Submission No 127

Inquiry into potential reforms of National Security Legislation

Organisation: Ms Jessica Smith

August 20, 2012 Jessica Smith

RE: Inquiry into potential reforms of National Security Legislation

Dear Mr Secretary,

I write in regard to the current Inquiry into potential reforms of National Security Legislation. I am very concerned that some of the proposed reforms are over-reaching in their scope and intent. I am also concerned that the submissions process was incredibly brief for an inquiry with complex proposals and terms of reference, and which ranges across the important issues of national security, data privacy, data security, and human rights.

My perspective is that of an IT professional with more than 15 years' experience in system and network administration (including server deployment and hardening), and provision of Internet connectivity and web hosting services.

Because of the short time available for review and analysis of the proposed reforms, I will confine my submission mainly to the proposed reform listed as item 15.c.

Part of the bedrock of our legal system in Australia is the presumption of innocence. There are strict controls over when, and how, search warrants, wiretaps, etc., can be applied for and obtained. There is, rightly so, a burden of proof on law enforcement to demonstrate sufficient grounds for breach of a citizen's right to privacy. Only where there is judicial agreement that there is sufficient cause to breach that right to privacy is the necessary permission granted. This is a system with built-in checks and balances, and with appropriate oversight.

Item 15.c proposes a reform to request or require internet service providers (ISPs) to retain data on their clients—Australian citizens, for the most part—for periods up to two years. Setting aside the relatively trivial issue of cost-of-implementation and a potential requirement for compensation of ISPs, there are several serious issues with such a proposal:

- **This would effectively implement 'round-the-clock surveillance of all Australian citizens, for no clearly-articulated security benefit.**

  Statistics from the ABS about the current prison population clearly show that only a vanishingly small percentage of Australian citizens are ever the perpetrators of crimes, much less serious or violent crimes.[1] The curtailing of the right to privacy of all Australians in the unsubstantiated 'hope' that doing so will lead to prevention of serious crimes is an unacceptable encroachment on human rights. The government, law enforcement agencies, and intelligence agencies have not made a strong case that demonstrates the public benefit

to be gained in exchange for the wholesale breach of the right to privacy for Australian citizens.

There are of course cases in which violation of this right *is* acceptable—and there is already a mechanism by which this can be implemented through application for court orders to permit wiretapping, surveillance, and search. This proposed reform turns the presumption of innocence on its head, replacing it instead with the tacit suggestion that all citizens have something illicit to hide, and need to be monitored.

- **The implied assumption in this proposed reform is that security and privacy are mutually exclusive, and that in order to provide one (security), we must be prepared to sacrifice the other (privacy).**

  The quote attributed to Benjamin Franklin, "They who can give up essential liberty to obtain a little temporary safety, deserve neither liberty nor safety" is practically the touchstone in discussions on security and privacy. Yet it, too, implies that security can be had by sacrificing privacy. This is a false dichotomy, although a useful one for anyone seeking to expand their surveillance powers. If people believe that security and privacy are mutually exclusive, there is a certain inevitability about acceptance of such a tradeoff. However, neither the government, nor any of our law enforcement agencies or intelligence agencies have offered any evidence that security can only be had at the expense of privacy. Unless an extremely strong case can be made that reduction or removal of privacy will result in a real increase in security (rather than simply 'security theatre'), any proposal to encroach on citizens' right to privacy should be dismissed as unwarranted.

- **Requiring ISPs to store—and secure—sensitive information about Australian citizens is a recipe for disaster.**

  ISPs have expertise in providing connectivity services to Australian citizens, businesses, and organisations. The quality of service, and the depth of expertise, varies from ISP to ISP. Further, an expertise in the provision of connectivity does not automatically translate into expertise in data security. Assuming that all the ISPs required to collect, store, and secure data on their clients have the skill and infrastructure required to safely do so is foolhardy, at best.

  Data breaches are an everyday occurrence. Many high-profile companies with significant resources at their disposal are unable to prevent unauthorised access to their core systems.[2] Even data security experts such as RSA have had high-profile breaches resulting in loss of their customers' private, highly-sensitive information.[3] The inescapable conclusion is that, with enough at stake, ANY system can be breached. Detailed information about Australian citizens' Internet usage, potentially including personally-identifying information much sought-after by identity thieves and blackmailers, is an attractive and lucrative target for organised crime, among others. ***The only way to ensure that highly-sensitive information about Australian citizens is not able to be used against them is***

not to routinely collect and store it in the first place. In instances where there is sufficient cause to gain the appropriate wiretapping or search provisions from a court of law, then collection and storage of data on a case-by-case basis is still, of course, available to the law enforcement and intelligence community.

