



Submission No 204

**Inquiry into potential reforms of National Security Legislation**

**Organisation:** Australian Crime Commission

UNCLASSIFIED



# AUSTRALIAN CRIME COMMISSION

**Submission to the  
Parliamentary Joint Committee on  
Intelligence and Security's inquiry into  
potential reforms of national security legislation**



UNCLASSIFIED

**UNCLASSIFIED**

**UNCLASSIFIED**

# Table of Contents

## Contents

|                                      |    |
|--------------------------------------|----|
| Executive Summary.....               | 5  |
| The Australian Crime Commission..... | 7  |
| Organised Crime .....                | 7  |
| Legislative Limitations.....         | 8  |
| Proposed Reforms .....               | 10 |
| Privacy.....                         | 11 |
| Accountability.....                  | 12 |
| Conclusion.....                      | 13 |

**UNCLASSIFIED**

**UNCLASSIFIED**

# Executive Summary

1. In today's increasingly globalised society the opportunities for organised crime are unprecedented. Complex networks stretch across continents to support 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. Organised crime is sophisticated, resilient, highly diversified and pervasive. It operates within and alongside legitimate businesses, spanning multiple sectors to maximise return and minimise risk.
2. The social, economic and health-related harms caused by illicit drug trafficking, financial crime, and associated violence and intimidation have a very real impact on the whole community. For this reason, the Government recognised organised crime as a matter of national security in Australia's first National Security Statement to Parliament in 2008.
3. Targeted, lawful and independently authorised access to telecommunications is a critical tool in the disruption of organised crime. However the Australian Crime Commission (ACC) and its national security and law enforcement partners confront persistent and growing challenges in obtaining such access. The growth and rapid change in telecommunication technologies, global participants and consumer behaviours have created a more diverse and dynamic telecommunications environment than was envisaged when the *Telecommunications (Interception and Access) Act 1979* (TIA Act) was first enacted. Notwithstanding the legislative modifications to the TIA Act over the intervening period, a holistic review of this framework and the need to consider the dramatic change in technologies, services and requirements to lawfully respond to the contemporary and emerging threats impacting the Australian community is welcomed.
4. This submission highlights a number of areas, as they pertain to the TIA Act and related legislation where reform could usefully contribute to addressing these challenges , without diminishing accountability, including:
  - a. Ensuring that data retention standards and periods have consistent application.
    - i. Retaining historical data for certain periods can provide significant value to ACC activities where criminal associations and events can be established through the use of communications. However, in practical terms, the duration and scope of data retention is not consistent, and there would be value in standardising data retention and destruction practices across all telecommunications providers.
  - b. Clarifying and simplifying alignment between the communications legislation and the ACC Act. Two areas of focus relate to this reform consideration:
    - i. The inclusion of explicit reference to ACC Special Operations and Special Investigations in communications related legislation, to

provide for targeted, lawful and independently authorised access to communications and stored data.

- ii. Enhanced alignment between the disclosure provisions within the telecommunications access legislative regime and the ACC Act, to include agencies that play a critical role in the response to organised crime, such as the Australian Taxation Office (ATO), Australian Securities and Investment Commission (ASIC) and the Australian Customs and Border Protection Service (ACBPS). Such an initiative recognises Australia's multifaceted law enforcement community, which seeks to combat serious and organised crime groups from every angle.
5. Importantly, these proposed reforms in no way seek to limit accountability and the need for an independent authority to sanction the interception of information or data. They do not seek access to any or all communications, but rather access when organised criminal activity is suspected and an independent authority permits the lawful interception of the content of those telecommunications.

# The Australian Crime Commission

6. In order to unite the fight against organised crime, the Australian Government established the ACC on 1 January 2003 as an independent statutory authority under the *Australian Crime Commission Act 2002* (ACC Act). The ACC's primary objective is to support and complement Australian law enforcement efforts to reduce the threat and impact of serious and organised crime on the Australian community. As the national criminal intelligence agency, the ACC is a niche, complementary agency that delivers specialist law enforcement intelligence analysis and investigative capabilities to its partners. It also provides a unique and valuable understanding of serious and organised crime, including its activities, methodologies and emerging areas of influence.
7. The ACC's priorities are set by its Board, which consists of the Commissioners of all Commonwealth, state and territory police forces, as well as the heads of the Attorney-General's Department (AGD), the ATO, ACBPS, the Australian Security Intelligence Organisation (ASIO), and ASIC.
8. One of the Board's primary roles is to establish Special Investigations and Special Operations, which enlivens the ACC coercive powers. Before establishing Special Investigations and Operations, the Board must judge that either ordinary police methods of investigation have been, or are likely to be, ineffective. In this way, the ACC through its Act and the Determination of its Board addresses the elements of organised crime that represent the greatest threat to the Australian community.

