Submission No 153

Inquiry into potential reforms of National Security Legislation

Organisation: Ms Ashley Hull

Sent: Monday, 20 August 2012 11:33 PM
To: Committee, PJCIS (REPS)
Subject: Edited: National Security Legislation Inquiry Submission

Hello Committee,

I am writing in response to the reform proposals to the Telecommunications (Interception and Access) Act 1979, the Telecommunications Act 1997, the Australian Security Intelligence Organisation Act 1979 and the Intelligence Services Act 2001, as outlined on the APO website here: http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/index.htm

Thank you for the opportunity to provide a formal submission to the national security inquiry. As an Australian citizen, I am seriously concerned about the over-reaching changes proposed by this reform. The proposal is aimed at taking advantage of the ease of which large scale and predictable surveillance is possible in the age of Facebook and our always online social footprints. The laws don't offer me security in providing me the right to a private life, and a presumption of innocence. Guarantees and protections must be met to protect the innocent while granting the law enforcement the ability to prove their cases in court.

People are giving up their privacy to services such as Facebook and Twitter, and these services (and similar) have created an environment were monitoring of the entire country is possible and easy. Ten years ago, this kind of real time details and locational aware services were science fiction and now every single phone with an GPS is connected 24/7 to the internet. J Edgar Hoover would be proud. Yet while I say this, I'm completely aware these technological advancements offer equal easy and opportunity to criminals.

We should be heading in the opposite direction, with security legislation tightening the first and third party companies from storing and sharing these personal details in a secure manner and limiting their exposure. ISPs shouldn't be told to keep data for customers whom have not yet been targeted by law enforcement with an open case and a warrant. As the lines between terrorism, civil disobedience and healthy dissent are deliberately blurred, our rights must be protected from these overarching sweeping reforms which target the select few while touching all of us. We need to ensure there is no room for ambiguity - The crosshair must be aimed precisely.

My right to privacy should be extended online, not taken advantage of due to the ease and bulk of data available about me. The places I visit, webpages I view, articles I read, people I contact, copies of my SMSes and the products I consume should be kept locked with restrictive and tighter security. Monitoring people based on patterns, past interests or poisonous activities will always result in false-alarms. This is an fundamental human rights and piracy issue and I think arguing to support omnipresent surveillance is disruptive to the common good. This reform proposal disregards these rights, is clearly an attempt to remove the last vestiges of personal privacy, the legal presumption of innocence, and introduce overreaching tentacles of an Orwellian hivemind into every aspect of their lives as Australians. The preserved data also creates a security risk of misused and/or publication - How the information is used and mined is also important, this information must not be used for any additional reasons outside of law enforcement within the view of a criminal investigation and not outside of it in any way outside of the case, public citizens must not be profiled. Private companies must not have access to share this information.

I see the proposal by the Australian government as futile and expensive and the argument 'If you have done nothing wrong you have nothing to fear' is disingenuous and short minded. Police powers should be held behind a series of checks and balances, investigators need to build probable cause, judges need to approve surveillance and a case needs to be proven in a court of law. These amendments overshadow how criminals should be caught. Living in a strong and law abiding society assumes the citizens are not guilty until proven innocent.

Focusing on these points raised in the discussion paper. The criminalisation of encryption, the criminalisation of withholding computer passwords and the breech of personal property is a horrible overreach and won't protect anybody. Further, the level of powers suggested here for ASIO are far beyond what I would consider ‘reasonable’. No-one would allow a bill to pass that allows a federal agent to have a ‘master key’ for everyone’s homes where they could enter the premises and remove, change or even leave new documents or other material in their homes without their permission or knowledge, yet this reform is attempting to achieve the electronic equivalent and I will not stand for it. This reform seeks to remove accountability from the governing bodies involved, which in itself flies in the face of a democratic government. For the benefits to law enforcement that this would admittedly provide, I do not believe that the sacrifice of privacy that every Australian must make to facilitate the reform is even remotely worth it. I strongly disagree with the reform.

There have been numerous recent events which could be used as examples of the need to restrict data retention and extend the privacy rights online. The existence of Trapwire and similar facial recognition technology is a great example of the kinds of technology which should be banned - This technology echoes something which should be limited and restrictive to police powers let alone by a private corporation.

Regards,
Ashley Hull