INTERNET ASSOCIATION OF AUSTRALIA LTD
ABN 71 817 988 968
ACN 168 405 098
PO Box 8700
Perth Business Centre WA 6849
Phone: 1300 653 132

09 October 2025

To the Committee Secretary
Parliamentary Joint Committee on Law Enforcement

PO Box 6100
Parliament House
Canberra ACT 2600

By submission:
https://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Law_Enforcement/CombattingCrimeServices

RE: Combatting Crime as a Service Inquiry

The Internet Association of Australia Ltd (**IAA**) thanks the Parliamentary Joint Committee on Law Enforcement (**Committee**) for the opportunity to respond to its inquiry on Combatting Crime as a Service.

IAA is a member-based association representing Australia's Internet community. Our membership is largely comprised of small to medium sized Internet service providers within the broader telecommunications industry. We are therefore keenly interested in the Inquiry as our members play a key role in enabling Australia's digital infrastructure, which is increasingly exploited by malicious actors engaging in Crime as a Service (**CaaS**) operations. Furthermore, many of our members are subject to the electronic surveillance legislative regime, including the lawful intercept framework which are critical to law enforcement's ability to combat CaaS. Thus, from the outset, we express our interest in contributing to regulatory reform to ensure policy settings are proportionate and practical to effectively combat CaaS but also uphold principles of privacy and technical feasibility and does unduly burden industry. Our response primarily focuses on the below terms of reference:

a. the nature and impact of these and other technology-driven advancements on criminal methodologies and activities, including the use of cryptocurrencies;
d. whether the existing legislative, regulatory, and policy frameworks to address these and other evolving criminal methodologies are fit for purpose;

Telecommunications networks vs OTT services

Firstly, we note the complexity of CaaS whereby malicious actors are exploiting the complexity of the various layers of the digital ecosystem, and thus the need to clearly distinguish between the telecommunications infrastructure layer and the over-the-top (**OTT**) application layer. While CaaS exploits underlying telecommunications networks such as via caller ID and SMS spoofing, or the operation of Distributed Denial-of-Service attacks, we also note that CaaS heavily relies on OTT services which operate at the application layer over the internet.

Importantly, in contrast to telecommunications networks, these OTT services are often unregulated or under-regulated, sitting outside of many of the legislative frameworks that seek to address cybercrime such as the *Telecommunications (Interception and Access) Act 1979*. We note the added complexity due to the often global nature of these OTT services complicating data access arrangements, as well as the existence of technical limitations due to end-to-end encryption. Thus, telecommunications providers are often bearing responsibility for complying with law enforcement requests despite having limited control or visibility into activities occurring in the application layer.

We consider this an important technical distinction that has regulatory implications, especially as it affects the effectiveness and efficiency of law enforcement efforts, as well as undue compliance burdens for the telecommunications industry.

We therefore recommend clearer delineation between the regulatory obligations for telecommunications providers and OTT providers to prevent misaligned regulatory frameworks and ensure proportionate, effective and efficient law enforcement action that properly addresses cybercrime occurring at the application layer.

Data retention regime

In today's increasingly digital age, much of CaaS focuses on exploiting data, including personal information of individuals. While we acknowledge valuable work that has been undertaken in recent years to better ensure data protection, including the recent review of the Privacy Act by the Attorney General's office, we are concerned about the complexity of data retention requirements across various legislative frameworks which we consider to be a key factor that drives over-retention of data by entities, and therefore poses greater vulnerabilities to cyber-attacks.

This issue is even more pronounced for small businesses, who often lack the resources to navigate the complex legislative instruments that establish various data retention requirements, to adopt practices and processes that minimise data collection, and promptly dispose of data. While the recommendation arising from the Privacy Act Review was to remove the small business exemption, we do not believe this will have the intended outcome, as it will introduce yet further regulatory burdens.

