Communications Alliance
Australian Mobile Telecommunications Association
Joint Submission

to the Parliamentary Joint Committee on Law Enforcement
Inquiry into

Law enforcement capabilities in relation to child exploitation

20 August 2021

Contents

Communications Alliance

Communications Alliance is the primary telecommunications industry body in Australia. Its membership is drawn from a wide cross-section of the communications industry, including carriers, carriage and internet service providers, content providers, equipment vendors, IT companies, consultants and business groups.

Its vision is to provide a unified voice for the telecommunications industry and to lead it into the next generation of converging networks, technologies and services. The prime mission of Communications Alliance is to promote the growth of the Australian communications industry and the protection of consumer interests by fostering the highest standards of business ethics and behaviour through industry self-governance.

Australian Mobile Telecommunications Association

The Australian Mobile Telecommunications Association (AMTA) is the peak industry body representing Australia's mobile telecommunications industry. Its mission is to promote an environmentally, socially and economically responsible, successful and sustainable mobile telecommunications industry in Australia, with members including the mobile network operators and carriage service providers, handset manufacturers, network equipment suppliers, retail outlets and other suppliers to the industry.

1. Introduction

Communications Alliance and the Australian Mobile Telecommunications Association (Associations) welcome the opportunity to make a joint submission to the Parliamentary Joint Commission on Law Enforcement (Committee) Inquiry into Law enforcement capabilities in relation to child exploitation.

The Committee has set the following Terms of Reference:

> *"Pursuant to subsection 7(1) of the Parliamentary Joint Committee on Law Enforcement Act 2010, the Committee will inquire into and report on the capability of Australia's law enforcement agencies to tackle the growing scourge of child exploitation, with particular reference to:*
>
> *a) trends and changes in relation to the crime of online child exploitation;*
> *b) reviewing the efficacy of and any gaps in the legislative tools and tactics of law enforcement used to investigate and prosecute offenders;*
> *c) considering opportunities and suitability of streamlining legislative constraints to enable faster investigations that can better respond to rapidly evolving trends in offending;*
> *d) considering the use by offenders of encryption, encryption devices and anonymising technologies, and Remote Access Trojans to facilitate their criminality, along with the resources of law enforcement to address their use;*
> *e) considering the role technology providers have in assisting law enforcement agencies to combat child exploitation, including but not limited to the policies of social media providers and the classification of material on streaming services;*
> *f) considering the link between accessing online child abuse material and contact offending, and the current state of research into and understanding of that link; and*
> *g) any related matters."*

In the following, we will seek to provide some general feedback and observations as they relate to the issues above.

2. Overview over current legislative assistance and cooperation arrangements

2.1. The Associations and their members are keen to assist intelligence and law enforcement agencies to protect our society against child exploitation that may be carried out through the use of communications services and other electronic equipment and infrastructure.

2.2. Carriers and carriage service providers (C/CSPs) represented by the Associations already provide significant levels of assistance to intelligence and Law Enforcement Agencies (LEAs), including under the following pieces of legislation

- Data Retention Regime (*Telecommunications (Interception and Access) Amendment (Data Retention) Act 2015*);
- Telecommunications Sector Security Reform (TSSR) requirements in Part 14, Division 3 of the *Telecommunications Act 1997;Telecommunications (Interception and Access) Act 1979;*
- *Telecommunications Other legislation Amendment (Assistance and Access) Act 2018; and*
- Section 313(3) of the *Telecommunications Act 1997*, which requires C/CSPs (among other things) to "give help as reasonably necessary" to assist authorities with enforcing the criminal law and laws imposing pecuniary penalties.

2.3. All C/CSP, digital platforms and search engines also provide assistance, both voluntary and legislated, for example through compliance with the *Criminal Code Amendment (Sharing of Abhorrent Violent Material) Act 2019* (AVM Act).

2.4. All C/CSP, digital platforms, search engines, app distribution services and other members of the online industry will also continue to lend their assistance under formalised existing and new arrangements in the recently enacted *Online Safety Act* 2021. The Associations – in cooperation with other industry associations – are currently in the process of developing industry codes that accompany the *Online Safety Act 2021* to further strengthen online safety. The codes are to be submitted to the eSafety Commissioner for registration in July 2022. Once registered, these codes become enforceable by the Commissioner.

