Submission No 28

Inquiry into potential reforms of National Security Legislation

Name: James McPherson

Organisation: Private Capacity

20 July 2012

Committee Secretary
Parliamentary Joint Committee on Intelligence and Security
PO Box 6021
Parliament House
CANBERRA ACT 2600
AUSTRALIA

Fax: +61 2 6277 2067
email: pjcis@aph.gov.au

To the Parliamentary Joint Committee on Intelligence and Security,

Re the Inquiry into potential reforms of National Security Legislation

I am writing to you regarding the Attorney General's discussion paper on potential reforms to National Security Legislation and the associated terms of reference for the Committee's inquiry, published on 9 July 2012.

It is my opinion that the proposals are completely unjustified. My concerns cover many areas, including but not limited to

- Trust and confidence in government agencies.
- Agency competence.
- Our legal and societal expectation of a person's right to privacy.
- Human rights.
- The democratic expectation that our government agencies can and will be held accountable for their actions through effective and regular review *by the people.*
- The opportunities which will be created for identity theft, fraud, corruption and other sorts of malfeasance (whether corporate or government).
- The sharing of personal data and information with foreign governments and foreign corporations.
- The cost to carriers/carriage service providers (C/CSPs) to comply with the proposals.

The cost to Australia if these proposals became law would be immense and irreversible.

With the exception of proposals 2a, 6a, 6b, 6c, 6d, and 7 in the terms of reference, I urge the committee in the strongest possible terms to reject the proposals.

Trust and confidence in government agencies

The discussion paper starts by trumpeting the successes which covert Australian agencies have had over the last 10 years[1]. The paper then asserts that in order to enable the agencies to do their jobs, they need to log every single data and voice packet which flows through carriers and communication service providers' (C/CSPs) networks. The assertion leads to the conclusion that the earlier mentioned successes were, in fact, dumb luck rather than good investigation and policing.

Why should the Australian public be saddled with an unaccountable (to the *people*) government agency logging their every online activity for at least two years? Despite the year-on-year budget increases which the agencies have been blessed with, they claim they are still unable to do the tasks which they are required to do. The evidence should point towards fixing the agencies, rather than just throwing money, resources and our personal data at them in the hope that this will somehow make them better.

If covert agencies store all our data, every other part of the federal and state governments will clamour to gain access to it, and as we have seen with the litany of changes to the Telecommunications (Interception and Access) Act over the last ten years, eventually all of government will get access to it. There will be no reason for people to trust any part of government; this is an unhealthy state of affairs for any democracy.

The proposals assert that there should be fewer privacy protections because "many of the requirements reflect historical concerns about corruption and the misuse of covert powers and do not reflect the current governance and accountability frameworks within which agencies operate."[2]

The fact that we have these requirements is a direct response to the well-documented corruption and misuse by federal government agencies, state police forces and state Special Branches in preceding decades. It is said that with great power comes great responsibility; removing the responsibilities regarding privacy and human rights gives the agencies unfettered power to act as they see fit. This is not acceptable to a democratic society.

1 http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/additional/discussion%20paper.pdf, page 3.

2 Discussion paper, page 26

Apart from our own history, we have examples from the UK (with RIPA[3]) and the USA with its warrant-less wiretapping[4] cases, USA state police forces operating in defiance of court orders and constitutionally protected speech to harass Occupy protesters (including subpoenaing Twitter for metadata[5]), and the infamous Homeland Security "No Fly List"[6]. It is not a question of **if** these powers might be abused, but how soon after enactment **will** those powers be abused.

Our legal and societal expectation of a person's right to privacy

Our society expects that our words and deeds, unless actually illegal, *will remain private unless we as individuals choose to offer them* for public consideration in one form or another. This expectation is reflected in Australian court decisions, is called out in international agreements[7] and in the Australian Privacy Act[8]. While it is correct that social media is immensely popular, and that many people share too much information about themselves on facebook, twitter and blogs, that is their choice to do so. This is seen as such an important problem that schools, universities, state and federal police as well as government bodies such as state departments of Fair Trading issue frequent warnings and run training about how *we can control* what information we should share.

The two-year data retention proposal smashes right through long-standing legal and legislative history, and societal norms, and completely undermine the good work which organisations at every level of society have done to make the online world safer.