Rather, we consider it paramount that the government conducts a comprehensive data retention regime review to properly identify the various data retention requirements pertaining to each of an entity's business units and activities. While we understand that a targeted consultation was held in early 2025 as part of a data retention review by the Departments of Home Affairs and Attorney General, we note that no outcomes or details of its progress has been published, nor was the review comprehensive enough due to its limited scope which excluded state and/or territory legislation, international data sharing arrangements, and limitation periods for litigation.

IAA thus recommends the prioritisation of a comprehensive review of data retention laws and other schemes that may necessitate or justify data retention, with a view to consolidate and streamline laws and will assist entities to practice data minimisation and prompt data destruction or de-identification.

Harmonised regulatory reform

Furthermore, we consider it necessary to harmonise regulation and streamline regulations relevant to law enforcement's efforts to combat CaaS. In particular, we consider it extremely important that

any regulatory reform that is embarked on as a result of the Inquiry is harmonised with the overarching electronic surveillance reform currently underway.

We note that the Department of Home Affairs has been undertaking a major reform of Australia's electronic surveillance framework since 2021. We further note other important regulatory reform work that is currently ongoing, or has been conducted recently, including the recent review by the Independent National Security Legislation Monitor into the extraordinary powers under the *Surveillance Legislation Amendment (Identify and Disrupt) Act 2021*, expansion of the Security of Critical Infrastructure regime in relation to the telecommunications sector, the *Scam Prevention Framework Act 2025* and the overarching 2023-2030 Australian Cyber Security Strategy which is now approaching Horizon 2.

We consider the current regulatory landscape to be overly complex and increasingly difficult for industry to comply with. The Committee should recommend a comprehensive review of the various legislative frameworks to harmonise and streamline regulation relating to cybercrime, scam prevention, lawful intercept and other electronic surveillance regimes. A more coherent regulatory environment would enable both law enforcement and industry to operate more effectively and efficiently in preventing and responding to technology-enabled crime.

Privacy and encryption

As the Committee considers regulatory reform actions to better address CaaS, including obligations for OTT service providers as discussed above, we emphasise that any reform should uphold the fundamental principles of privacy, data protection and strong encryption. While lawful access is important for law enforcement, we strongly oppose any laws that would create systemic vulnerabilities or undermine end-to-end encryption. It is vital that regulatory frameworks appropriately balance security and privacy to maintain public confidence in the digital ecosystem. **We therefore recommend that any legislative reform in response to evolving criminal methodologies explicitly safeguard encryption standards and privacy rights.**

Once again, IAA appreciates the opportunity to contribute to the Parliamentary Joint Committee on Law Enforcement for the opportunity to respond to its inquiry on Combatting Crime as a Service. As technology continues to evolve and the digital ecosystem continues to expand, we understand that so too will malicious actors. Thus, IAA and our members, as part of the telecommunications industry which enables the digital ecosystem, reiterate our commitment to working with Government and law enforcement to combat CaaS which is threatening Australian individuals and businesses, and our ability to safely and confidently use digital services. We look forward to continue contributing to a fit-for-purpose regulatory regime that effectively and efficiently addresses CaaS, while appropriately safeguarding privacy rights, robust technical standards, and proportionate compliance to ensure best outcomes for Australia.

ABOUT THE INTERNET ASSOCIATION OF AUSTRALIA

The Internet Association of Australia (IAA) is a not-for-profit member-based association representing the Internet community. Founded in 1995, as the Western Australian Internet Association (WAIA), the Association changed its name in early 2016 to better reflect our national membership and growth.

Our members comprise industry professionals, corporations, and affiliate organisations. IAA provides a range of services and resources for members and supports the development of the Internet industry both within Australia and internationally. Providing technical services as well as social and professional development events, IAA aims to provide services and resources that our members need.

IAA is also a licenced telecommunications carrier and provides the IX-Australia service to Corporate and Affiliate members on a not-for-profit basis. It is the longest running carrier neutral Internet Exchange in Australia. Spanning seven states and territories, IAA operates over 30 points of presence and operates the New Zealand Internet Exchange on behalf of NZIX Inc in New Zealand.

Yours faithfully,
Internet Association of Australia