## Organised Crime

9. In 2011, the ACC produced its most comprehensive unclassified assessment of the threats and harms posed to Australia by organised crime: the *Organised Crime in Australia* report (OCA)<sup>1</sup>. The assessment determined that organised crime posed a 'high' overall threat to the Australian community, with money laundering, identity crime, and amphetamine-type stimulants (ATS) representing a particular critical risk.
10. The threat posed by organised crime is not unique to Australia. Organised crime has gone global, moving well beyond a simple law and order problem within the remit of an individual agency, jurisdiction or country. Unlike the citizens of today's globalised world, organised crime does not align itself to symbols of nationality and sovereignty, such as flags, language, religion, currency and national borders. Organised crime has seized upon the economic, social, and technological opportunities made possible by globalisation in a manner which surpasses the capabilities of many global governments and law enforcement agencies.

---

<sup>1</sup> The ACC released the OCA in 2011. The report is available online via the ACC's website: [www.crimecommission.gov.au](http://www.crimecommission.gov.au).

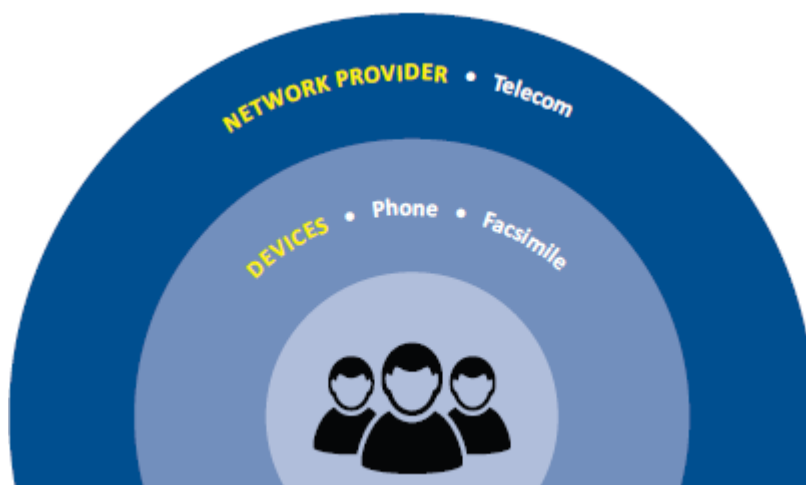


11. As organised crime activities become increasingly globalised and transnational in nature, organised crime groups become more reliant on information and telecommunication technologies to facilitate their activities. Whether it relates to a brief meeting between two criminal individuals, or the international shipment of a million dollar illicit drug cache, organised crime groups are reliant on modern communication technologies to achieve their objectives.
12. In recent decades, information and communication technologies have diversified at a staggering rate. Some office employees can attest to these changes, having commenced their career with a word processor, telephone, and occasional facsimile, and having adapted to the gradual shift to instantaneous electronic telecommunications, social media, and communication encryption. Just as legitimate businesses have adapted their telecommunication practices to remain competitive in the global market, organised crime has demonstrated an ability to adapt along with the technological opportunities available. And just like legitimate business, organised crime's adaptability has enabled many organised crime groups to establish business networks that span continents.
13. These changes have resulted in technology and telecommunications being exploited in ways that were unimaginable in 1979 when the original legislation was introduced.

## Legislative Limitations

14. In 1979, when the TIA Act was first enacted, the Australian Telecommunications Commission (Telecom), a government instrumentality, was the monopoly supplier of telecommunications services in Australia. Figure 1 illustrates this environment, which consisted of a single carrier providing telecommunications services on two possible devices.