2.5. The *Online Safety Act 2021* and the industry codes will be complemented by the *Online Safety (Basic Online Safety Expectations) Determination* (currently in consultation) which sets out expectations to uphold online safety for Australian end-users for social media services and other sections of the industry.

2.6. All communications member organisations (i.e. C/CSPs, platforms, search engines, hardware and software manufacturers, etc.) also assist LEAs through the workings of the *Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018* (Assistance and *Access Act 2018)*.

2.7. Moreover, our members will assist agencies through any legislated measures that will flow out of the *Telecommunications Legislation Amendment (International Production Orders) Act 2021* and any associated international treaties and the *Surveillance Legislation Amendment (Identify and Disrupt) Bill 2020,* once the latter passes Parliament.

3. Assistance currently provided

3.1. It goes without saying that illegal content, especially material relating to child sexual exploitation, abuse and terrorism, must be eradicated to the extent possible and as quickly as possible, to minimise the detrimental effects on all parties involved.

3.2. As in the past, our industry continues to engage closely with all stakeholders, including enforcement agencies, and is keen to assist, where appropriate and feasible, to create, maintain and promote a safe online environment.

3.3. Under current arrangements, and at the request of the Australian Federal Police and pursuant to section 313(3) of the *Telecommunications Act 1997*, several carriers block access to the INTERPOL 'Worst of' list of domains that disseminate the most severe child abuse material worldwide.

3.4. C/CSPs should be provided with legal certainty in relation to providing assistance to enforcement agencies. For example, during and in the aftermath of the Christchurch terror attacks, internet service providers (ISPs) did not receive a direction (despite concerted efforts by ISPs to elicit such a direction), from the eSafety Commissioner, nor from any other authority, to block access to any of the material that the perpetrator had live-streamed and/or posted online. Given the heinous nature of the material involved, in the absence of a direction to block the websites that hosted the footage of the shootings and the manifesto, all major Australian ISPs took the decision, at their own initiative, to block the identified websites. This left the ISPs exposed to legal liability – a situation which lasted almost 6 months.

3.5. Communications Alliance has since worked with the eSafety Commissioner to put in place a Protocol that governs processes for website blocking for larger ISPs during online crisis events. The formalised powers to direct ISPs to block access to abhorrent violent material in the recently enacted *Online Safety Act 2021* and the AVM Act complement this protocol.

3.6. Digital platforms member organisations have well established processes in place for supporting law enforcement investigations into child exploitation. All Communications Alliance member platforms proactively notify the National Centre for Missing and Exploited Children (NCMEC) when child exploitation material is discovered on their platforms, and NCMEC distribute any Australian leads to the Australian Federal Police for further investigation. Many platform members deliver regular training to Australian LEAs about what data is collected and retained by each platform and the process by which Australian agencies can issue lawful data access requests, account preservation requests and emergency requests (when life is at imminent risk).

3.7. Digital platforms have also invested in technologies to assist in proactively detecting and removing child sexual abuse material on their services, such as PhotoDNA and PDQ/TMK+PDQF. This is in addition to tools and features that digital platforms make available in order to keep children safe on their services.

4. Encryption – technological and legal context

4.1. Given the Committee's Terms of Reference make reference to encryption in the context of facilitating crime and LEAs' ability to address the use of the technology, it appears useful to place encryption into a broader technological and legal context.

4.2. Encryption is a vital part of modern electronic communications as it allows two or more parties to securely and confidentially engage with each other in many forms of communication and online activities. The ability to encrypt (and subsequently decrypt) communications underpins almost every online activity, from chatting on a mobile phone, messaging friends, accessing Government services to online banking, shopping and web browsing. It is fair to say that most of the common online activities that so many Australians engage with numerous times each day would not exist in their current form, or not at all, if not for the security that encryption affords. Therefore, it is important to ensure that encryption, and the resultant trust that communications (in their widest form) are secure and private, are not weakened as our societies increasingly become digitised and 'all online' and does not hinder or disrupt the normal activities undertaken by a law-abiding society.

