



Submission No 144

Inquiry into potential reforms of National Security Legislation

Organisation: Ms Kellie Tranter

Your ref:

Our ref: KAT:gl

Parliamentary Joint Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

By email

20 August 2012

Dear Sirs/Madams

RE: Inquiry into potential reforms of National Security Legislation

I welcome the opportunity to raise concerns about proposals relating to the Telecommunications (Interception and Access) Act 1979, the Telecommunications Act 1997, the Australian Security Intelligence Organisation Act 1979 and the Intelligence Services Act 2001.

One always wonders where the impetus comes from for legislative changes. The who, why and when questions often remain unanswered and seldom do we see empirical data to detail or substantiate claims for the expansion of powers. Although the intended purpose (sworn on the graves of the mothers of the reformers) is always publicly stated as the need to ensure that police and intelligence services keep technological pace with criminals and terrorists, I am deeply concerned that the proposed changes will be misused as a tool for turning open source data into actionable intelligence to block legitimate political dissent and political movements and to spy on the activities, interests and political views of innocent ordinary citizens.

According to a series of articles published by Slate magazine, it appears that the United States, Canada and the United Kingdom have separately been arguing the case for expanded power to monitor Internet communications "quietly collaborating to reform surveillance laws so that they are "harmonised" to a similar standard from country to country."



Slate also reported that Australia intends to sign The Council of Europe's Convention on Cybercrime, which codifies a commitment to establish a system of mutual assistance for issues related to computer crime. This includes measures related to enabling real-time surveillance of communications content.

Australia is heavily involved in intelligence sharing under the United Kingdom-United States (UKUSA) Agreement that governs signals intelligence co-operation between the US, Britain, Australia, Canada and New Zealand.

Coincidentally Lockheed Martin has developed 'LM Wisdom' which it describes as:

“ a predicative analytics and big data technology tool that monitors and analyses rapidly changing open source intelligence data (newspaper feeds and social media content for example). This type of content has the power to incite organised movements, riots and sway political outcomes. LM Wisdom turns this data into actionable intelligence for our customers. Think of Wisdom as your eyes and ears on the web... Wisdom's high performance analytic algorithms analyse the content in near-real time, distinguishing noise from high value information. It captures cultural context, trends, sentiment and influence, giving our customers deeper situational awareness.”

I understand that the US airforce awarded Lockheed Martin a \$27 million contract to develop the Web Information Spread Data Operations Module (WISDOM) with military analysts already using it to monitor Central and South America and the Pacific region. It was reported recently that the FBI is talking to software vendors and the Department of Homeland Security in the United States already has a monitoring system up and running.

Clearly Australian citizens need to know the extent to which overseas countries or their servants or agents, and in particular any private corporation, will be given access to information and will be able to take advantage of any proposed changes to Australia's laws. What appropriate safeguards will be put in place to ensure that the information of Australian citizens will not be used to single out dissidents, quash political dissent or be used for commercial or quasi-commercial purposes? This is particularly important in light of calls to amend subsection 19(1) of the ASIO Act to avoid any doubt about ASIO's ability to cooperate with the private sector.

The Communications Data Bill in the United Kingdom has been dubbed the "Snooper's Charter" because it forces internet service providers to keep data of every website visit, email, text message and visit to Facebook or Skype for a minimum of 12 months (as opposed to the current proposal in Australia for a period of two years – twice as long!). Police and other government agencies allegedly will not be able to access the contents of the emails or messages, but will know who was contacted, when and by what method. The cost is estimated to be an extraordinary 2.5 billion pounds over 10 years. The current discussion paper provided for this inquiry does not provide any details of the likely cost to Australian taxpayers.

