Submission No 129

Inquiry into potential reforms of National Security Legislation

Organisation: Ms Deborah Pickett

Sent: Monday, 20 August 2012 1:09 PM
To: Committee, PJCIS (REPS)
Subject: Inquiry into potential reforms of National Security Legislation

After going through the terms of reference in the discussion paper, I feel neither safe nor secure.

The government is pursuing powers that it does not need. The cavalier approach set out in the paper barely mentions safeguards to protect citizens from misuse.

There is no talk of preventing scope creep. Today, terrorism and child exploitation. Tomorrow, BitTorrent and whistleblowers? If the government does not intend to extend the scope, it should come out and say so.

There is no talk of accountability, for how to prevent corruption, misuse and just plain careless loss of these troves of data by government organization staff. A data breach is forever; so should be the punishment for staff who cannot protect my data.

The suggestion that it be permitted for security staff to break into my equipment in the course of their duties leaves me speechless. I will consider unauthorized access to my computers an assault, and if I find any hardware keyloggers on my equipment I will detach them and feed them false keystrokes for my amusement. Or maybe sell them on eBay, or put a teardown on iFixit.

To make it an offence for me to not provide a password for encrypted material is insane. It is essentially legitimizing "rubber hose" cryptanalysis. Not only might I legitimately not remember the password, it makes a mockery of protections such as of a journalist's sources. Worse, a determined staff member bent on my destruction, can declare any random data to be "password protected" and insist that I hand them the nonexistent password.

These provisions give the government the power to single out any troublemaker and assassinate their character. I will oppose them in any way I can.