CORRUPTION AND CRIME COMMISSION

INQUIRY INTO COMPREHENSIVE REVISION OF THE *TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979*

SUBMISSION TO THE SENATE LEGAL AND CONSTITUTIONAL AFFAIRS REFERENCES COMMITTEE

FEBRUARY 2014

TABLE OF CONTENTS

INTRODUCTION

The Corruption and Crime Commission of Western Australia ("the Commission") was established on 1 January 2004 to "combat and reduce the incidence of organised crime; [and] to reduce the incidence of misconduct in the public service". In order to perform these functions significant powers have been afforded, including the authority to apply for telecommunications interception warrants issued under the *Telecommunications (Interception and Access) Act 1979* (Cth) ("TIA Act"). The Commission is a declared Agency under the TIA Act for the purposes of obtaining interception warrants and operates equipment to facilitate the lawful interception of communications by virtue of such warrants.

Lawful interception and access to telecommunications data offer an effective investigative instrument that supports and complements Commission operations and investigations. The Commission supports the primary objective of the current legislation, which seeks to protect the privacy of individuals who use the Australian telecommunications system, understanding the need for this to be balanced against Australia's law enforcement and national security interests.

The Commission's use of telecommunications interception is deployed under warrant and only to support investigations of serious offences. The Commission's access to telecommunications data is used exclusively to support investigations into serious misconduct and where it is reasonably necessary for the enforcement of the criminal law.

Advancements in communications technologies and methods since 1979 have created a complex and dynamic telecommunications landscape which has driven the need for reform to the current TIA Act. The Commission supports potential reforms of the TIA Act having reviewed the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, and the recommendations relating to the TIA Act from the Parliamentary Joint Committee on Intelligence and Security *Inquiry into the potential reforms of Australia's National Security Legislation* report.

The Commission welcomes the opportunity to make a submission to the Senate Legal and Constitutional Affairs Committee ("the Committee") concerning its inquiry into comprehensive revision of the TIA Act. In August 2012, the Commission made a submission to the Parliamentary Joint Committee on Intelligence and Security ("PJCIS") in relation to its inquiry into potential reforms of National Security Legislation. That submission, which comments on a number of issues relevant to this inquiry, is attached at **Appendix 1** for the information of the Committee.

SCOPE OF SUBMISSION

The Senate inquiry is seeking to review the TIA Act, with regard to:

(a) the recommendations of the Australian Law Reform Commission ("ALRC") *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2; and

(b) recommendations relating to the TIA Act from the PJCIS *Inquiry into the potential reforms of Australia's National Security Legislation* report, dated May 2013.

The Commission's submission seeks to directly address the ALRC recommendation 71.2 and the PJCIS report recommendations in Parts A and B respectively. This submission also comments on other key issues that directly affect the agency relating to its powers and functions under the TIA Act in Part C.

RESPONSE TO PART A

Comprehensive revision of the *Telecommunications (Interception and Access) Act 1979*, with regard to the recommendations of the Australian Law Reform Commission *For Your Information: Australian Privacy Law and Practice* report, dated May 2008, particularly recommendation 71.2.

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 communications 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;

The Commission considers that reform is required to effectively regulate communication technologies and the individuals and organisations that supply communication technologies and communication services.

The Commission's comment is limited to the lawful assistance required for Commission investigations. The Commission considers that the provisions under section 313 of the *Telecommunications Act 1997* for law enforcement are vital where assistance is not clearly defined by the TIA Act.

The Commission considers that there are regulatory changes required with regards to assisting law enforcement agencies where technology has produced new forms and methods of communications, particularly at the application service level. The Commission has detailed its views within this submission under Part B - Recommendations 11, 13, 14, and 15.

In general, the Commission maintains strong working relationships with telecommunication carriers and carriage service providers ("CSPs") and recognises that generally the assistance it receives for its investigations is quite good. On occasion, however, the Commission has encountered difficulties acquiring assistance from particular providers. In these cases the Commission considers that further regulatory options should be available to the Australian Communications and Media Authority ("ACMA") or the Attorney-General's Department. Further specific comment regarding industry compliance

considerations for regulatory reform is contained within this submission under Part B - Recommendations 12, 16 and 17.

