Submission No 15

Inquiry into potential reforms of National Security Legislation

Name: Andrew Bartlett

Organisation: Private Capacity

From: Andrew Bartlett

Sent: Wednesday, 18 July 2012 11:34 PM

To: Committee, PJCIS (REPS)

Subject:[SUBMISSION] Very concerned about new intercept powers

I'm writing to you due to my very serious concern about the Government's proposals for expanded intercept powers, and the lack of time for consultation that the Government is permitting on giving our 'security agencies' an incredibly broad range of new powers.

http://delimiter.com.au/2012/07/16/new-surveillance-powers-akin-to-china-iran/

I'm concerned about this on a few levels. The electronic dragnet is very easy to deploy, but very hard to retract. Once agencies become accustomed to intercepting our private communications as a matter of course, they become dependent on it.

We see this for example in the US with:

https://www.nytimes.com/2012/04/01/us/police-tracking-of-cellphones-raises-privacy-fears.html

https://www.nytimes.com/2012/07/15/opinion/sunday/the-end-of-privacy.html

Yet this dragnet is often so poorly targeted - with that article recounting how 'tower dumps' are obtained of every communication with a particular mobile phone tower.

With such broad-brush intercepts, who is looking out for the privacy of everyone not 'of interest'?

Furthermore, even if we trust the security agencies with laser-perfect targeting (which is unlikely, as it is cheaper to just snoop on everyone, and worry about their privacy later), we see this week that simple mistakes mean that even those not of any security interest so easily have their privacy intruded:

http://www.theregister.co.uk/2012/07/16/interception_of_communcations_commissioner_report/

And of course, it isn't only the security agencies who have access to this information, once stored information is too easily accessed. Even AusCERT couldn't safely return private data to the Government.

http://www.illawarramercury.com.au/news/national/national/general/most-embarrassing-blunder-government-contractor-paid-1m-for-esecurity-alerts-service-loses-8000-subscribers-personal-information/2617721.aspx

Given that level of security in agencies with the technical skill and know-how, why should we expect any better in the broad range of agencies that will have these intercept powers? They are not accountable to those who they intercept - indeed they consider that they have done something wrong - so why should we expect a higher level of care?

The same applies to ISPs, who have sadly had a poor record as well. If Telstra can't keep customer private data private, what hope is there that the trove of personal data it would be forced to keep, only for the benefit of the government, would be more secure?

http://www.theaustralian.com.au/australian-it/telecommunications/privacy-commissioner-eyes-telstra-after-telco-sends-customer-data-offshore/story-fn4iyzsr-1226410406053

http://www.zdnet.com/telstras-2011-privacy-bungle-breached-code-1339340561/

We are not at a time of heightened terrorist threat. Why is it so urgent to bring in these powers now, and with such little consultation?

Thanks,

Andrew Bartlett