Submission No 88

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Adrian Gasparini

Submission

Adrian Gasparini

Parliamentary Joint Committee
on Intelligence and Security
Office of the Clerk Assistant (Committees)
House of Representatives
PO Box 6021
Parliament House
CANBERRA ACT 2600
Tel: 02 6277 4397
Fax: 02 6277 4034
Email: pjcis@aph.gov.au

19-08-2012

Dear Committee Member,

I am submitting this response to highlight my concerns with the proposed reforms to the National Security Legislation. This is my full submission. I request if this submission is published my name and contact details are withheld from publication, as it could affect my future employment prospects in the sector I am currently employed in.

Regarding the expansion of ASIO's powers, I believe the proposals afford ASIO too much power without enough oversight in order to conduct their investigations. Changes such as the Terms of Reference (ToR) point 8. expanding the powers of a warrant as well as ToR 5. (b) extending its legitimacy from 90 days to 6 months, in conjunction with ToR 10. making them exempt from criminal and civil liability affords the agency with too much power and will only lead to corruption and the abuse of their position. There are many historical examples from around the world where government agencies have abused their powers. I believe it is best to avoid such possibilities by ensuring the agency must seek judicial oversight when exercising their powers and be held accountable for their actions. I don't know of any instances of terrorist attacks and other national security incidents that have occurred on Australian soil that could have been prevented by expanding ASIO's current limited powers, despite the existence of online social networks during much of this time. This to me suggests their current powers are adequate.

Regarding the data retention proposal in ToR 15. (c) the scheme is an unacceptable and unjustified intrusion into the privacy of any internet user and is a large cost to ISPs that will pass on the cost to it's customers without adequately safeguarding the data.

Firstly, I want to elucidate exactly how sensitive a person's browsing is. A person's browsing history is a very personal snapshot of that person's life and personality. A person should have the right to keep aspects of his personal life completely private. For example, take into consideration searches conducted on Google maps; the social networks a person may log into; medical symptom related searches on Google; and a snapshot of the adult content searched for on various websites. It would be easy to determine the identity and address of a person, their circle of friends and their partner, possibly identify any affairs being conducted, determine their sexual orientation, age, as well as any possible embarrassing medical conditions that the person may have searched for. It is easy to also

attribute those conclusions to that person, whether they are true or not. Such personal and private insights into a person's life shouldn't be aggregated or accessed without the oversight of authorities to ensure there is just cause to intrude into this person's life to this extent, and to ensure entities with access to this data don't abuse it.

Secondly, however, I want to illustrate how an ISP account's browsing history can also be incorrect. As an example, I live in a household of 4 people, with one ADSL account with an ISP. We regularly have visitors over and they often use our internet connection. Everyone who uses the internet connects to our wireless router. From the perspective of our ISP, they only see one computer connected – the router. The ISP cannot differentiate between me connecting and my friend who came over for dinner. Now if my friend was to search the internet "how to cure genital warts" or other more embarrassing or illegal content, how can the people examining the browsing history differentiate between me and my friend? Some other questions worthy of being answered are:

- If the logs are leaked will be unfairly portrayed as suffering from genital warts?
- What if the security of my wifi router became comprimised and a third party utilised it for downloading illegal sexual content?
- What if my computer is infected with a virus that accesses IP addresses that are flagged as containing illegal content without my consent?
- In the event that an illegal IP address is accessed from my machine without my knowledge, will I be arrested for accessing illegal content and have my photo splashed across the front pages of newspapers?
- Will I forever have to tick the box on application forms necessary to study and apply for certain jobs that asks if I have ever been arrested for a sexually oriented crime if some of the IP addresses accessed without my knowledge relate to such material?
- Is it fair or acceptable for my reputation, or any innocent individual's reputation, to be tarnished in such a way in order to 'protect the nation'?

I can see such misrepresentations occurring frequently, and few actual crimes will be solved as a result of keeping details on a ISP user's browsing history alone. Hence I believe retaining the browsing history of an user's ISP account will not provide evidence strong enough to resonably convict or even attribute with any degree of certainty to a particular person. Not only is the evidence gathered not specific enough, it isn't acceptable to treat all internet users as criminals, and may lead to people's reputations being unfairly tarnished.

In light of the extreme sensitivity associated with an individual's browsing history, and in conjunction with the low fidelity of an ISP account's browsing logs, and the substantial cost of maintaining such a secure database, the proposal is unjustifiable.

