIFIED

reported by the AMR as required by the legislation. Equally as important, the funds were then provided to other customers of the remitter.

The ACC report to AUSTRAC was unable to contain specific details which would have been of significant assistance to AUSTRAC and would have permitted enforcement action due to the current restrictions in the TIA Act relating to the sharing of TIA Act material with non-intercept agencies.

Redrafting of the TIA Act

52. The ACC supports redrafting of the TIA Act to remove legislative ambiguity, to be technology neutral, to standardise compliance processes in common with surveillance device legislation¹² (for example tests for warrants, restrictions on use, communication and destruction), and to restore the original spectrum of interception as was intended by the TIA Act when enacted in 1979. The ACC considers that reform of the TIA Act is required in order for the legislation to effectively regulate communication technologies and facilitate the investigation of serious criminal activity.

ACC Board Position

53. ACC Board members are supportive of the ACC's proposed amendments to the TIA Act. The Board is particularly supportive of the introduction of a standard mandatory data retention scheme. At its meeting in November 2013, the Board recognised the importance of the retention of telecommunications data to law enforcement and noted its support for a mandatory telecommunications data retention regime.

Conclusion

54. The ACC supports amendment of the TIA Act that will facilitate the detection, disruption and deterrence of serious and organised crime and enables the Agency to lawfully respond to the contemporary and emerging threats impacting the Australian community. It considers that the existing application thresholds and compliance and oversight mechanisms are sufficiently robust and stringent and uphold the important balance of maintaining and supporting the privacy of individuals while at the same time enabling the investigation of serious criminal activity.

55. The ACC welcomes the opportunity to present further information to the Committee at an oral hearing.

¹² Frequently, the ACC makes applications under the TIA Act and Surveillance Devices Act at the same time, yet the legislation has different application and compliance requirements.

UNCLASSIFIED

Attachment A – ACC response to PJCIS recommendations

RECOMMENDATION	ACC RESPONSE
<p>Recommendation 1</p> <p>The Committee recommends the inclusion of an objectives clause within the <i>Telecommunications (Interception and Access) Act 1979</i>, which:</p> <ul style="list-style-type: none">expresses the dual objectives of the legislation –<ul style="list-style-type: none">to protect the privacy of communications;to enable interception and access to communications in order to investigate serious crime and threats to national security; andaccords with the privacy principles contained in the <i>Privacy Act 1988</i>.	<p>An objectives clause within the TIA Act would support the dual purposes of the legislation – the protection of privacy and to enable interception by law enforcement agencies.</p>
<p>Recommendation 2</p> <p>The Committee recommends the Attorney-General’s Department undertake an examination of the proportionality tests within the <i>Telecommunications (Interception and Access) Act 1979</i> (TIA Act). Factors to be considered in the proportionality tests include the:</p> <ul style="list-style-type: none">privacy impacts of proposed investigative activity;public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; andavailability and effectiveness of less privacy intrusive investigative techniques. <p>The Committee further recommends that the examination of the proportionality tests also consider the appropriateness of applying a consistent proportionality test across the interception, stored communications and access to telecommunications data powers in the TIA Act.</p>	<p>The inherent differences between interception, stored communications and telecommunications data would make the application of a consistent proportionality test potentially difficult to implement. The important distinction between content and data also needs to be considered and maintained. The ACC has previously strongly opposed consideration of applying a warrant regime for telecommunications data. A consistent proportionality test across content and data would have adverse consequences on the investigative ability of law enforcement.</p> <p>In addition, the application of a proportionality test on a single warrant regime outlined in Recommendation 10 needs to consider instances where only specific aspects of a warrant (such as stored data) are sought, and not the full extent of powers under a single warrant regime.</p>

