Submission to the Parliamentary Joint Committee on Law Enforcement: Inquiry into Crime as a Service and Technological Impacts on Law Enforcement

Date: Monday, 13th October, 2025

Contact: Private submission, please see email address attached separately.

Executive Summary

This submission responds to the Parliamentary Inquiry into Crime as a Service and the technological challenges facing Australian law enforcement. It argues that the central issue is not a lack of data or capability, but a misalignment between digital policy, privacy law, and trauma-informed governance. Expanding surveillance powers will not prevent crime; rather, it risks breaching existing privacy frameworks and undermining public trust. The submission highlights the need for evidence-based, proportionate, and ethically grounded approaches that balance security with human rights. It recommends investment in digital forensics training, cross-jurisdictional cooperation, decentralised system design, and the integration of psychological safety and trauma-informed principles into all future cybercrime and data legislation.

Statement of Interest

I submit this statement as an independent professional working within the fields of psychological insight, digital ethics, and human behaviour. My interest in this inquiry arises from direct experience with technology-enabled harm, digital identity abuse, and systemic gaps in Australia's law enforcement and privacy frameworks. My perspective combines lived experience with analytical understanding of surveillance systems, trauma-informed governance, and digital policy.

Overview

Australia's proposed approach to "technology-driven crime" risks expanding surveillance powers without addressing the long-standing deficiencies in enforcement and data governance. The issue is not a lack of information but a lack of capability, proportionality, and accountability within existing systems.

Existing Data Architecture

Australia already operates one of the most integrated civilian data ecosystems in the world. The Single Touch Payroll network links employers, the Australian Taxation Office (ATO), and superannuation funds in real time. My Health Record aggregates national health data under a single identifier, automatically capturing GP, pathology, and prescription records. The Data Availability and Transparency Act 2022 authorises data sharing among more than 500 Commonwealth and State entities for "public-interest purposes."

Telecommunications metadata—including location, IP addresses, and call logs—is retained under the Telecommunications (Interception and Access) Amendment Act 2015, accessible to more than twenty government agencies without warrant. Commercially, a Ghostery 2024 audit found that major Australian news and retail websites load an average of 35–50 third-party tracking scripts per page, including Google Analytics, DoubleClick, Meta Pixel, and TikTok Tracker. Smartphones further transmit continuous geolocation, accelerometer, and biometric data via default system

services such as Google Play Services and Apple Health. These telemetry feeds are routinely stored in U.S. cloud regions governed by the CLOUD Act, allowing compelled foreign-government access.

In this context, the claim that Australia lacks sufficient data is demonstrably false. What is missing is secure architecture, analytical capability, and enforcement capacity—not visibility.

Centralisation and Vulnerability

Consolidating medical, financial, and personal records into a single repository magnifies systemic risk. A single breach could expose the entire life profiles of millions of citizens. True public safety requires decentralisation, end-to-end encryption, and data sovereignty, not further aggregation into offshore-managed systems that expand both exposure and liability.

Enforcement, Not Information, Is the Gap

Evidence shows enforcement failure, not informational scarcity. The AFP Cyber Command reported in 2023 that fewer than two percent of cyber-crime complaints submitted through ReportCyber resulted in prosecution, citing a shortage of skilled investigators and backlogs in case processing. The Victoria Police Digital Forensics Unit reported an average 14-month delay for device examinations in 2022.

Communities such as Malvern, Victoria, highlight these gaps: despite extensive home-security networks and video evidence, residents experience ongoing break-ins while police lack the capacity to respond. Victims of technology-facilitated domestic abuse face the same neglect. Agencies already hold the information required to identify offenders but lack the training, coordination, and resources to act.

Jurisdictional and Technical Limits

Digital crime is inherently borderless. Offenders targeting Australians often operate abroad through decentralised networks such as Tor, a peer-to-peer anonymity system active since 2002. Centralising domestic data cannot overcome these jurisdictional limits. In my own case, a cyber-crime traced to the United States required direct liaison with Californian law enforcement because Australian police lacked both jurisdiction and expertise. International cooperation frameworks exist, but they remain under-resourced and under-trained.

Burden of Proof on Victims

Current practice places the evidentiary burden on victims to prove that they have been hacked or impersonated—an unrealistic expectation without forensic tools or specialist assistance. Even when evidence is supplied, agencies frequently lack digital literacy or trauma-informed procedures. A system unable to act on existing evidence should not be granted expanded surveillance powers over the population it already fails to protect.