3 https://en.wikipedia.org/wiki/RIPA
4 https://en.wikipedia.org/wiki/Warrantless_wiretapping
5 http://gawker.com/5908692/why-a-fight-over-an-occupy-wall-street-protesters-tweets-matters-to-your-privacy, https://www.eff.org/deeplinks/2012/02/malcolm-harris-occupy-wall-street-twitter-government-pressure, http://www.forbes.com/sites/andygreenberg/2012/05/08/twitter-fights-prosecutors-seeking-occupy-protesters-data-without-warrant/#more-6254
6 It is indicative of the difficulties that security agencies face that there is a TRIP number for every passage into the USA. This stands for Travel Redress Inquiry Program, whereby misidentified passengers can appeal their inclusion on the No Fly List. There is a summary of documented problems with this List at https://en.wikipedia.org/wiki/No_fly_list.
7 Article 17 of the International Covenant on Civil and Political Rights of the United Nations of 1966 also protects privacy: "No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks."
8 Privacy Act 1988 (Cth), see also the list of Federal and State Acts summarised at https://en.wikipedia.org/wiki/Privacy_in_Australian_law

Consider the brief list below, which is just some of the personal information which is now primarily sent via C/CSPs rather than in the post:

- medical test results
- xray/mri/CT scan results
- medical referrals from one doctor to another
- payments and their associated receipts
- bank account and credit card statements
- communication with accountants
- communication with lawyers
- telephone bills and call details

I am sure that the Committee recognises that medical information is considered by that profession as well as under the law as strictly Private between a doctor and patient. Our society places considerable value on the trust and privacy of that relationship; the data retention proposal will destroy that trust. Likewise, communication between a lawyer and a client is also covered by privilege unless otherwise ordered by a court, and society places a similar value on that privacy.

Even if the only data which was logged was email message headers, or a list of visited websites, there is more than enough information there to build accurate profiles of people, their opinions and their social networks. The most likely outcome of such surveillance is self-censorship, to avoid harassment by covert agencies “just in case” an expressed opinion might fit some criteria which the agencies make up to justify invasive actions.

I am sure that members of the Committee are aware of the current Federal Court case regarding the Speaker of the House of Representatives. Under these proposals there would be no need for court action to force the discovery of emails between a News Ltd. Journalist, the media advisor and members of the Opposition. That information would be readily available via the covert agencies' data gathering. Likewise, the Member for Denison might have found it more difficult to present his evidence to the Inquiry into the Iraq War.[9]

At present law enforcement agencies (and other branches of government such as the covert agencies) need to obtain a warrant (and present evidence to a court or officer designated by an Act) to justify obtaining that information. The data retention proposal would make the courts irrelevant; which agency is going to bother going to get court authorisation to look at data which they have already stored?

9 "Intelligence on Iraq's weapons of mass destruction". Official Committee Hansard, Commonwealth of Australia. 22 August 2003.

It is also proposed (15a) that an offence of “failing to assist in the decryption of communications” be created. Without a warrant issued by a court, why should a person be required to incriminate themselves just because the agencies want to get that particular communication data? This proposal is objectionable in the absence of a court-authorised warrant, and downright offensive. The statement “if you have nothing to hide then you have nothing to fear” or a variant thereof is frequently trotted out when this topic is raised, which completely misses the point: *my communication is mine, and is private unless I choose otherwise*. It does not belong to the government, nor to its agencies. Law-abiding members of society should not have to censor their speech or thoughts in order to “have nothing to hide”.[10]

It has been suggested amongst the internet community that this proposal would make Virtual Private Networks (VPNs) illegal. If that were to be the case, every company operating in Australia which allowed its staff to work outside of a secured office environment would be in breach. As a person who works from home fulltime, the only way that I get my job done is via a VPN connecting me to my company. In order to not break such a provision, I would have to commute to and from an office every day, increasing the load on our public transport system. Our company's field support staff would also be unable to provide quick turnaround on support problems; any data gathered on site would need to be driven back to the office. This is an incredibly short-sighted and pre-internet way of doing things.

Human Rights

In addition to the rights mentioned above, the proposal recommends authorising ASIS to train "persons cooperating with the agency" in weapons use and other related areas[11]. Since it is admitted that ASIS operates outside of Australia's borders, this part of the discussion paper leaves open the possibility that ASIS could train terrorists and agents from foreign governments with dubious human rights records. Our Department of Defence has been involved with this in the past, when the SAS provided training for member of the Indonesian Kopassus unit. It is my opinion that allowing this provision to become law would breach our obligations under national and international human rights law.

Australians are quite proud (and with good reason) of our international record on human rights issues. Opening us up to the charge of supporting repression overseas through covert agencies will do our international reputation considerable harm. It also increases the dangers to our troops, overseas-posted police and other peacekeepers as well as our foreign aid workers. This is not acceptable.