- **Data surveillance is able to be circumvented by the use of widely-available and vitally-important encryption tools.**

  At the moment, most Internet traffic is sent unencrypted. Most people quite rightly believe that most of their online activities are of little interest or value to anyone. When they use services that require them to submit sensitive information (banking passwords, credit card details, etc.), most Internet users now know that they need to ensure that the site they're using utilises (SSL) encryption to protect the data in transit.

  Some people, especially those living in restrictive or abusive regimes, desperately need their communications and activities to remain secret from their oppressors, and routinely use encryption tools like Tor[4] to protect their very lives. Others, including those engaged in organised crime, use encryption to assist in remaining undetected when organising or committing crimes. It is clear that encryption tools are both easily found and used, and able to be used equally for good or bad purposes.

  Those who want to keep their activities secret from law enforcement and the intelligence community *are already doing so*. The data that the proposed reforms want ISPs to collect and store is of negligible value to law enforcement, since it will not contain the data of the people in whom law enforcement and intelligence agencies are interested. It will simply contain the (legal) mundane 'secrets' of ordinary Australian citizens. And if widespread surveillance is introduced, more and more average citizens will be encouraged to use encryption tools to claim back their right of privacy—making it far more difficult for law enforcement and intelligence agencies to even identify *which* data streams are actually of potential interest to them in the first place. Introduction of ubiquitous online surveillance is likely to make the job of law enforcement and intelligence agencies *more* difficult, not easier.

- **The falsity of the "if you have nothing to hide, you shouldn't object" argument.**

  This argument has been thoroughly countered by others far more eloquent and expert than I. In 2009, as a response to Google's CEO, Eric Schmidt making the "if you have nothing to hide" argument in relation to the now-notorious #nymwars saga[5], leading online security expert Bruce Schneier wrote:

  "My Reaction to Eric Schmidt

  Schmidt said:

I think judgment matters. If you have something that you don't want anyone to know, maybe you shouldn't be doing it in the first place. If you really need that kind of privacy, the reality is that search engines -- including Google -- do retain this information for some time and it's important, for example, that we are all subject in the United States to the Patriot Act and it is possible that all that information could be made available to the authorities.

This, from 2006, is my [Bruce Schneier's] response:

Privacy protects us from abuses by those in power, even if we're doing nothing wrong at the time of surveillance.

We do nothing wrong when we make love or go to the bathroom. We are not deliberately hiding anything when we seek out private places for reflection or conversation. We keep private journals, sing in the privacy of the shower, and write letters to secret lovers and then burn them. Privacy is a basic human need.
[...]
For if we are observed in all matters, we are constantly under threat of correction, judgment, criticism, even plagiarism of our own uniqueness. We become children, fettered under watchful eyes, constantly fearful that -- either now or in the uncertain future -- patterns we leave behind will be brought back to implicate us, by whatever authority has now become focused upon our once-private and innocent acts. We lose our individuality, because everything we do is observable and recordable.
[...]
This is the loss of freedom we face when our privacy is taken from us. This is life in former East Germany, or life in Saddam Hussein's Iraq. And it's our future as we allow an ever-intrusive eye into our personal, private lives.

Too many wrongly characterize the debate as "security versus privacy." The real choice is liberty versus control. Tyranny, whether it arises under threat of foreign physical attack or under constant domestic authoritative scrutiny, is still tyranny. Liberty requires security without intrusion, security plus privacy. Widespread police surveillance is the very definition of a police state. And that's why we should champion privacy even when we have nothing to hide." [6]

In summary:

- I strongly object to any proposed reforms to national security legislation which would curtail the right to privacy of Australian citizens.
- I strongly object to any proposed reforms that would turn the presumption of innocence on its head, effectively turning all Australian citizens into *de facto* 'suspects'.

- I believe that there has been no case made to suggest that wholesale encroachment on the privacy of Australian citizens would elicit *any* benefit in terms of security, and in fact believe that it could have quite the opposite effect by masking genuinely 'suspect' traffic with completely innocent traffic encrypted in response to the introduction of the proposed reforms.
- I suggest that the idea that privacy and security are mutually exclusive is a false dichotomy, and that in fact security and a right to privacy are both essential to all Australian citizens.

Sincerely,

Jessica Smith

References:

1. http://www.abs.gov.au/ausstats/abs@.nsf/Products/B1BDF0A59F16AB85CA25795F000DB327?opendocument
2. http://www.itworld.com/security/288372/worst-data-breach-incidents-2012-so-far
3. http://www.cio.com.au/article/401401/security_breach/
4. https://www.torproject.org/
5. http://en.wikipedia.org/wiki/Nymwars
6. http://www.schneier.com/blog/archives/2009/12/my_reaction_to.html