Submission No 136

Inquiry into potential reforms of National Security Legislation

Organisation: Kendall Lovett and Mannie De Saxe

Sent: Monday, 20 August 2012 4:53 PM
To: Committee, PJCIS (REPS)
Subject: National Security Legislation Inquiry

To: The Committee Secretary,
Joint Parliamentary Committee on Intelligence and Security,
Parliament House,
Canberra, A.C.T. 2600.
Email: picis@aph.gov.au

Friday, 17 August 2010.

From: Kendall Lovett and Mannie De Saxe,

SUBMISSION

To the **Inquiry into potential reforms of National Security Legislation.**

We wish to draw the attention of the Committee to our concerns about the possible threat to the Australian public's democratic rights to privacy, freedom of expression and the presumption of innocence should the matters outlined in the *Discussion Paper* be approved.

It seems to us that, even though there have been rapid changes in the telecommunications environment, aligning industry interception assistance with industry regulatory policy by extending the regulatory regime to ancillary service providers not currently covered by the legislation (page 13) this provides the Government and its security intelligence agencies with almost unlimited power.

Figures quoted (page 14) of the number of arrests made by law enforcement agencies as 91, prosecutions as 33 and convictions as 33, sound impressive for the twelve months 2010 to 2011. Apparently, all 91 arrests were based on evidence obtained under stored communications warrants. Therefore, it follows that the current laws are very efficient and obviously workable.

One has to wonder how much of this apparent need by the Government and its agencies for greater power is allied to the shared security intelligence with the government of the United States of America. A Cyber Intelligence Sharing and Protection Act which is still under consideration there, would allow companies doing business in the US to collect exact records of all on line activities and hand them over to the US Government, without ever notifying its citizens that they were being watched. It seems that such an Act would provide a government and corporations with blanket immunity to protect them from being sued for violation of privacy and other illegal actions. It's like giving the government a blank cheque to monitor its citizens' every move.

If carriage and carriage service providers (C/CSPs) are providing such a supportive service to the Government and its intelligence agencies currently, why extend it to other providers such as social media and ISPs? We think the answer is obvious in the last couple of word in the last sentence on page 27 *–to better position Australia to meet domestic and* ***international demands.***

According to the Analysis (page 33), the Australian Government believes that the telecommunications industry is not fully informed about national security risks and therefore not equipped to respond adequately to these risks. So it says it has a responsibility to intervene in the market to educate and assist carriage and carriage service providers to maintain a minimum level of security for the purpose of protecting the data on their networks. To do this, the Government has a plan to require C/CSPs to provide it, when requested, with information to assist in the assessment of national security risks to telecommunications infrastructure; and *powers of direction and a penalty regime to encourage compliance.* Sounds very much like 'handing over exact records of online activities.'

In totalitarian states, such as Germany, Italy and Russia during World War Two, citizens were able and required to spy on their neighbours and families and report them to the authorities if they thought they were not complying with the requirements of the state. These proposals would indicate that the Australian Government intends introducing legislation which would have the same result.

It's the hidden messages in this *Discussion Paper* which are of concern. There's the latent but unrealised ability here to turn all citizens into suspects. There is, too, the distinct possibility of doubling, even tripling, those other statistics (2441 arrests) based totally on intercepted material (page 14). Misconstrued comments and actions on a pre-paid service such as a mobile phone, email, or twitter etc by innocent people would put them *at risk* of arrest, incarceration and interrogation at a secret location without access to legal assistance if many of these new powers were approved.

We urge the members of the Committee to carefully consider the ramifications of these powers that are being presented as necessary by the Government and take into full account Article 19 of the Universal Declaration of Human Rights: *Everyone has the right to freedom of opinion and expression; this right includes freedom to hold opinions without interference and to seek, receive and impart information and ideas through any media and regardless of frontiers.*

Signed: Kendall Lovett and Mannie De Saxe.