10 Universal Declaration of Human Rights, articles 18, 19 and 20.
11 Discussion paper (ibid) p54

The cost to carriers/carriage service providers (C/CSPs) to comply with the proposals.

According to the Attorney-General's discussion paper, in the quarter ending June 2011, 274202 terabytes of data was downloaded by Australians, a year-on-year increase of 76%.[12] This is not only a staggering amount of data, but a staggering growth rate. As the NBN continues to transform broadband access, it is reasonable to assume that we will continue to see similar rates of growth into the future.

If we work on the reasonable assumption that over the course of a year Australians downloaded on the order of 1 million terabytes, which is 1000 petabytes or 1 exabyte, then storing all this data becomes prohibitively expensive. We should not forget the cost in compute power that would be required to manage that data, let alone the cost of compute power to search through that data and make sense of it. That, too, is only for one year, and does not include the amount of storage or compute power required by the covert agencies themselves in order to make use of this ocean of data.

For data storage of this magnitude, you need to purchase mainframe capability disk storage, compute power and provision environments to house that capability in. You would need to provision at least 1000 full disk cabinets (or frames) using enterprise-quality disks. These cabinets typically provide 100 terabytes of usable storage space in one to five racks.[13] At this level of capacity, the industry standard is to provide two or preferably three 32amp power feeds from different electricity providers. Network cabling for management and fibre-optic cabling for access to the data is also required, as is consideration of the cooling requirements.

While it is tempting to assume that this could all be housed in one secure data centre, that would be foolish from both security and business points of view. Since the proposal is for each C/CSP above a certain size to store this data, you would need more than 1000 frames spread out at perhaps twenty data centres around the country. This is to allow for different fill rates depending on the C/CSP, redundancy of the data and access to it. If these frames and the associated compute nodes were to be housed in existing data centres, those data centres would need to be secured and audited for compliance on a regular basis. In addition, dedicated and security-cleared operations and management staff would be required from the C/CSPs.[14] With the number of physical disks involved, it would be a fulltime task for several people just to change out failed disks in each frame under their management.[15]

---

12 Discussion paper p18

13 One industry-standard Rack is approx 1.9m high, 60cm wide and 80cm deep.

14 Several years ago it was estimated that obtaining a Secret clearance cost between $50,000 and $100,000. This is unlikely to have decreased.

15 This is a well-known feature of large installations. Please refer to descriptions of the *Bathtub Curve* for more details.

Even if the agencies were able to negotiate a significant discount to the price of each disk frame to be used for this proposal, they would still cost around $500,000 each. Further, since these would need support coverage from the vendors using a Secure support contract (where broken components are securely destroyed rather than being returned to the vendor for rework), the necessary agreements are noticeably more expensive than standard contracts.

Making backups of this data to tape would take too long, even with the fastest, most high-capacity tape media available. The appropriate enterprise-quality solution is to provision duplicate frames and duplicate compute nodes and do disk-to-disk backups across a dedicated fibre-optic link.

As you can see, the costs mount very rapidly and this is without even considering the expense involved for compute nodes, network connections, extra power, cooling and security auditing for existing data centres, building of new secure data centres or the cost to the agencies themselves for maintaining this data and access to it.

Please remember, the estimates above are for one year only. The proposal talks about maintaining the data for two years, so you would actually need to triple the number of frames required so that the agencies could have a rolling two-year period. I do not think it is unreasonable to suggest that the startup costs alone would be over one billion dollars, with ongoing costs that exceed $200 million per year. This cost would be passed on to the customer by the C/CSP, and to the taxpayer through an increased opaque budget allocation for the covert agencies.

The opportunities which will be created for identity theft, fraud, corruption and other sorts of malfeasance (whether corporate or government)

As a society we are well aware of the opportunity for, and increasing incidence of identity theft and fraud. Every single data center housing any part of the nation's logged data will become almost unbearably attractive to nefarious persons. It only takes one slip in one C/CSP procedure for a weakness to be exploited.

We see this reported in the news every few weeks. Just during the month of July 2012 there have been widely publicised reports of hacks to Yahoo! Accounts[16] and to Billabong[17]. AusCERT and DBCDE managed to lose several

16 http://arstechnica.com/security/2012/07/yahoo-service-hacked/
17 http://arstechnica.com/security/2012/07/user-passwords-dumped-in-alleged-billabong-com-hack/

thousand customer details[18]. Information on an unknown (but sizeable number) of Telstra's customers was available without protection for two weeks before it was taken down[19]. We have seen several instances where the Sony PlayStation Network (PSN)[20] was cracked, and last year two US Government contractors (Stratfor[21] and HBGary Federal[22]) were cracked wide open.

