[redacted]

From: [redacted]
Sent: Friday, 12 November 2021 12:15 AM
To: Committee, PJCIS (REPS)
Subject: submission: Review of Administration and Expenditure No. 20 (2020–21) – Australian Intelligence Agencies

Categories: [redacted]

to the committee,

Addressing emerging technologies, initiatives and their threats to domestic security. Recalling historical security events involving sensitive cartographic information repositories and publicly owned surveillance equipment. Investment in the development and deployment of power usage watchdog technologies would mitigate the attractiveness of their exploitation by providing an early warning system.

Emerging threats to the obscurity of domestic intelligence operations and the consequent safety of personnel and integrity of investigations posed by the liberalization of artificial intelligence technologies threaten to render covert operations transparent. The proliferation of processing intensive applications simultaneously obscures the footprint of malicious tasks.

The lack of legislated privacy protections in step with technological development renders agents of the state heavily exposed to adverse surveillance with the excuse of aiding the sale of consumer products or productivity.

Over-reliance on AI technology is likely to occur while diminishing human resources but Microsoft's Tay AI would be an important cautionary tale. Similarly, the Christchurch Massacre report revealed intelligence failures that were attributed to the individual's ability to present in a way that allowed them to be ignored. Both examples present an important lesson on the vulnerabilities of learning systems..

Robert Heron
[redacted]