(b) how these two Acts interact with each other and with other legislation;

The ARLC report concluded that the *Telecommunications Act 1997* and the *Privacy Act* should continue to regulate privacy in the telecommunications industry. The Commission has reviewed these findings and concurs. The Commission further considers that the regulatory arrangements and offence provisions within the TIA Act strengthen privacy within the telecommunications industry.

The Commission considers the designation of serious offences under section 5D within the TIA Act is overly complex. The Commission recommends that the TIA Act should interact with other legislation regarding the threshold for serious offences in a more simplistic manner.

As previously stated, section 313 of the *Telecommunications Act 1997* is a vital measure and should remain. Consideration could be given to placing this obligation under the TIA Act.

(c) the extent to which the activities regulated under the Acts should be regulated under general communications legislation or other legislation;

The Commission considers that there is a specific need for the TIA Act given its importance to law enforcement to effectively investigate serious criminal offences including corruption, and its importance to protect the privacy of individuals.

The Commission considers that the TIA Act should remain as a stand-alone piece of 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

The Commission considers the central coordination of policy and regulations should remain at Commonwealth level with the Attorney-General's Department. As previously stated, it also considers that the ACMA requires more regulatory authority for non-compliance with the TIA Act.

(e) whether the *Telecommunications (Interception and Access) Act* should be amended to provide for the role of a public interest monitor.

The Commission has reviewed the ARLC's analysis regarding the requirement of the public interest monitor ("PIM"). The ARLC did not recommend the establishment of a PIM because many of the functions of the PIM are adequately provided by other bodies. The Commission concurs with this finding and notes that it is consistent with the submissions to this review by both the Australian Federal Police and the Attorney-General's Department.

RESPONSE TO PART B

Comprehensive revision of the *Telecommunications (Interception and Access) Act 1979* (the TIA Act), with regard to recommendations relating to the TIA 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.

Strengthening the safeguards and privacy protections

Recommendation 1

The legislation's privacy protection objective

The Committee recommends the inclusion of an objectives clause within the TIA Act, which:

- **expresses the dual objectives of the legislation -**
  - **to protect the privacy of communications;**
  - **to enable interception and access to communications in order to investigate serious crime and threats to national security; and**
- **accords with the privacy principles contained in the Privacy Act 1988.**

The Commission fully supports Recommendation 1.

Recommendation 2

The proportionality tests for issuing warrants

The Committee recommends the Attorney-General's Department undertake an examination of the proportionality tests within the TIA Act. Factors to be considered in the proportionality tests include the:

- **privacy impacts of proposed investigative activity;**
- **public interest served by the proposed investigative activity, including the gravity of the conduct being investigated; and**

- **availability and effectiveness of less privacy intrusive investigative techniques.**

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.

The current TIA Act is overly complex and this is one of the main reasons reforms are required. The Commission considers that proportionality tests, as outlined in Recommendation 2, will bring further complexity to the regime for both interception agencies and issuing authorities.

A threshold tied to serious offences is clear and better reflects the legislative intent regarding thresholds for interception. The current system requires consideration to be given to various elements including; privacy impacts, the gravity of the conduct and offence, the value of the information to the investigation (public interest value), and the availability and effectiveness of less intrusive investigative techniques. Accordingly, the proportionality test is unnecessary.

Methods employed by criminal or corrupt persons evolve over time and become more sophisticated. Criminals exploit emerging and new technologies, particularly in the communications sector, to further serious criminal and/or corrupt activity.

Law enforcement methodologies must also evolve to match increasingly effective corrupt and criminal activities. To this end, telecommunications interception is an essential investigative methodology.

The Commission notes that the current regime addresses the concerns regarding privacy, the public interest and the consideration of less intrusive investigative techniques. The imposition of this particular recommendation is likely to duplicate aspects of the current regime and lead to a high degree of uncertainty about warrant application outcomes.

Recommendation 3

Mandatory record-keeping standards

The Committee recommends that the Attorney-General's Department examine the TIA Act 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.

(See combined Recommendations 3 & 4 response below.)