Institutional Misunderstanding of Digital Abuse

Victims reporting digital tracking or hacking by known individuals are often dismissed as paranoid. Yet purchasing personal information through the dark web or compromised databases is simple and inexpensive. Digital coercion and stalking are recognised forms of abuse, but law-enforcement training and policy remain inadequate. Expanding surveillance powers within a system that lacks even foundational understanding of these harms will not enhance public safety.

Psychological and Social Consequences

Framing mass surveillance as a mechanism of public safety establishes a precedent of state-induced hypervigilance. Continuous monitoring conditions individuals to exist in a prolonged state of perceived threat, a psychological response recognised in trauma frameworks (DSM-5) as impairing cognitive functioning, emotional regulation, and long-term wellbeing. The cumulative effect of such measures is the erosion of public trust and civic engagement, undermining the legitimate objectives of safety and social order that these interventions purport to achieve.

Current legislative conceptions of safety are legally and psychologically incomplete, failing to integrate trauma-informed principles or acknowledge psychological security as an element of public welfare. In governance terms, this omission conflicts with the intent of the Public Governance, Performance and Accountability Act 2013 (Cth), which requires Commonwealth entities to act ethically, manage risk effectively, and promote the wellbeing of the Australian public. It also runs counter to the Charter of Human Rights and Responsibilities Act 2006 (Vic) and equivalent human rights instruments that enshrine the rights to privacy, dignity, and protection from degrading treatment.

Under established human-rights jurisprudence, including Article 17 of the International Covenant on Civil and Political Rights (ICCPR), any limitation on privacy must pursue a legitimate purpose, be demonstrably necessary, and remain proportionate to the harm it seeks to prevent. Policies that induce sustained hypervigilance or the perception of surveillance fail this proportionality test by inflicting psychological harm disproportionate to their stated objectives.

Trauma-informed governance requires that state interventions minimise re-traumatisation, coercion, and the persistent perception of monitoring. Genuine safety therefore demands the integration of both physical protection and psychological integrity, ensuring citizens can live free from undue intrusion, coercion, and perpetual observation.

Legal and Ethical Contradictions

The proposed expansion conflicts with the Privacy Act 1988 and the Australian Privacy Principles, particularly APP 3 (limiting collection to necessity) and APP 11 (requiring secure handling of information). It also raises concerns under Article 17 of the International Covenant on Civil and Political Rights, which prohibits arbitrary interference with privacy. The principle of proportionality demands that any intrusion be necessary, evidence-based, and the least intrusive means available. Australia has already exceeded that threshold through its current data-retention and sharing frameworks.

International Context

Comparable jurisdictions have already recognised that expanding surveillance powers alone does not prevent technology-enabled crime. The European Union's General Data Protection Regulation (GDPR) and the United States' state-level privacy and cybersecurity laws emphasise encryption, data-minimisation, and accountability over mass data collection. International cybersecurity strategies now prioritise decentralised architectures and privacy-by-design principles rather than centralised information repositories. Australia should align with these evidence-based practices and focus on secure-system design, cross-border cooperation, and technical capacity-building rather than expanding domestic data retention.

Cryptocurrency and Misrepresentation of Risk

The inclusion of cryptocurrency within the scope of "technology-enabled crime" conflates a financial innovation with criminal misuse. Cryptocurrency itself is a financial technology, not a criminal one. While offenders may exploit decentralised networks or private wallets to obscure activity, the same principle applies to any technological medium historically used for crime—including telecommunication systems, banking networks, and even postal services. The tool is not the threat; the misuse of it is.

Criminal actors will continue to adapt to emerging technologies faster than regulatory frameworks can evolve. Expanding surveillance or restricting technological freedom does not eliminate risk—it merely displaces it. The appropriate response is to strengthen law enforcement capability, international cooperation, and digital forensic expertise, rather than extend surveillance to lawful users and innovators.

Australia already possesses comprehensive oversight through AUSTRAC and the Anti-Money Laundering and Counter-Terrorism Financing Act 2006 (Cth), which regulate digital currency exchanges and mandate reporting obligations. Calls for additional surveillance powers on this basis are therefore neither necessary nor proportionate and risk penalising compliant sectors while doing little to prevent sophisticated cybercrime.

Conclusion and Recommendations

If the Government is serious about addressing technology-enabled crime, focus must shift from data accumulation to capability. Investment should prioritise:

- expanding and training the digital-forensics workforce;
- implementing genuine end-to-end encryption and privacy-by-design standards across all existing systems;
- establishing trauma-informed victim-support programs; and
- introducing transparent, independent oversight to rebuild public confidence.

Australia faces a trust deficit, not a data deficit. Real safety will arise from competence, enforcement, and respect for privacy—not from further centralising the personal information of its citizens within networks already proven insecure.