Figure 1: Australian Communications Environment – 1979



15. Since this time, the environment has shifted significantly. In 1981, the first car-phones were introduced, followed by the first truly mobile telephones in 1987. The Internet emerged in Australia in 1989, and has revolutionised global communications. Today, Internet compatible mobile devices have mobilised the technology.
16. The growth of the Internet has had a dramatic effect on culture and commerce. The ongoing and ever rising demand for reliable, near instantaneous, globally accessible, secure telecommunications to support discussion forums, blogs, social networking, and shopping sites has spawned an abundance of services and suppliers of services.
17. The industry has expanded to the point where individuals have access to a range of industry participants, with multiple options available at each level, including attributes, application services, network access, network providers and application service providers. Figure 2 illustrates the complexity of the modern communications environment.



Figure 2: Australian Communications Environment - 2012

18. The TIA Act was written to suit the 1979 telecommunications environment. Law enforcement agencies such as the ACC, whose mandate is to disrupt the highest threat organised crime groups impacting on Australia, have witnessed an erosion of their capabilities to lawfully target these groups, despite independent authorisation to do so. As such, the ACC is proposing that the Parliamentary Joint Committee on Intelligence and Security consider recommendations to enhance existing legislation in support of law enforcement's aim to respond to present and future organised crime activities.

## Proposed Reforms

19. The reform options the ACC wishes to raise with the Committee directly impact the ACC and are aimed at maintaining strong and appropriate governance whilst enabling the strict lawful access to information where serious offences are suspected. This will support law enforcement's efforts to understand the serious and organised crime environment, intervene against serious criminal activities threatening Australia and its citizens, and prevent similar activities from being perpetrated in the future.
20. Reform considerations that are proposed by the ACC specific to our operations are outlined below.
  - a. Ensuring that data retention standards and periods have consistent application.
    - i. Retaining historical data for certain periods can provide significant value to ACC operations where criminal associations and events can be established through the use of communications. However, in practical terms, the duration and scope of data retention is not consistent, and there would be value in standardising data retention and destruction practices across all telecommunications providers.
  - b. Clarifying and simplifying alignment between the communications legislation and the ACC Act. Two areas of focus relate to this reform consideration:
    - i. The inclusion of explicit reference to ACC Special Operations and Special Investigations in communications related legislation, to provide for targeted, lawful and independently authorised access to communications and stored data.
    - ii. Enhanced alignment between the disclosure provisions within the telecommunications access legislative regime and the ACC Act, to include agencies that play a critical role in the response to organised crime, such as the Australian Taxation Office (ATO), Australian Securities and Investment Commission (ASIC) and the Australian Customs and Border Protection Service (ACBPS). Such an initiative recognises Australia's multifaceted law enforcement community, which seeks to combat serious and organised crime groups from every angle.
21. The ACC has outlined these proposals in detail along with supporting justification in a classified submission to the Committee.
22. Domestic and international experience has established an express need for reform in these areas. The response capabilities sought by law enforcement are proportionate to the threat posed by the highest threat serious and organised crime. Indeed, as communications and commercially available encryption services continue to evolve, law enforcement capacity and authority to respond will continue to diminish unless appropriate legislative reform is enacted.

## Privacy

23. The ACC's legislated mandate is to detect, disrupt and deter the highest risk serious and organised crime threats only. This is a narrow but crucial component of Australia's broader law enforcement and national security infrastructure.
24. All people deserve the fundamental right to engage in communication and the global exchange of ideas in a personal and private manner, free from the threats posed by external infiltration and malicious perversion. The ACC supports this fundamental civil liberty and believes that it is worthy of protection.
25. Serious and organised crime groups, both domestic and international, represent the most significant threat to the privacy and civil liberties of Australian citizens and their international associates. Some organised crime groups have the capability and the motivation to infiltrate the personal telecommunication channels and devices of Australian citizens from anywhere in the world to steal identity credentials, defraud personal savings and superannuation investments, and hijack personal computers for the malicious and covert perpetration of additional crime. Organised crime groups exploit the increasingly public nature of modern telecommunications to their advantage. By virtue of the anonymity afforded by the Internet, organised crime can now be whoever their victim needs them to be, whether this be a renowned and certified investment firm, a generous international beneficiary, or an online soul-mate who's fallen on hard times. In short, organised crime does not respect, and actively exploits, the private lives of Australian citizens.
26. The capabilities proposed by the ACC in this submission are aimed at maintaining a strong accountability framework where access to communication and data is only obtained through meeting serious offence thresholds, independently authorised, and externally reviewed. In the absence of this timely review, it is likely that organised crime's capability to infiltrate the privacy of Australians will continue to exceed law enforcement's capability to counter these very real threats.