4.3. Our sector recognises that encryption is also being used, at times, to conceal illicit and criminal activities, including the exchange of child exploitation material and the potential planning and execution of terrorist acts, and that it necessitates changes in the approach that industry, Government and law enforcement take to keeping Australians safe.

4.4. It is, therefore, key, to the extent technically possible, to rely on a secure framework that safeguards individual freedoms and privacy of individuals, including the privacy afforded through encrypted communications, while simultaneously allowing LEAs to pursue their goal of upholding and enforcing law and order where there are reasonable grounds to believe that those are at risk. All of the existing cooperative processes will remain in place and will continue to provide meaningful data for law enforcement investigations. When applying such a framework, it is key to recognise that the integrity of security within the supply chain is critical to the security of all services provided to Government, Industry and the public. Supply chain resilience has been a topic of significant focus in the security sector, and any weakening of security in the supply chain will have adverse systemic effects upon all products and services in the chain.

4.5. The digitisation of our societies over the past 20 years and the exponential growth in the use of communications services and electronic equipment and services have necessarily required significant changes to the legal basis that underlies the regulation of those services, networks and infrastructures, including the legislative basis for intelligence gathering, law enforcement and cybersecurity. In many instances, the

Associations' member companies, who are not C/CSPs, are voluntarily providing assistance to Australian law enforcement and intelligence agencies, in the absence of any legislative framework that directly applies to them.

4.6. In the past three years alone, the communications industry has seen a number of legislative changes, including the introduction of the mandatory Data Retention regime, the TSSR and the *Assistance and Access Act 2018*.

4.7. The recently enacted *International Production Orders Act 2021,* which paves the way for the establishment of a bilateral agreement between Australia and the United States under the *US Clarifying Lawful Overseas Use of Data (CLOUD) Act*, will see another step-change with respect to international cooperation and offer another powerful tool in the fight against terrorism and child exploitation for intelligence organisations and LEAs.

4.8. As noted above, it is fair to also expect the passage (after consideration of the recommendations recently made by the PJCIS) of the *Identify and Disrupt Bill* in the not too distant future.

4.9. Particularly the latter three pieces of legislation (*Assistance and Access Act 2018, International Production Orders Act 2021* (and any associated agreements) and the *Identify and Disrupt Bill*) provide LEAs and intelligence organisations with far-reaching and intrusive powers to access any network, system, device, account etc. covertly and, where required, with the assistance of the service provider. Providers may be also required to develop capabilities (where those do not exist) to facilitate intelligence gathering activities for agencies, should this be requested. To put it simply, in our view, the nature of the existing pieces of law (and those we expect soon to exist), do not indicate that there is any need for further intrusive powers for intelligence and enforcement agencies. We are concerned that any further powers, particularly directed at encryption, will not strike an appropriate balance between preserving the technological environment that our digital societies (including our privacy) depend on and powers for intelligence and enforcement agencies.

4.10. Recent media reports have indicated that Australian LEAs continue to use a range of techniques – both technological solutions and human intelligence – to continue vital law enforcement work even when devices or applications are encrypted.

4.11. We recognise that this Inquiry was initiated by the Committee. It would, therefore, be helpful to understand if the Committee is aware of a gap in LEAs' capabilities relevant to the communications sector and has any suggestions as to how those could be addressed been raised. We would also be helpful if LEAs could make specific suggestions for sub-sections of our sector as to what additional forms of assistance they require that are currently not available. It would be reasonable to assess the effectiveness of recent (and forthcoming) expansions in law enforcement powers before making any recommendations about further expansions.

5. Conclusion

The Associations look forward to continued engagement with the Committee and other relevant stakeholders on this important topic.

Our members will continue to assist intelligence organisations and LEAs wherever possible and technically feasible to eradicate, to the extent possible, any material relating to child exploitation and terrorism and to minimise the detrimental effects on all parties involved.

For any questions relating to this submission please contact [redacted] on [redacted] or at [redacted].

Published by:
COMMUNICATIONS
ALLIANCE LTD

Level 12
75 Miller Street
North Sydney
NSW 2060 Australia

Correspondence
PO Box 444
Milsons Point
NSW 1565

T 61 2 9959 9111
F 61 2 9954 6136
E info@commsalliance.com.au
www.commsalliance.com.au
ABN 56 078 026 507