Furthermore, what is wrong with seeking a warrant to target a specific ISP user account to the exclusion of all other users prior to any data being logged if the data is deemed necessary? We should ensure the person's individual privacy is worth comprimising only if there is evidence a crime is being committed. I believe this is what occurs with the postal, and telephony systems. I believe everyone's phone calls and mail are not automatically recorded and stored for a period of time, and to intercept a person's phone calls a warrant needs to be issued if there is evidence of wrongdoing. Why is the internet being treated differently? From this proposal it appears as though every internet user is to be treated as a criminal; therefore it is an unacceptable intrusion into the private lives of any internet user.

Regarding the increased access to social networks, I am also curious as to why the government is specifically interested in aaquiring further access into people's online social networks. Especially since Facebook and Google already willingly provide authorities with information on their users

when presented with a reasonable request from the authorities. It suggests to me the government and/or the authorities are interested in obtaining this information in the absence of a reasonable request.

Also, the idea that private sector companies will be responsible for building and securing the data is a worry. Private sector companies exist for one reason only, and that is to generate profits. Anything that doesn't contribute to profits and consumes resources is seen as a cost centre, and is optimised accordingly. A large secure database that stores a user's browsing history over a period of multiple years is costly to implement, and doesn't contribute to profits. I doubt consumers would be interested in spending exra to have their browsing logs secured properly. Hence, I question the motivation of privately owned ISPs to spend the necessary money to keep the data secure, and as a result, the average internet user is left vulnerable to possibly having his very personal browsing history misused or leaked. Obligating these private companies to secure the data under the threat of fines is not good enough. Once the data is leaked, no fine on the ISP will take away the humiliation and violation felt by the people who have had their lives and their privacy comprimised.

In addition to these points, I also believe this data retention proposal suggests that authorities are not interested in utilising it in a manner to prevent terrorist attacks or detect threats. If they were they would have no interest in who searched what on the internet a year ago. To me this proposal suggests a way of easily generating lists of people that need to be arrested and investigated during law enforcement quiet periods, or identifying individuals for investigation and prosecution first and then building up a cache of circumstantial evidence to add further justification to their continued investigation. None of these reasons justify the economic cost or intrusion into people's lives. Hence, the data is not needed to safeguard Australia from emerging national security issues and terrorist threats.

Putting the threat of terrorism in perspective, ddespite Australia making itself a target since September 11 2001 by loudly backing the USA's interests and participating in many foreign wars and the broadening of terrorism related police powers, Australia has not been attacked on its own soil in the past 11 years and beyond and only a handful have been arrested for planning something. This would suggest to me the current laws are actually working, or no one is interested or motivated enough to terrorise the residents of Australia. This is important, because it determines the appropriate cost that should be invested in dealing with terrorism. To illustrate this point, I question the dollars that are spent in the name of fighting terrorism, given that there are so few Australian victims from terrorist events on our soil, compared to other dangers that we could be addressing that kill and maim far more people. An example would be Australia's obesity epidemic. Alternatively, the money could be spent in areas that are likely to have a greater impact on people's day to day lives, such as the education system or the health system. I believe it is time to rectify the policy overreaction that has occurred as a result of the terrorist attack on the USA in 2001.

Finally by building this infrastructure in the first place, you are facilitating any future abuse that arises as a result of the exploitation and misuse of these logs. Today the logs will be used to secure convictions of people who have viewed child pornography; many more innocent people may suffer from their reputations being unjustly smeared with the same accusation. How long until 2 years data retention is deemed insufficient,and is extended to five, ten, or fifteen years? Is it just to hold someone to account for something they searched for 5 to 10 years ago? How long until someone advocates for a police check as a condition of employment to include vetting a person's browsing history? How long until a data leak at an ISP results in the outing of a leading AFL footballer, swimmer, politician, or anyone else of interest who is a high profile individual as a homosexual due to their browsing history? I am thinking of the ordeal David Campbell underwent as a result of channel 7 filming him leaving a gay sauna in Sydney. The affected individual's desire for privacy will be countered by the media's belief that the 'news' is in the public interest. Having everyone's

browsing history so easily searchable will only increase the number of people that will suffer the same fate.

Building and utilising such infrastructure will make arrests and policing easier. It is no wonder the authorities are all in favour. It makes their jobs easier to arrest people. However their jobs by definition should be dificult, to ensure who they arrest and charge are reasonable suspects, with enough evidence to secure a reasonable chance of conviction. Police and other authorities should interfere with as few innocent people as possible. I would rather some guilty people escape punishment for a crime, than have some innocent people suffer and be punished for a crime they didn't commit. The government states this is necessary for the 'protection of the nation', but exactly who is being protected? What about the average internet user, don't they deserve the protection of their privacy?

These proposals must not go ahead.

Regards
Adrian Gasparini