# Accountability

27. The ACC recognises the value of comprehensive and stringent accountability and governance measures for Australia's law enforcement and intelligence agencies. As such, the ACC has established a number internal mechanisms to safeguard the integrity of the ACC and its staff when conducting its activities. The ACC is also accountable to a number of well established external scrutiny mechanisms, including the:
- a. ACC Board
  - b. Intergovernmental Committee on the ACC (IGC-ACC), which is chaired by the Commonwealth Minister for Justice and consists of the police ministers from each State and Territory
  - c. Parliamentary Joint Committee on Law Enforcement
  - d. Australian Commission for Law Enforcement Integrity
  - e. Commonwealth Ombudsman, and
  - f. Australian National Audit Office.
28. The ACC works closely with all of its governance bodies to ensure maximum compliance and accountability.
29. As previously stated, the ACC's priorities are set by its Board through the establishment of Special Investigations and Special Operations. The establishment of these Special Investigations and Operations is influenced by significant intelligence holdings on the most critical threats posed by organised crime to the Australian community. The Board's decision to establish a Special Investigation or Operation is based on considerations of the magnitude and extent of the particular market or aspect of organised crime that is the focus of that Special Investigation or Operation, and whether or not traditional law enforcement methods have been, or are likely to be, effective in addressing that market or aspect of organised crime.
30. In making its decision to establish a Special Operation or Investigation, the Board is accountable to the IGC-ACC, which has the authority to veto the Board's decisions. In this way, the ACC's priorities are determined by Australia's 14 most senior law enforcement officials, and each of Australia's nine Commonwealth, State and Territory Police Ministers.
31. The ACC's expertise and capability in telecommunication access and electronic surveillance is grounded in its implementation and application of robust accountability and compliance measures. The ACC has received no recommendations from the Commonwealth Ombudsman over the past three years on its compliance with the TIA Act and the Surveillance Device Act. The Ombudsman has remarked favourably on the strong mechanisms in place for ensuring compliance in the ACC. Central to this

compliance model is the ACC's five-point strategy designed to demonstrate and practice an excellence in compliance that extends beyond general compliance.

