# Submission No 14

## Inquiry into potential reforms of National Security Legislation

**Name:** Andrew Butcher

**Organisation:** Private Capacity

To whom it may concern,

I am writing in response to the reform proposals to the Telecommunications (Interception and Access) Act 1979, the Telecommunications Act 1997, the Australian Security Intelligence Organisation Act 1979 and the Intelligence Services Act 2001, as outlined on the APO website here: http://apo.org.au/call/inquiry-poten...ty-legislation.

As an Australian citizen I am seriously concerned about the over-reaching changes proposed by this reform, I have outlines a few of my concerns below I have with the plans laid out within the document "EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS"

**From Chapter 2, 1, page 13, EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS**

*Establishing an offence for failure to assist in the decryption of communications.*

Given the points below it is no unreasonable to assume that if this law is passed it will result in innocent parties receiving harsh penalties.

1. It is impossible to determine if a person charged with decrypting a data file is either unable to do so or unwilling to do so. It is widely excepted in the IT field that forgetting a password is very common place.[1]
2. It is impossible to know the contents of an encrypted data file without first decrypting it. If the opposite was true then decryption would not be necessary.
3. Without knowing the contents of a data file it is impossible to determine the relevance of that file to national security.

*1. Password reset requests make up 10% - 30% of help desk calls*

*Study Title: Password Reset: Self-Service That You Will Love (Gartner Research Note T-15-6454)*

**From Chapter 2, 1.2, page 15, EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS**

*While terrorism is a key issue, the ASIO Report to Parliament 2010-11 notes that espionage is an enduring security threat to Australia, both through the traditional form of suborning persons to assist foreign intelligence agencies and new forms such as cyber espionage. Nation states, as well as disaffected individuals and groups, are able to use computer networks to view or siphon sensitive, private or classified information for the purpose of espionage, political, diplomatic or commercial advantage. As the actors involved undertake this activity within 'cyberspace', the lawful interception of their communications is often a crucial aspect of any investigation aiming to resolve the nature of the activity and the identity of the perpetrators.*

The legal obligation of CSPs to store data transmitted over their network may be used by said "Nation states, as well as disaffected individuals and groups" to further the very goals you are trying to prevent with this new legislation. While there is provision in this legislation reform to regulate the security level of a CSP this does not guarantee that the data can't be accessed, even government systems are not immune to attacks[1].

[1] http://www.hacklabs.com/ausecdb/

**From Chapter 4, 3.2, Page 48, EQUIPPING AUSTRALIA AGAINST EMERGING AND EVOLVING THREATS**

*Subsection 25A(5) currently restricts ASIO from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons. This prohibition operates regardless of how minor or inconsequential the interference, interruption or obstruction may be.*

*To address this, section 25A could be amended so that the prohibition does not apply to activity proportionate to what is necessary to execute the warrant.*

I have several issues with this amendment

1. Adding or modifying data on a target computer system calls into question the validity of data retrieved and used for later prosecution as data might not be in its original form.
2. It is very open for abuse and relies persons within ASIO and associated bodies following regulations, there are several examples of corruption within the Australian government so it would be ignorant that it could not happen[1, 2], an agency may plant data on a suspect's computer or even plant an encrypted file which they could requested the suspect to decrypt and prosecute based on non-compliance.
3. Acts that may disrupt a target computers operation may hamper legitimate business operations and cause undue harm to said business.

1. http://govnetconference2006.anu.edu.au/papers_etc/bartos.pdf
2. www.opi.vic.gov.au/file.php?61

In closing here is a saying from Benjamin Franklin that is very pertinent to ever increasing reduction of personal privacy in today's society.

**They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety.**

- as published in *Memoirs of the life and writings of Benjamin Franklin* (1818).