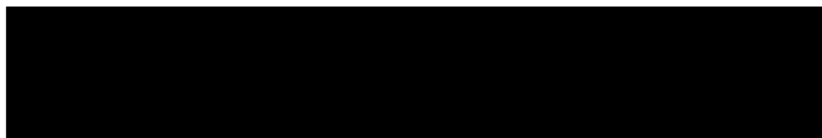




**Submission No 93**

**Inquiry into potential reforms of National Security Legislation**



---

**Sent:** Monday, 20 August 2012 1:40 AM  
**To:** Committee, PJCIS (REPS)  
**Subject:** National Security Inquiry - Needs serious rethinking

Submission against proposed changes to national security laws.

To whom it may concern,

I am extremely concerned with the proposed changes to national security laws. These proposed changes are outrageously broad and allow almost any type of online malicious activity to take place. I have faith in the men and women in our ASIO team, whom I'm sure hold the highest standards of professionalism in the protection of the Australian people, but unfortunately as we all know there are always bad apples, and these laws WILL be misused.

One of the most frightening aspects is what constitutes a 'third party' to a potential online criminal. At the moment, the broad definitions in the proposed laws make almost any individual a third party, as long as the device has had even the most insignificant indirect connection with the potential criminal's device. It seems the law intends to make all users a potential third party, making everyone on the internet a suspected criminal.

Another major concern is the lack of clarity over how the ability to both add and delete data from a citizen's device will be managed. To not have the most strict standards over this kind of power is reckless. The idea that an innocent third party or even a potential criminal can have data placed into their device is extremely serious. Again, these laws WILL be misused eventually, and we will be seeing innocent people being charged of crimes or even sent to jail. We have already seen unnecessary interference with innocent Australian's Twitter and Facebook accounts. These laws are not acceptable in a liberal democratic country.

One of the most important factors is the security of the stored information. We already know for a fact that even the most 'secure' organisations worldwide are easily capable of having this information hacked and stolen for private use. The government has no safe way of storing this data, despite any arguments to the contrary. The very idea that in modern Australia I am now having to consider whether I can trust our secret intelligence organisation with my private communications is insane. This is an insult to any citizen living in a democratic society.

These laws are also a direct attack on free speech. When people know their communications are being stored for potential investigation, they are unable to communicate freely with confidence. We do not need people whispering in the shadows.

What is to become of journalism and the media, if those in the industry are aware that they can no longer promise anonymity to a source. Social media has become an important tool for those in the media, and if people are aware that the government has access to all these communications, it would interfere with the way many journalists choose to approach their stories. The protection of journalism as a practice, with its role as the Fourth Estate, is one of the most precious institutions and must be protected from any new laws.

Now I'm sure there are many in government who chuckle at the hysteria these laws have created, but those who are aware of the evolution of similar policies over the past decade in America know there is nothing

more serious. Post 9/11 saw many changes in American policy, from rapid changes to the NSA and bills such as the Patriot Act. These changes have allowed complete surveillance of all telecommunications across the nation, and have had terrible impacts on many of its citizens, especially those who chose to question such powers. We have seen people detained at airports for significant lengths of time without charge, as well as innocent citizens charged with serious crimes against the state. Consider the cases of former NSA employees turned whistleblowers William Binney and J. Kirk Wiebe.

Lastly, despite the idea of separating the 'online' and 'offline' world, this is misleading. The internet is reality, and this level of surveillance is not legitimate, state endorsed or not. I see no difference to making it legal for ASIO officers to storm into my house at will to read my diary or copy my phone contacts.

“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.”

**Article 19 of the Universal Declaration of Human Rights**

1. No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation.

2. Everyone has the right to the protection of the law against such interference or attacks.

**Article 17 of the International Covenant on Civil and Political Rights**

Regards,