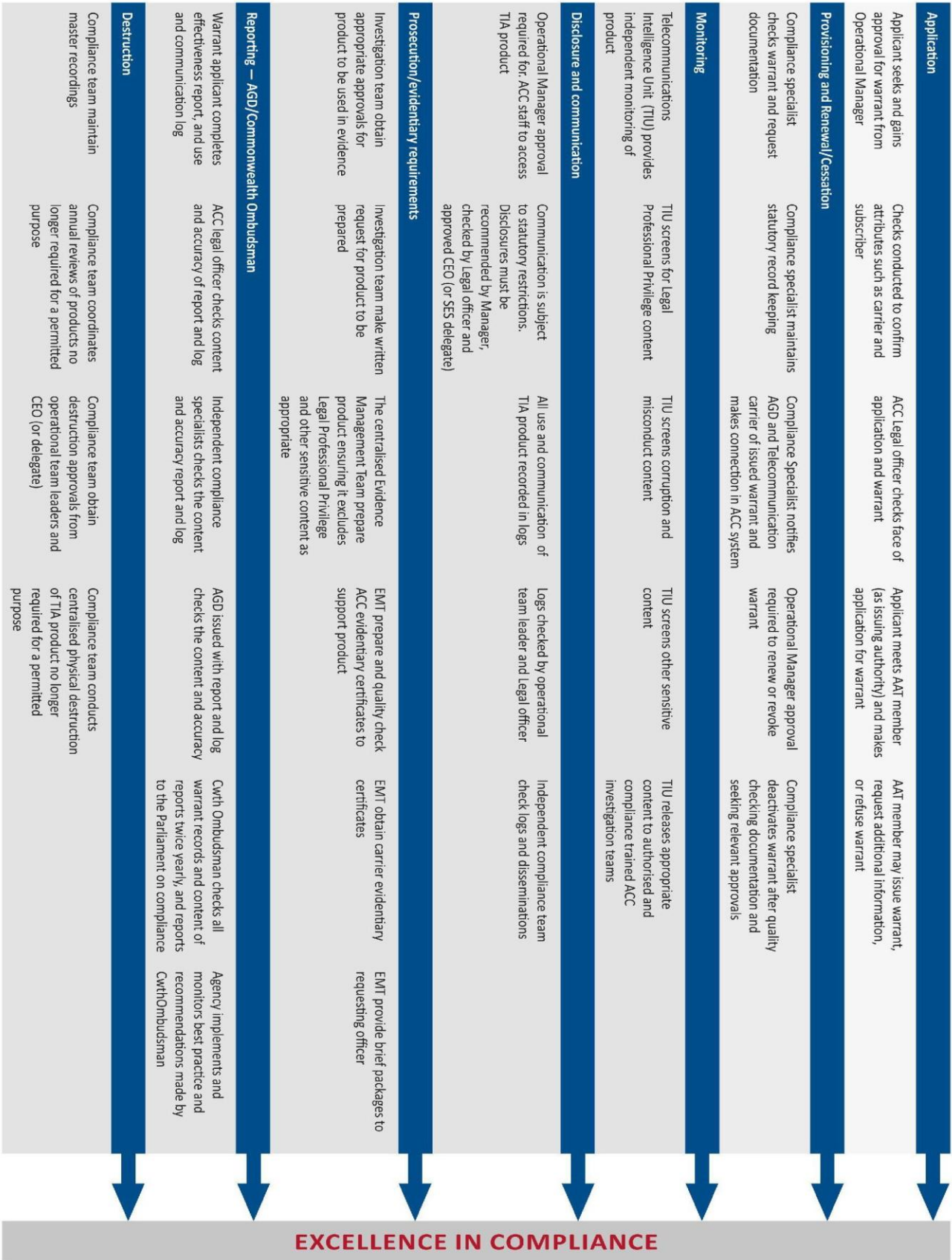
32. The Components of the ACC's five-point compliance strategy are:
- a. centralised administration
  - b. quality assurance at all stages
  - c. mandatory initial, and annual refresher, training
  - d. annual compliance review, and
  - e. a communication strategy for highlighting matters of concern.
33. The ACC considers that its accountability for the use of telecommunications intercept material is stringent, comprehensive and appropriate. The oversight provided by the Commonwealth Ombudsman's office is thorough and provides avenues for complaints and for addressing natural justice concerns.
34. ACC accountability measures for its telecommunications interception products, from initial warrant application to final destruction, are outlined at Attachment A.
35. The ACC Act, specifically requires the ACC to protect the safety and reputation of persons, and the interests of justice.

## Conclusion

36. Australia's telecommunications environment as it was when the TIA Act was enacted in 1979 has evaporated. Australia now communicates via a truly global telecommunications network, and Australian citizens are increasingly engaging and living their lives in an ethereal cyber world. This global community has enabled unprecedented opportunities for Australia, its citizens, and its criminals. As engagements become more public and accessible, the necessity for privacy and security also grows. Australians have now reached an impasse between the opportunities and the threats to privacy and personal security that today's globalised world affords.
37. The ACC's mandate is to assist in the intervention and prevention of serious and organised crime being perpetrated against the Australian community. At present, however, organised crime's capability to infiltrate the privacy of Australians exceeds the ACC's capability to infiltrate organised crime telecommunication channels in order to attack its activities. This is a detriment to Australia's national security.
38. A timely review of National Security Legislation is welcome to ensure that it adequately supports both the national security and law enforcement communities in their collective efforts to protect Australia, its economy, and its citizens.



**MANDATORY INITIAL AND ANNUAL REFRESHER TRAINING**



**EXCELLENCE IN COMPLIANCE**

**UNCLASSIFIED**

**UNCLASSIFIED**





© ACC 2011. All rights reserved.