MPs, ISPs and civil liberties groups in the United Kingdom have already raised significant concerns about the proposed legislation, including that:

- it allows pervasive black boxes that would monitor every online information flow;
- it is an unprecedented and unwarranted attack on privacy that will see the Government track where we make calls, who we email and what everyone does online;
- if the target is criminals, get a warrant. Get a judge to sign a warrant – not the guy at the next desk, not somebody else in the same organisation;
- the "communications data" trail can build up a frighteningly detailed picture of your life: who you have texted, emailed and telephoned on any given day; where you were when the contact was made and for how long; which websites you have visited in the privacy of your own home and more. In particular, web addresses can tell you an awful lot about a person – the state of their health, their hobbies or political interests;
- for the first time private companies will be instructed to collect information on billions of communications made by their customers for no reason other than the authorities' future demands for access. This amounts to mass, blanket, surveillance of the population outsourced to the private sector. For these reasons courts in Germany, Romania, Bulgaria, Cyprus and the Czech Republic have found similar arrangements in their respective countries to be unconstitutional;

- the police already have the power to put individuals they suspect of committing crime under surveillance. But this proposal will allow information to be collected about everyone, not just suspects. What's more there have and will always be methods of communication that do not come within the State's reach, ranging from the use of pay-as-you-go mobile phones to complicated encryption techniques. Whilst the data of many innocent people will be captured serious criminals will likely avoid detection;
- building such a comprehensive database of the web habits of the whole population leaves us all at risk of bureaucratic error and even fraud; and
- this will set up the mechanics for a police state. Data-mining looks for patterns in huge datasets – for example, to build up an intelligence picture of an individual or group of people.

In the United States whistleblower William Binney revealed the NSA's massive power to spy on Americans with the Utah spy center containing near-bottomless databases to store all forms of communication collected by the agency, including private emails, mobile phone calls, Google searches and other personal data. He warned that the NSA's data-mining program has become so vast that it could "create an Orwellian state." He commented:

"[the government] has a licence to take all the commercially held data about us, which is exceedingly dangerous, because if you take that and put it into forms of graphing, which is building relationships or social networks for everybody, and then you watch it over time, you can build up the knowledge about everyone in the country. And having that knowledge then allows them the ability to concoct all kinds of charges, if they want to target you.....[government copies of emails] I would think –I believe they have most of them, yes....All they would have to do is put various Narus devices at various points along the network, at choke points or convergent points, where the network converges, and they could basically take down and have copies of most everything on the network...."


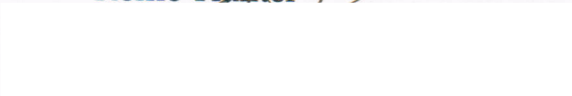
I find this particularly disturbing when we now know that Australia's cyber-spy agency, the Defence Signals Directorate, and the Australian Government Information Management Office have warned agencies the Patriot Act allows the US government to access data held by American companies "without necessarily advising" the information's owners. That power extends to data stored outside America.

ASIO is known for making adverse security findings against innocent people. In light of William Binney's revelations, combined with proposals that will allow ASIO to "plant material on people's computers, and destroy material and go through a third party's computer to do so; criminalising refusing to cooperate with government decryption attempts and freeing up ASIO agents to break the law if it helps to stay undercover", it doesn't require much exercise of one's imagination to see a pattern of behaviour emerging here.

ASIO is not subject to the provisions of the Freedom of Information Act 1982. The Privacy Act 1988 does not apply to the disclosure of personal information to ASIO by other agencies and while Attorneys-General come and go the bureaucracy remains the same with little scope for Australian citizens to hold it to account. This must be rectified.

Walter Binnie's concerns apply as much to the data gathering activities of Australian security and intelligence organisations as they do to US organisations. If you have any doubt that the proposals for legislative expansion of the powers of our security and intelligence organisations are anything but the groundwork for an Orwellian state I invite you to reread "1984" and to watch Lockheed Martin's promotional video for "LM Wisdom". By expanding the powers of these unaccountable organisations, without any properly established justification, Parliament will not only be abnegating its responsibility to protect the rights and interests of the Australian people, but it will be putting the future of the Australian people, and probably its own, in the hands of organisations and corporations over which there is no effective control.

Yours faithfully
Kellie Tranter



Lawyer and human rights activist

Encl