UNCLASSIFIED

<p>Recommendation 3</p> <p>The Committee recommends that the Attorney-General's Department examine the <i>Telecommunications (Interception and Access) Act 1979</i> with a view to revising the reporting requirements to ensure that the information provided assists in the evaluation of whether the privacy intrusion was proportionate to the public outcome sought.</p>	<p>The ACC already has a high degree of oversight and governance arrangements that support independent scrutiny of telecommunications interception powers utilised by the ACC. The ACC supports public accountability of the powers it accesses and deploys. However, as a criminal intelligence agency, the ACC also stresses there is a need to maintain confidentiality of the sources and methods used to detect, disrupt and investigate organised criminal activities.</p>
<p>Recommendation 4</p> <p>The Committee recommends that the Attorney-General's Department undertake a review of the oversight arrangements to consider the appropriate organisation or agency to ensure effective accountability under the <i>Telecommunications (Interception and Access) Act 1979</i>.</p> <p>Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.</p> <p>The Committee also recommends the Attorney-General's Department consult with state and territory ministers prior to progressing any proposed reforms to ensure jurisdictional considerations are addressed.</p>	<p>As outlined in the ACC's submission to the PJCIS and this submission, the ACC has robust oversight and accountability arrangements and does not consider that additional supervision is required.</p>
<p>Recommendation 5</p> <p>The Committee recommends that the Attorney-General's Department review the threshold for access to telecommunications data. This review should focus on reducing the number of agencies able to access telecommunications data by using gravity of conduct which may be investigated utilising telecommunications data as the threshold on which access is allowed.</p>	<p>Any change in the threshold for access to telecommunications data should ensure the ACC is not hampered from carrying out its functions under the <i>Australian Crime Commission Act 2002</i> to discover, understand and respond to serious and organised crime. As the TIA Act warrant application process does now, application for data should recognise the qualification of ACC investigations (and also intelligence operations).</p>

UNCLASSIFIED

Recommendation 6

The Committee recommends that the Attorney-General's Department examine the standardisation of thresholds for accessing the content of communications. The standardisation should consider the:

- privacy impact of the threshold;
- proportionality of the investigative need and the privacy intrusion;
- gravity of the conduct to be investigated by these investigative means;
- scope of the offences included and excluded by a particular threshold; and
- impact on law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.

The ACC supports examination of the standardisation of thresholds for accessing the content of communication, where outcomes of the examination will not restrict investigative capabilities. The ACC is supportive of warrant thresholds that facilitate the ACC in conducting its functions under the *Australian Crime Commission Act 2002*, including ACC Special Operations and Special Investigations.

UNCLASSIFIED

Recommendation 7

The Committee recommends that interception be conducted on the basis of specific attributes of communications. The Committee further recommends that the Government model 'attribute based interception' on the existing named person interception warrants, which includes:

- the ability for the issuing authority to set parameters around the variation of attributes for interception;
- the ability for interception agencies to vary the attributes for interception; and reporting on the attributes added for interception by an authorised officer within an interception agency.

In addition to Parliamentary oversight, the Committee recommends that attribute based interception be subject to the following safeguards and accountability measures:

- attribute based interception is only authorised when an issuing authority or approved officer is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;
- oversight of attribute based interception by the ombudsmen and Inspector-General of Intelligence and Security; and
- reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of attribute based interception.

An attribute based model provides a number of advantages in being able to detect serious and organised criminal activity which is not available under named person warrants.

With technological changes, the utilisation of attributes will likely be essential to protect Australians from serious and organised criminal activities. This will allow the ability of law enforcement to prevent criminal acts where only an attribute is known given that technology could render names irrelevant in some instances. This fits in with the need for the TI Act to be technology neutral.

Ultimately, an attribute based model would enable the ACC to better detect criminal activity conducted by one or more individuals, while ensuring operational flexibility to improve targeting of suspects and avoiding innocent parties. The benefit of this approach is to provide targeted and measured interception, improving privacy outcomes.

