Submission No 138

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Steve Versteeg

20 August, 2012

Re: Submission to Parliamentary Committee in Response to the Public Discussion Paper - "Equipping Australia Against Emerging and Evolving Threats"

Dear Honourable Members of Parliament,

Thank you for inviting me to submit to the National Security Inquiry.

On a recent visit to Canberra, when I saw the size of new ASIO building, I thought to myself: "Wow, I didn't realise Australians were such a big threat to themselves." In a similar vain, the proposed vastly expanded powers of Australia's intelligence agencies are a disproportionate response to the ill-defined "new and evolving threats". While there is no doubt that laws need to be updated to reflect the new communication technologies being used, the proposed changes represent a massive expansion of the powers which currently exist - by greatly increasing the amount of monitoring and lowering the barrier to how that information may be accessed and by whom. Logging and archiving for 2 years every private communication and every click made on the Internet by every citizen is unacceptable in a democratic society. This would represent an erosion of the privacy and freedoms of ordinary citizens.

My principle objections to the proposals outlined in the public discussion paper are as follows:

- It will subject every Australian citizen to data mining of their private communications and profiling by Australia's security agencies. Given the amounts of data that will be produced, it is self-evident that automated data mining systems will need to be used. However, these automated systems are notorious for producing false positives (and false negatives). As a consequence of using these automated systems, there is a risk that innocent people will be misclassified as security risks by ASIO, which would have a detrimental affect on these people's lives (e.g. having trouble flying etc.)
- Giving government agents access to the private communications of law-abiding Australian citizens is an invasion of privacy. There is something inherently creepy about writing a private message to someone knowing that government officials may also be reading it.

- There is a disturbing trend of creep in what ASIO considers a "threat". It is clear that "threat" already goes beyond monitoring suspected foreign spies, terrorists and organised criminals. There have been disturbing reports published in newspapers that ASIO now also monitors environmentalists, protesters, political activists and whistleblowers. It is important to note that in the historical context, many of the social and political changes which we take for granted today, were radical at the time. For example racial equality was considered a radical idea in the 1960s. By expanding the definition of threat to include anyone calling for radical change, we risk undermining our democracy. Attempts to stifle the free expression of those calling for radical change undermines one of the natural checks to keep our political system from stagnating and being corrupted. The proposed expansion of powers coupled with the trend of what ASIO's existing powers are being directed at monitoring, I believe represent a threat to our democracy.
- It is inevitable that the monitoring data proposed to be collected by ISPs will leak beyond the intended recipients. There is growing evidence that irrespective of any laws and regulations imposed, it is technically infeasible to prevent data leaks completely. Furthermore, the rate of data breaches is increasing. For example in 2011 there were 1041 breaches of personal information reported by companies and organisations, with some breaches affecting tens of millions of customers. The total number of breaches was 29% higher than in 2010, and 600% higher than in 2005. Furthermore, 2012 is projected to be the highest year ever for number of data breaches. (See www.datalossdb.org for more quantitative figures.) On this evidence, it is likely therefore that the personal information collected about people's private communications will leak into the hands of criminals.
- The proposed changes will be ineffective at monitoring the true threats to Australia's security: foreign spies, terrorists and organised criminals. These people will continue to use encryption and anonymisation technologies which make communications impossible to monitor. Furthermore, it is likely that law abiding citizens will also increasingly start to use these technologies, which would actually make the job of security agencies harder.

Rather than expanding the powers of security agencies, any changes in the law should instead focus only on allowing internet communications to be monitored to the same extent and with the same safeguards as currently

apply to phone tapping. That is, a warrant should be required to monitor someone's communications, and communications should not be able to be monitored retrospectively. Monitoring the mouse click of every citizen goes far beyond this. Furthermore, rather than broadening the scope of our security agencies, their scope should instead be refocused on their original intention. ASIO should focus on foreign spies, terrorists and organised criminals - not political activists and whistleblowers.

In conclusion, the proposals in the discussion paper are disturbing. They are unjustified and represent an intrusion into the private lives of law abiding Australian citizens by our security agencies. Furthermore they would be ineffective and have unintended consequences. The proposed changes are in themselves a threat to our democracy and would put Australia on a path towards becoming a totalitarian state.

Steve Versteeg