Recommendation 4

Oversight arrangements by the Commonwealth and State Ombudsman

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 TIA Act.

Further, the review should consider the scope of the role to be undertaken by the relevant oversight mechanism.

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.

(Recommendations 3 & 4)

The Commission fully supports a robust regime of mandatory record keeping and reporting requirements for agencies exercising powers under the TIA Act. The Commission considers the current system can be improved by the Attorney-General's Department reviewing the oversight arrangements to reduce the burden of unnecessary records, but at the same time providing stronger accountabilities and more practical methods that reflect current interception practices.

The Commission considers that changes to the reporting requirements to evaluate proportionality require a subjective assessment. This increases the complexity and reduces the clarity of the reporting regime and may introduce inconsistencies across different oversight bodies.

Record keeping and reporting is a crucial mechanism to ensure compliance within the regime and is vital for public confidence. The Commission considers the TIA Act should stipulate clear and unambiguous obligations as opposed to subjective assessments.

The Commission is currently oversighted by both State and Commonwealth Ombudsman's offices. The accountability under the current regime is extremely rigorous. Both the State and Commonwealth Ombudsman's offices ensure a high degree of accountability and it is therefore appropriate for them to continue to perform the oversight function.

Reforming the lawful access regime for agencies

Recommendation 5

Reducing the number of agencies eligible to access communications information

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 utilitising telecommunications data as the threshold on which access is allowed.

The Commission principally accesses two categories of telecommunications data for investigative purposes. The first category is commonly known as subscriber data. This information provides details of the telecommunications account holder, similar to the information contained in a telephone directory. The second category can be described as traffic data (both historic and prospective). This information gives details about communications, such as the services involved, the date and time, and in some cases, location information. Telecommunications data does not include the content of communications, i.e. the voice content of a telephone call or the contents of a text message or email.

In simple investigations, telecommunications data is used to provide information and evidence that directly relates to the investigation. In complex investigations, telecommunications data is used to build a picture of suspected offences by identifying participants and establishing relationships and levels of contact. The use of telecommunications data to identify methods of communication is a crucial investigative tool, particularly when investigating criminal activity conducted by a syndicate of people. Telecommunications data is also used in excluding people from further investigation.

The Commission fully supports Recommendation 5 and further supports a stronger threshold for access to traffic data as opposed to a lower threshold for access to subscriber data. The Commission considers this will strengthen the privacy protections within the TIA Act.

Recommendation 6

Standardise warrant tests and thresholds

The Committee recommends 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;**
- **impact on the law enforcement agencies' investigative capabilities, including those accessing stored communications when investigating pecuniary penalty offences.**

The Commission considers the level of privacy intrusion is similar for access to either stored or live communications and, therefore, the threshold for access to both should be the same.

Recommendation 7

Expanding the basis of interception activities

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.**

The Commission fully supports Recommendation 7 and refers to its comments in section 14(a) of the Commission's PJCIS submission (Submission No 156) (Appendix 1):

> *The current regime of identifying communication based on services or devices for interception can be restrictive. In the modern telecommunications environment communications can be associated with or described by various identifiers which can be more clinically targeted than by simply specifying device or service identifiers. By expanding the basis of interception activities the Commission believes that better targeting communications associated to particular offending behaviour can be achieved providing greater operational effectiveness and reducing the level of privacy intrusion. Being able to identify particular communications within the service, for example, may allow agencies to exclude or include particular communications through relevant identifiers. For example, if an internet based interception were to be conducted on a user's account the agency may only be interested in particular communications such as those linked to an email address or internet chat protocol. By expanding the basis for interception activity, agencies may be able to exclude other communications thereby better targeting the communications of interest and providing greater privacy protection by excluding other content.*

Streamlining and reducing complexity

Recommendation 8

Simplifying the information sharing provisions that allow agencies to cooperate

The Committee recommends that the Attorney-General's Department review the information sharing provisions of the TIA Act to ensure:

- **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.**

The current TIA Act is very restrictive in the mechanisms for agencies to share information with other agencies, even where it may be in the public interest to do so. The Commission has encountered many situations where investigations in other agencies could have commenced or been assisted by sharing information. However, the Commission was unable to assist due to legislative restrictions about disclosure of lawfully intercepted information (LII).