UNCLASSIFIED

<p>Recommendation 8</p> <p>The Committee recommends that the Attorney-General's Department review the information sharing provisions of the <i>Telecommunications (Interception and Access) Act 1979</i> to ensure:</p> <ul style="list-style-type: none">• protection of the security and privacy of intercepted information; and• sharing of information where necessary to facilitate investigation of serious crime or threats to national security.	<p>The ACC notes that information sharing is a key requirement for delivering relevant, accurate and timely intelligence.</p> <p>The case studies outlined in the submission demonstrate instances where the inability to share information has resulted in negative outcomes in the fight against serious and organised crime.</p> <p>It is important that any TIA Act material sharing regime considers not only the benefits derived from enforcement of law and prosecutorial outcomes – domestically and internationally - but also enhancements to government policy and regulation and the sharing of intelligence under the ACC Act.</p>
<p>Recommendation 9</p> <p>The Committee recommends that the <i>Telecommunications (Interception and Access) Act 1979</i> be amended to remove legislative duplication.</p>	<p>The ACC supports simplification of the TIA Act as was outlined in its submission to the PJCIS.</p>

UNCLASSIFIED

<p>Recommendation 10</p> <p>The Committee recommends that the telecommunications interception warrant provisions in the <i>Telecommunications (Interception and Access) Act 1979</i> be revised to develop a single interception warrant regime. The Committee recommends the single warrant regime include the following features:</p> <ul style="list-style-type: none">• a single threshold for law enforcement agencies to access communications based on serious criminal offences;• removal of the concept of stored communications to provide uniform protection to the content of communications; and• maintenance of the existing ability to apply for telephone applications for warrants, emergency warrants and ability to enter premises. <p>The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:</p> <ul style="list-style-type: none">• interception is only authorised when an issuing authority is satisfied the facts and grounds indicate that interception is proportionate to the offence or national security threat being investigated;• rigorous oversight of interception by the ombudsmen and Inspector-General of Intelligence and Security;• reporting by the law enforcement and security agencies to their respective Ministers on the effectiveness of interception; and• Parliamentary oversight of the use of interception.	<p>A single warrant regime will reduce complexity in warrant provisioning and the associated compliance processes, increasing administrative efficiency and operational capability.</p> <p>However, support for the recommendation is also dependent upon a suitable threshold being identified which continues to provide access to powers necessary to undertake investigations into serious and organised crime. This issue is not resolved in the PJCIS report. A threshold which facilitates the ACC in conducting its functions under the <i>Australian Crime Commission Act 2002</i> (Cth), including ACC Special Operations and Special Investigations, would be appropriate.</p>
<p>Recommendation 11</p> <p>The Committee recommends that the Government review the application of the interception-related industry assistance obligations contained in the <i>Telecommunications (Interception and Access) Act 1979</i> and <i>Telecommunications Act 1997</i>.</p>	<p>The ACC supports a review of industry assistance obligations. Assistance from telecommunication service providers is a necessary part of lawful telecommunications interception. Increasingly important is capturing ancillary service providers which are deploying new and complex telecommunication services currently beyond the remit of the TIA Act.</p>

UNCLASSIFIED

<p>Recommendation 12</p> <p>The Committee recommends the Government consider expanding the regulatory enforcement options available to the Australian Communications and Media Authority to include a range of enforcement mechanisms in order to provide tools proportionate to the conduct being regulated.</p>	<p>No comment.</p>
<p>Recommendation 13</p> <p>The Committee recommends that the <i>Telecommunications (Interception and Access) Act 1979</i> be amended to include provisions which clearly express the scope of the obligations which require telecommunication service providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.</p>	<p>As outlined in this submission, the ACC supports inclusion of provisions which require telecommunication service providers and ancillary providers to provide assistance to law enforcement.</p>
<p>Recommendation 14</p> <p>The Committee recommends that the <i>Telecommunications (Interception and Access) Act 1979</i> and the <i>Telecommunications Act 1997</i> be amended to make it clear beyond doubt that the existing obligations of the telecommunications interception regime apply to all providers (including ancillary service providers) of telecommunications services accessed within Australia. As with the existing cost sharing arrangements, this should be done on a no-profit and no-loss basis for ancillary service providers.</p>	<p>As outlined in this submission, the ACC supports inclusion of provisions which require telecommunication service providers and ancillary providers to provide assistance to law enforcement.</p>
<p>Recommendation 15</p> <p>The Committee recommends that the Government should develop the implementation model on the basis of a uniformity of obligations while acknowledging that the creation of exemptions on the basis of practicability and affordability may be justifiable in particular cases. However, in all such cases the burden should lie on the industry participants to demonstrate why they should receive these exemptions.</p>	<p>The ACC recognises that in some cases exemptions are necessary to ensure the viability of legitimate businesses. The ACC would see merit in ensuring that where an exemption exists, there is an obligation by exempted businesses to provide reasonable and necessary support to law enforcement agencies to resolve interception challenges.</p>

