Submission No 48

Inquiry into potential reforms of National Security Legislation

Name: M Abbey

Organisation: Private capacity

Mr Michael Abbey

11/8/2012

Re: Submission for the potential reform for security

To Whom It May Concern

I read with interest that there is a review and the opportunity to make a submission regarding Australia's future legislation related to internet technology, data retention and the privacy of individuals. My comments relate primarily to the storage of data by Internet Service Providers (ISPs).

- I understand that there are many challenges for the Law Enforcement Agencies (LFA) when it comes to cybercrime. There are the heinous crimes of paedophilia and pornography that is against all mores of our culture.
- I understand that the level of encryption that is available to the general public, such as "TrueCrypt" can make it impossible to access encrypted information.
- I understand the importance of having useful evidence to prosecute offenders
- I understand the need for laws to be up to date where possible with technology

My questions to the legislators and LFA are:

- Will all data stored for 2 years include all levels of government from the Prime Minister's Office, LFA, Military, Australian Tax Office to the local member of parliament as well as the public?
- How do you expect the Internet Service Providers (ISPs) to protect my privacy, when they store my data?
- How will you expect the ISPs to maintain this data in a form that is acceptable for a court of law?
- Are LFA not able to access data now if they request it of an ISP?

My role in the community is to be proactive in security of my local information. It is also my role to teach my family good security practices. However, I feel a certain helplessness when I deal with a company (this week past) over the internet and they send my username and 32 character password that is linked to my credit card details as free text in an email.

The LFA need all the tools that are available to identify, develop a case that leads to a prosecution which leads to a conviction. When this amount of data is stored for such a long time I believe there are a number of risks:

- Astronomical costs of storage for the ISPs that will flow on to Government and Public
- A honey pot of information that can be attacked relentlessly from anywhere in the world
- A potential for information to be abused either externally or internally

A number of security breaches have occurred from inside an organisation, this concerns me when there is a large blob of information held by all ISPs in Australia. The oversight of this process will need to be boilerplate if it becomes an eventuality.

Thank you for considering my submission.

Sincerely

Michael Abbey