Some of these examples are outlined below.

CASE STUDIES

Currently the Commission is empowered under the *Corruption and Crime Commission Act 2003* ("CCC Act") to investigate suspected misconduct by public officers in Western Australia. As an outcome of an investigation, the Commission may prosecute for criminal offences, form opinions as to the occurrence of misconduct or recommend the taking of disciplinary action against a public officer, pursuant to section 43(1) of the CCC Act.

In many instances, public officers who are investigated by the Commission may be stood down by their employer pending the results of a Commission investigation. Currently the Commission is restrained from being able to provide any LII to the Chief Officer of State Government agencies, except for the Commissioner of the Western Australia Police, to enable them to undertake disciplinary action against government employees for serious misconduct.

The Commission would like the provisions of sections 67 and 68 of the TIA Act to be expanded to enable the Commission to communicate LII to Chief Officers of State Government agencies for matters involving serious misconduct. The Commission is currently able to disseminate LII for the purposes of police disciplinary action, but not for the equivalent public sector misconduct investigations.

The following are a number of case study examples to illustrate the limitations of this restriction.

Operation Rocky

The Commission investigated allegations that a Department of Education employee was communicating inappropriately with primary school students. During the course of the investigation the Commission intercepted multiple telecommunications services.

During the course of the investigation the individual was prohibited from entering school premises by the Department of Education. The Commission captured LII revealing that the individual was breaching this ban by attending other schools and school events.

The Commission was unable to disclose this information to the Department of Education enabling it to enforce the ban. The Commission deployed its own measures to ensure the safety of children; however, the inability to disclose the LII prevented an overt intervention by the Department of Education.

While the Commission did employ other techniques to monitor the target, the Commission's inability to disseminate LII meant that there was an increased risk to the safety of students.

The telecommunications intercepted by the Commission captured the individual accessing significant amounts of child pornography material, which formed the basis of eight Commonwealth charges of unlawfully using a carriage service for child pornography material. The individual was convicted of six of these charges and received 12 months' imprisonment, suspended for 18 months and $12,000 in fines.

Although the individual lost their job as a result of the criminal convictions, the Commission was unable to release LII to the relevant department for disciplinary proceedings prior to the criminal trial.

Operation Tiberias-Franklin

During a protracted investigation into the improper influence of public officers by lobbyists, the Commission identified suspected offences whereby lobbyists and a building industry union member were attempting to extort money from sub-contractors and were ultimately paid by the project owner. At this time the lobbyists were also acting for the project owner.

Under the current TIA Act, the Commission was unable to disclose this information to the Australian Building and Construction Commissioner for the purposes of their investigation.

Operation Wilson

The Commission conducted an investigation into leaks of information to a target of another agency's investigation. The target was involved in activities that were causing serious ecological damage. During the Commission's investigation, telecommunications interception revealed that the CEO of the agency informed the target he was being investigated and another

employee of the agency was disclosing operational methodologies and coaching the target.

Despite the seriousness of the leak, coupled with the CEO's position within the agency, the Commission was not able to communicate LII to the internal investigations area of the agency immediately to prevent the compromise of their internal investigation and to promptly and appropriately respond to the actions of the CEO.

Operations Huskisson, Supply and Rosebery

The Commission has conducted a number of significant investigations into misconduct by Department of Corrective Services' ("DCS") employees that involved telecommunications interception.

In two examples, prison officers were using their positions to access information pertaining to prisoners and releasing that information to outlaw motorcycle gang members. The Commission charged two individuals, both who were subsequently convicted of unlawful access of computers pursuant to section 440A of the *Criminal Code Act 1995*. The Commission was, however, restricted in respect to the information that could be disclosed to DCS prior to the prosecution. This meant that administrative action could not be taken at an early stage, resulting in continued costs to the public whilst the employee maintained employment status.

In another Commission investigation, prison officers and health workers were using drugs and transporting drugs into prisons. These individuals were imprisoned as a result of giving false testimony to the Commission, but the Commission was unable to disseminate any of the relevant LII indicating the drug usage patterns to DCS.