UNCLASSIFIED

<p>Recommendation 16</p> <p>The Committee recommends that, should the Government decide to develop an offence for failure to assist in decrypting communications, the offence be developed in consultation with the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. It is important that any such offence be expressed with sufficient specificity so that telecommunications providers are left with a clear understanding of their obligations.</p>	<p>As outlined in this submission, the ACC supports inclusion of provisions which require telecommunication service providers and ancillary providers to provide assistance to law enforcement.</p>
<p>Recommendation 17</p> <p>The Committee recommends that, if the Government decides to develop timelines for telecommunications industry assistance for law enforcement and national security agencies, the timelines should be developed in consultation with the investigative agencies, the telecommunications industry, the Department of Broadband Communications and the Digital Economy, and the Australian Communications and Media Authority. The Committee further recommends that, if the Government decides to develop mandatory timelines, the cost to the telecommunications industry must be considered.</p>	<p>As outlined in this submission, the ACC supports inclusion of provisions which require telecommunication service providers and ancillary providers to provide assistance to law enforcement.</p>

UNCLASSIFIED

Recommendation 18

The Committee recommends that the *Telecommunications (Interception and Access) Act 1979* (TIA Act) be comprehensively revised with the objective of designing an interception regime which is underpinned by the following:

- clear protection for the privacy of communications;
- provisions which are technology neutral;
- maintenance of investigative capabilities, supported by provisions for appropriate use of intercepted information for lawful purposes;
- clearly articulated and enforceable industry obligations; and
- robust oversight and accountability which supports administrative efficiency.

The Committee further recommends that the revision of the TIA Act be undertaken in consultation with interested stakeholders, including privacy advocates and practitioners, oversight bodies, telecommunications providers, law enforcement and security agencies.

The Committee also recommends that a revised TIA Act should be released as an exposure draft for public consultation. In addition, the Government should expressly seek the views of key agencies, including the:

- Independent National Security Legislation Monitor;
- Australian Information Commissioner;
- ombudsmen and the Inspector-General of Intelligence and Security.

In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.

As outlined in this submission, comprehensive revision of the TIA Act should ensure the maintenance of investigative capability. Any reform should also aim to ensure legislation is sufficiently flexible to apply to new technologies as they evolve.

UNCLASSIFIED

Recommendation 19

The Committee recommends that the Government amend the *Telecommunications Act 1997* to create a telecommunications security framework that will provide:

- a telecommunications industry-wide obligation to protect infrastructure and the information held on it or passing across it from unauthorised interference;
- a requirement for industry to provide the Government with information to assist in the assessment of national security risks to telecommunications infrastructure; and
- powers of direction and a penalty regime to encourage compliance.

The Committee further recommends that the Government, through a Regulation Impact Statement, address:

- the interaction of the proposed regime with existing legal obligations imposed upon corporations;
- the compatibility of the proposed regime with existing corporate governance where a provider's activities might be driven by decisions made outside of Australia;
- consideration of an indemnity to civil action for service providers who have acted in good faith under the requirements of the proposed framework; and
- impacts on competition in the market-place, including:
 - the potential for proposed requirements to create a barrier to entry for lower cost providers;
 - the possible elimination of existing lower cost providers from the market, resulting in decreased market competition on pricing; and
 - any other relevant effects.

No comment.

