Submission No 131

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Evan Slatyer

Sent: Sunday, 19 August 2012 8:53 PM
To: Committee, PJCIS (REPS)
Subject: RE: Potential reforms of National Security Legislation

Dear Mr Secretary,

I write in regards to the Committee's Inquiry into potential reforms of National Security Legislation.

The following proposals before the Committee are neither appropriate nor proportionate:

- Page 8, Section 5b - specifically with regards to extending warrants. I think it would be generally agreed that, if there is a risk of a terrorist attack, time is critical. Therefore I do not understand how three months can be too short a time for a search warrant to expire; in fact I'd go as far as saying that if the warrant has not been used for three months, and no additional evidence (eg. an attack) has come to light, then there's a very good chance that the suspects are in fact innocent. Extending this to six months seems ludicrous; if ASIO is unable to deal with warrants within three months then there's a problem with ASIO.

- Page 9, Section 9 - while I agree that modernising the industry assistance framework may be a good idea, the proposed changes are not explained. As such, I would strongly object to any changes until details are made available and comments have been gathered.

- Page 9, Section 10 - while it seems like a good idea to shield individual ASIO agents from legal repercussions (when acting under orders), it is also highly unfair for anyone on the receiving end to be forced to deal with potentially expensive results of actions that were (in hindsight) unjustified. As such, I would suggest that ASIO, rather than individual agents, is held responsible and can be relied upon to pick up the bill.

- Page 10, Section 11c - I would like to see some safeguards here; for example if this "disruption" of a computer costs a company ten million dollars, and it later turns out that the company had nothing to do with any terrorist attack, then ASIO would be required to cover the cost. It seems rather unfair that ASIO could potentially damage a business beyond repair, on little more than a hunch, and then wash their hands of it and continue as before. In engineering terms, this would complete a negative feedback loop with a stabilising effect on ASIO's actions.

- Page 10, Section 15a - This appears to be moving from an "assumed innocence" to an "assumed guilt" platform, in that it is assumed that the user actually has the ability to assist with decryption. I suggest that the government instead invests money in physics research; sooner or later that will produce a quantum computer that renders existing encryption systems useless and requires no cooperation from the user. It will also serve to render other countries' encryption useless (which is a huge win for ASIO) and promote science in Australia (which is a huge public win for the government).

- Page 11, Section 16c - Costs should be borne by providers only when the

providers are at fault. If, for example, the risk is a direct result of the government demanding data be retained for two years, then the government should pay for it.

- Page 11, Section 17b and 17c - I am concerned about this "clarification". The issue appears to be that the existing laws are ambiguous, with one interpretation more useful to ASIO than the other. The intention is to simply change the laws to support the interpretation preferred by ASIO, without considering whether this is the interpretation originally intended. More work is required here.

I will also suggest a system for demonstrating "reasonable force" (as per part 17c). This could take the form of video surveillance of all ASIO employees at all times, with the video to be retained and publicly available (apart from sensitive information) for the usual two year period. Any claims of excessive force could then be easily met with video evidence.

- Page 26 - it is claimed that the "legacy" requirements for record keeping (to show that powers are being used lawfully) are unnecessary due to the accountability framework under which the agencies now operate. I would expect to see a detailed logical analysis showing that every scenario that would be covered by the old requirements will be covered as well, if not better, by the new ones. It is also worth noting that the accountability framework can be changed much more easily than the existing requirements, and therefore replacing the existing requirements with the accountability framework represents a substantial weakening.

Apart from this, I will suggest that data retention by ISPs is impractical and extremely costly. With currently available internet plans and hard drives, ISPs could find themselves purchasing at least one new top-end hard disk per four users per month (current HDDs go up to 4TB, internet plans up to 1TB/month are easily accessible by home users). In addition to the hardware necessary to support this (eg. servers, buildings, etc) and backups necessary to ensure the data is stored for two years, there would be huge outlays in keeping the data secure and available to ASIO. A quick calculation suggests that internet bills would increase by at least 50%, if not more - this largely negates any advantages of the NBN. It is worth noting that Australia has zero local hard disk manufacturers, and that this would tend to result in large economic benefits for American and Chinese companies. With current fears about Chinese companies potentially including "phone home" devices in their products, there is a potential security risk even after the usual hacking is taken into account.

I suggest that a more suitable approach would be for this data to be transmitted directly to ASIO, to be stored as they see fit. ASIO, as Australia's top security experts, will be much better-prepared for handling large quantities of sensitive data. Additional advantages include consistent data organisation (as it is handled by ASIO and nobody else), ready access to the data (it is not unreasonable to guess that record-keeping at some ISPs will be poor), reduced costs to ISPs, and reduced risk of legal threats (eg. from AFACT) in an attempt to access customer data.

As the Committee deliberates on the proposals the government wishes to progress, is considering and others on which it is seeking the Committee’s view, I urge you to uphold and defend the rights of all Australians to privacy and freedom of expression.

I also remind you that in addition to the rights affirmed under the Universal Declaration of Human Rights, Australia supported the 6 July 2012 resolution of the United Nations Human Rights Council. This resolution affirmed that the

same rights that people have offline must also be protected online.

The internet is a vital communications medium that millions of people use to exercise rights to freedom of expression and collaboration. It is already playing a role in building a globally connected civil society, which has become an important part of how we confront the challenges of the 21st century. It is too important to risk with misconceived proposals such as the ones before the committee.

Sincerely,

Evan Slatyer