Recommendation 9

Removing legislative duplication

The Committee recommends that the TIA Act be amended to remove legislative duplication.

The Commission fully supports Recommendation 9.

Recommendation 10

A single warrant with multiple telecommunications interception powers

The Committee recommends that the telecommunications interception warrant provisions in the TIA Act be revised to develop a single interception warrant regime.

The Committee recommends the single warrant regime include the following features:

- **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.**

The Committee further recommends that the single warrant regime be subject to the following safeguards and accountability measures:

- **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.**

The Commission supports a single warrant regime. However, Recommendation 10 does not refer specifically to a B Party Warrant which is a crucial part of the current regime and this needs to be included in the single warrant regime. As previously stated, the Commission supports a threshold test for warrants linked to the offence, which includes clear evidence to establish reasonable suspicion, as opposed to proportionality.

Modernising the cost sharing framework

Recommendation 11

Align industry interception assistance with industry regulatory policy

The Committee recommends that the Government review the application of the interception-related industry assistance obligations contained in the TIA Act and *Telecommunications Act 1997.*

The Commission fully supports Recommendation 11 and refers to its comments in section 4(a) of the Commission's PJCIS submission (Submission No 156) (Appendix 1):

> *The Commission supports the concept of a tiered model, understanding that the current model was predicated on the existence of only Carriers and Carriage Service Providers all with similar resource backing and generally a large customer base. The reality is that smaller providers generally have fewer customers and therefore have less potential to be required to execute an interception warrant. Whilst the Commission understands that uniform obligation is a fairer system, the reality is that the majority of intercepts are executed through the major telecommunications carriers and supports a cost neutral environment for carriers.*

Recommendation 12

Clarify ACMA's regulatory and enforcement role

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.

The Commission fully supports recommendation 12. The Commission supports the concept of expanding the range of regulatory options available to the ACMA and clarifying the standards with which the industry must comply.

Recommendation 13

Requirements for industry interception obligations

The Committee recommends that the TIA Act be amended to include provisions which clearly express the scope of the obligations which require telecommunications providers to provide assistance to law enforcement and national security agencies regarding telecommunications interception and access to telecommunications data.

The Commission fully supports Recommendation 13 and refers to its comments in section 9(a) of the Commission's PJCIS submission (Submission No 156) (Appendix 1):

> *The current regulatory regime for industry interception obligations is administratively burdensome for both industry participants and the regulatory agency. The current requirement of industry to prepare and submit interception capability plans which are then assessed annually should be reviewed.*
>
> *The implementation of detailed requirements for industry interception obligations may assist in clarifying requirements and account for technical complexities. The Commission endorses the inclusion of administrative requirements as part of industry interception requirements. In many cases, difficulties or delays in interception are due to administrative, as opposed to, technical limitations.*

Recommendation 14

Clarify that the interception regime includes ancillary service providers

The Committee recommends that the TIA Act and the *Telecommunications Act 1997* 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.

The Commission fully supports Recommendation 14 and refers to its comments in section 9(b) of the Commission's PJCIS submission (Submission No 156) (Appendix 1):

As communications migrate to IP networks and applications, the lawful access to such communications to investigate serious offences has become more complex and challenging. Communications to further criminal activity are now taking place across a myriad of ancillary service providers including offshore web based email and social networking applications. The migration of offending behaviour across these networks or applications mirrors the general uptake of these technologies by the Australian public. However, it is often the case that offenders will attempt to use means of communications which they believe are secure or enable them to avoid interception to further criminal activity. In the modern communications environment it is vital that the legislative regime covers the new forms of IP based communications otherwise the ability of law enforcement agencies to investigate serious crime and to adequately protect the public will degrade over time. The Commission supports the inclusion of ancillary service providers to ensure both jurisdictional and technical issues can be addressed.

Recommendation 15

Industry participation model

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.

The Commission does not support Recommendation 15 but prefers the three tiered industry participation model as proposed by the AGD discussion paper. The Commission refers to its comments in section 9(c) of the Commission's PJCIS submission (Submission No 156) (Appendix 1):

The Commission acknowledges that the modern telecommunications industry environment is complex and dynamic and that applying a regulatory regime across such an industry requires some flexibility. The Commission believes that a three-tiered industry participation model could provide scope for a reasonable and more equitable system of industry participation based on the level of assistance required by agencies.