UNCLASSIFIED

<p>Recommendation 20</p> <p>The Committee recommends that the definition of computer in the <i>Australian Security Intelligence Organisation Act 1979</i> be amended by adding to the existing definition the words “and includes multiple computers operating in a network”.</p> <p>The Committee further recommends that the warrant provisions of the ASIO Act be amended by stipulating that a warrant authorising access to a computer may extend to all computers at a nominated location and all computers directly associated with a nominated person in relation to a security matter of interest.</p>	No comment.
<p>Recommendation 21</p> <p>The Committee recommends that the Government give further consideration to amending the warrant provisions in the <i>Australian Security Intelligence Organisation Act 1979</i> to enable the disruption of a target computer for the purposes of executing a computer access warrant but only to the extent of a demonstrated necessity.</p> <p>The Committee further recommends that the Government pay particular regard to the concerns raised by the Inspector-General of Intelligence and Security.</p>	No comment.
<p>Recommendation 22</p> <p>The Committee recommends that the Government amend the warrant provisions of the <i>Australian Security Intelligence Organisation Act 1979</i> to allow ASIO to access third party computers and communications in transit to access a target computer under a computer access warrant, subject to appropriate safeguards and accountability mechanisms, and consistent with existing provisions under the <i>Telecommunications (Interception and Access) Act 1979</i>.</p>	No comment.
<p>Recommendation 23</p> <p>The Committee recommends the Government amend the warrant provisions of the <i>Australian Security Intelligence Organisation Act 1979</i> to promote consistency by allowing the Attorney-General to vary all types of ASIO Act warrants.</p>	No comment.

UNCLASSIFIED

Recommendation 24 Subject to the recommendation on renewal of warrants, the Committee recommends that the maximum duration of <i>Australian Security Intelligence Organisation Act 1979</i> search warrants not be increased.	No comment.
Recommendation 25 The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to allow the Attorney-General to renew warrants.	No comment.
Recommendation 26 The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to modernise the Act's provisions regarding secondment arrangements.	No comment.
Recommendation 27 The Committee recommends that the <i>Intelligence Services Act 2001</i> be amended to clarify the authority of the Defence Imagery and Geospatial Organisation to undertake its geospatial and imagery functions.	No comment.
Recommendation 28 The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to create an authorised intelligence operations scheme, subject to similar safeguards and accountability arrangements as apply to the Australian Federal Police controlled operations regime under the <i>Crimes Act 1914</i> .	No comment.

UNCLASSIFIED

Recommendation 29 The Committee recommends that should the Government proceed with amending the <i>Australian Security Intelligence Organisation Act 1979</i> to establish a named person warrant, further consideration be given to the factors that would enable ASIO to request a single warrant specifying multiple powers against a single target. The thresholds, duration, accountability mechanisms and oversight arrangements for such warrants should not be lower than other existing ASIO warrants.	No comment.
Recommendation 30 The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to modernise the warrant provisions to align the surveillance device provisions with the <i>Surveillance Devices Act 2004</i> , in particular by optical devices.	No comment.
Recommendation 31 The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> not be amended to enable person searches to be undertaken independently of a premises search.	No comment.
Recommendation 32 The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to establish classes of persons able to execute warrants.	No comment.
Recommendation 33 The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to formalise ASIO's capacity to cooperate with private sector entities.	No comment.
Recommendation 34 The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended so that ASIO may refer breaches of section 92 to law enforcement for investigation.	No comment.

