Submission No 30

Inquiry into potential reforms of National Security Legislation

Name: C Eden

Organisation: Private Capacity

From: C Eden
Sent: Tuesday, 24 July 2012 3:32 PM
To: Committee, PJCIS (REPS)
Subject: Proposed New Internet Security Reforms - sub 30

Dear Joint Parliamentary Committee on Intelligence and Security,

I am writing to you regarding the **proposed new internet security reforms** mentioned by Ms Roxon. Some of the changes which have been reported do not sound particularly good for the welfare of Australian citizens.

**I do not agree with forcing ISPs to retain user data for two years. It is a privacy concern, this would allow the creation a personal profile on someone as if they were a criminal. It is also a privacy concern when the client does not know who will have access to this collection *(for one eg; ISP staff)* as well as security measures where it is stored. The client will also not know when their data has reached the two year mark and thus have to rely on the ISP to dispose of or continue recording data from an individual.

**I do not agree with 'wiretapping' and spying on Facebook accounts, Twitter and other social media. Citizens pay to use the internet, buy their own hardware and can use it in their own home where it is their business how they conduct their conversations, personal lives. Again, I do not agree with the surveillance and data analysing that would normally be reserved for those in the middle of a criminal investigation.

** Frankly, I am a little disturbed with the Australian Government's suggestion that ASIO be allowed to "plant material" on people's computers, destroy material and also go through a *third party* to do this. I feel this is a gross violation of a citizen's right to privacy and also to control how *their own property* is being used. It also allows for any corrupt personnel to set citizens up.

**I am concerned at the proposed changes that wish to allow ASIO personnel to break the law while undercover. I do not believe just because you have a badge or authority that you should be able to break the law and entrap others while you can commit crimes with no responsibility. The opportunity to flout this would be very hard to resist. (see above point)

**Considering to make criminal refusing to cooperate with government decryption attempts, eg: charging citizens or jailing them for refusing to give their password is like a police officer going to someone's door without a warrant. It is a violation of the rights of the individual if the police were to enter without permission. Through forensic computer science, once a suspect's computer

is confiscated for investigation, any passwords and deleted materials can be restored by law enforcement if they need.

**** Enabling non-ASIO intelligence agencies to work with ASIO is allowing foreign bodies to have a say on how Australian taxpaying citizens are processed if they are suspected of committing a crime. If citizens live in this country under Australian law they should be investigated by Australian law enforcement and agencies.

****Prosecution for naming an ASIO officer . If an agency breaks into your computer and you are aware, there should be nothing wrong with saying so. I do not think it is right to shut citizens up if they are experiencing disappointment with the way the Australian Government and other agencies are conducting themselves.

I urge you to take in account the concerns I have raised as I am not alone on this issue in this county.

-C. Eden