The Commission believes that all service providers should be obliged by law to provide reasonable assistance. Larger providers that are more likely to receive warrants should support a higher capability for support and response.

The Commission believes that a three-tiered model should not be based solely on market share or company size. The Commission would endorse an avenue for agencies to have input into the classification of providers within the tiers under such a model.

Recommendation 16

An offence for failure to assist in the decryption of communications

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.

The Commission supports Recommendation 16 and refers to its comments in section 15(a) of the Commission's PJCIS submission (Submission No 156) (Appendix 1):

The Commission supports the establishment of such an offence. Where communications are accessed by agencies lawfully under warrant, and decryption assistance is required the legislation should enforce the provision of assistance and an offence regime for non-compliance.

Recommendation 17

Institute industry response timelines

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.

The Commission supports the concept of industry response timelines and refers to its comments in section 15(b) of the Commission's PJCIS submission (Submission No 156) (Appendix 1):

> *The facilitation of lawful access to communications in most instances is time critical. Where vital evidence needs to be captured immediately due to circumstances, the lack of timeliness for lawful assistance can jeopardise investigations. In the Commission's experience lawful access can in many cases be instant or in other cases take up to several weeks. The Commission believes that reasonable obligations addressing response timelines is highly desirable within the TIA Act.*

The Commission considers that the consultation process and cost considerations, as denoted in Recommendation 17, are reasonable.

Recommendation 18

Revision of the interception regime

The Committee recommends that the 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.

The Commission supports Recommendation 18.

PART C

Other key issues relating to the Commission's function and powers under the TIA Act.

Data retention

The analysis of telecommunications data is crucial to the Commission's investigative function. The Commission wishes to restate its comments from section 15(c) of the Commission's PJCIS submission (Submission No 156) (Appendix 1):

> *Telecommunications data is a fundamental investigative tool within many investigations. Carriers retain some data sets currently for commercial purposes (i.e. call charge records relating to telephony services). There is no requirement for carriers to retain data should their business practices no longer require it. The Commission notes with concern that the discussion paper states that "some carriers have already ceased retaining such data for their business purposes and that it is no longer available to agencies for their investigations".*
>
> *In simple investigations telecommunications data is used to provide information or evidence directly related to the investigation.*
>
> *In complex investigations telecommunications data is used to build a picture of suspected offences by identifying participants, establishing relationships and levels of contact. The use of telecommunications data to identify methods of communication is a crucial investigative tool.*
>
> *Agencies will face many challenges as telecommunications technologies migrate to IP networks. Investigations across almost all serious crime types including corruption, counter-terrorism and homicide rely significantly on telecommunications data. Without legislated data retention obligations the degradation of investigative capability will be significant.*

Permitted Use - Emergency Provisions

Whilst it is not the Commission's role to intervene in life threatening situations, in an operational law enforcement environment unpredictable incidents may occur. There may be occasions where the Commission is required to respond to a life threatening situation. Ideally the Commission would refer the matter to the Western Australia Police; however, if this is not practicable due to the urgency of

the required response, it is appropriate that emergency powers under the TIA Act are available.

To enable a response in these situations, the Commission requests to be included in the emergency provisions under section 7(8) of the TIA Act and provisions be drafted for emergency disclosure of LII in emergency situations beyond the mechanisms currently contained under section 68 of the TIA Act.

CONCLUSION

For the reasons stated in this submission, the Corruption and Crime Commission firmly supports holistic reform of the *Telecommunications (Interception and Access) Act 1979* as proposed by the Government. The Commission is of the view that substantial consultation has occurred through the PJCIS inquiry and that this inquiry will enable further consultation with key stakeholders.

The rate of technological change in the communications sector is significant. The Commission considers that reforms to the TIA Act are overdue and that the Attorney-General's Department should produce an exposure draft to progress reform. Further consultation and policy consideration by the Parliament can then be conducted through a Parliamentary Committee process.