UNCLASSIFIED

<p>Recommendation 35</p> <p>The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to clarify that the incidental power in the search and computer access warrant provisions includes entry to a third party's premises for the purposes of executing those warrants. However, the Committee is of the view that whatever amendments are made to facilitate this power should acknowledge the exceptional nature and very limited circumstances in which the power should be exercised.</p>	<p>No comment.</p>
<p>Recommendation 36</p> <p>The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to clarify that reasonable force can be used at any time for the purposes of executing the warrant, not just on entry, and may only be used against property and not persons.</p>	<p>No comment.</p>
<p>Recommendation 37</p> <p>The Committee recommends that the <i>Australian Security Intelligence Organisation Act 1979</i> be amended to introduce an evidentiary certificate regime to protect the identity of officers and sources. The Committee also recommends that similar protections be extended to ASIO in order to protect from disclosure in open court its sensitive operational capabilities, analogous to the provisions of the <i>Telecommunications (Interception and Access) Act 1979</i> and the protections contained in the counter terrorism provisions in the Commonwealth Criminal code. The Committee further recommends that the Attorney-General give consideration to making uniform across Commonwealth legislation provisions for the protection of certain sensitive operational capabilities from disclosure in open court.</p>	<p>No comment.</p>
<p>Recommendation 38</p> <p>The Committee recommends that the <i>Intelligence Services Act 2001</i> be amended to add a new ministerial authorisation ground where the Minister is satisfied that a person is, or is likely to be, involved in intelligence or counter-intelligence activities in circumstances where such an investigation would not currently be within the operational authority of the agency concerned.</p>	<p>No comment.</p>

UNCLASSIFIED

<p>Recommendation 39</p> <p>The Committee recommends that where ASIO and an <i>Intelligence Services Act 2001</i> agency are engaged in a cooperative intelligence operation a common standard based on the standards prescribed in the <i>Australian Security Intelligence Organisation Act 1979</i> should apply for the authorisation of intrusive activities involving the collection of intelligence on an Australian person.</p>	<p>No comment.</p>
<p>Recommendation 40</p> <p>The Committee recommends that the <i>Intelligence Services Act 2001</i> be amended to enable ASIS to provide training in self-defence and the use of weapons to a person cooperating with ASIS.</p>	<p>No comment.</p>
<p>Recommendation 41</p> <p>The Committee recommends that the draft amendments to the <i>Australian Security Intelligence Organisation Act 1979</i> and the <i>Intelligence Services Act 2001</i>, necessary to give effect to the Committee's recommendations, should be released as an exposure draft for public consultation. The Government should expressly seek the views of key stakeholders, including the Independent National Security Legislation Monitor and Inspector-General of Intelligence and Security.</p> <p>In addition, the Committee recommends the Government ensure that the draft legislation be subject to Parliamentary committee scrutiny.</p>	<p>No comment.</p>

UNCLASSIFIED

Recommendation 42

There is a diversity of views within the Committee as to whether there should be a mandatory data retention regime. This is ultimately a decision for Government. If the Government is persuaded that a mandatory data retention regime should proceed, the Committee recommends that the Government publish an exposure draft of any legislation and refer it to the Parliamentary Joint Committee on Intelligence and Security for examination. Any draft legislation should include the following features:

- any mandatory data retention regime should apply only to metadata and exclude content;
- the controls on access to communications data remain the same as under the current regime;
- internet browsing data should be explicitly excluded;
- where information includes content that cannot be separated from data, the information should be treated as content and therefore a warrant would be required for lawful access;
- the data should be stored securely by making encryption mandatory;
- save for existing provisions enabling agencies to retain data for a longer period of time, data retained under a new regime should be for no more than two years;
- the costs incurred by providers should be reimbursed by the Government;
- a robust, mandatory data breach notification scheme;
- an independent audit function be established within an appropriate agency to ensure that communications content is not stored by telecommunications service providers; and
- oversight of agencies' access to telecommunications data by the ombudsmen and the Inspector-General of Intelligence and Security.

As outlined in this submission, and the ACC's submission to the PJCIS, the ACC considers that a mandatory data retention regime is required to prevent a decline in investigative capability.

UNCLASSIFIED

Recommendation 43

The Committee recommends that, if the Government is persuaded that a mandatory data retention regime should proceed:

- there should be a mechanism for oversight of the scheme by the Parliamentary Joint Committee on Intelligence and Security;
- there should be an annual report on the operation of this scheme presented to Parliament; and
- the effectiveness of the regime be reviewed by the Parliamentary Joint Committee on Intelligence and Security three years after its commencement.

As outlined in this submission, and the ACC's submission to the PJCIS, the ACC considers that a mandatory data retention regime is required to prevent a decline in investigative capability. Should such a scheme be implemented, the ACC supports the oversight mechanisms suggested by the PJCIS.