With so many opportunities just on the C/CSP side for data to leak (rendering the victims open to theft and fraud), it is important to remember that there will be similar opportunities from a large covert agency-held data store also.

When coupled with the discussion paper and terms of reference proposal (11c and 17a) to allow agency staff to disrupt a target or target's computer and the assertion that safeguards for society are not needed, it is very easy to see how this power can be abused by agencies, or by agents acting on their own. There is no justification for creating opportunities for malfeasance for agencies which are supposed to protect the Australian people. The agencies need to be reminded that they serve us, and we do not serve them.

Imagine if an agent decided to act on a grudge (or worse, just on a whim) and plant information about a person in the logged data. Imagine if the agent then acted to enable a leak of that data. There is a very real risk of this happening if agents are allowed to disrupt a target. *Let's be plain here – the agencies are asking for the "lawful" ability to plant evidence and to be immune from prosecution for doing so.*[23] We have seen how this plays out with state police in the past, as well as state police Special Branches. It does nothing to enhance our security, and weakens every case which the agency might want to bring to a court because the prospect of tainted evidence being used to secure a conviction brings our courts into disrepute.

18 http://www.smh.com.au/digital-life/consumer-security/most-embarrassing-blunder-government-contractor-paid-1m-for-esecurity-alerts-service-loses-8000-subscribers-personal-information-20120709-21q86.html

19 http://www.gizmodo.com.au/2011/12/telstra-leaves-bigpond-user-details-exposed/ , http://www.theregister.co.uk/2011/12/09/telstra_opens_customer_database_in_egregious_blunder/

20 http://www.theregister.co.uk/2011/04/26/sony_playstation_network_security_breach/

21 http://www.cryptome.org/0005/stratfor-hack.htm

22 http://nakedsecurity.sophos.com/2011/02/07/hbgary-federal-hacked-and-exposed-by-anonymous/, http://krebsonsecurity.com/2011/02/hbgary-federal-hacked-by-anonymous/, http://www.forbes.com/sites/andygreenberg/2011/02/28/hbgary-federals-aaron-barr-resigns-after-anonymous-hack-scandal/

23 Terms of reference 10 and 11c.

The sharing of personal data and information with foreign governments and foreign corporations

Proposal 12 in the terms of reference document seeks to clarify ASIO's ability to cooperate with the private sector. Unless this proposal is specifically intended to state, clearly, that *ASIO is under no circumstances allowed to cooperate with the private sector*, then this appears to be an attempt by the agency to allow sharing of data with organisations which have no security aspect whatsoever.

The first two organisations which come to mind are the United States' MPAA and RIAA, via their local operations team called AFACT. It is well known[24] that Australians use filesharing methods to obtain the TV series Game of Thrones, How I Met Your Mother and The Big Bang Theory in advance of their air dates in Australia. There are many reasons why people do this, but they are not germane to this inquiry. What is important, however, is that if ASIO was allowed to give data on what we download to (no doubt) “suitably qualified” third parties, then AFACT/RIAA/MPAA would be first in line to find out who was trying to get past their monopoly on content, and then extradite those people to the USA to face criminal proceedings in friendly courts, proceedings which our courts and parliament do not believe require a criminal trial.

I am sure that the Committee is aware of the recent decision in the AFACT vs iiNet appeal handed down by the High Court of Australia.[25] It is possible that this proposal would free foreign content licensors from a perceived need to lobby for changes to Australia's Copyright Act. To my mind, such data sharing could only be seen as a blatant rejection of the authority of the High Court. I doubt the Court would find this acceptable.

We would also be subject to our data being sent offshore to countries with fewer protections for our privacy and human rights. The nation which is first in line on this front is the United States of America. The provisions of their P.A.T.R.I.O.T. Act[26] for government meddling in private business are well-known. This is one reason KPMG found for a slow uptake in offshore cloud services.[27] Unfettered provision of data on Australians to foreign governments

---

24 http://delimiter.com.au/2012/05/22/australia-top-game-of-thrones-pirating-nation/, http://torrentfreak.com/whos-pirating-game-of-thrones-and-why-120520/, http://www.zdnet.com/game-of-thrones-outs-the-aussie-pirates-1339335201/, http://thronesblog.com/tag/australia/

25 http://www.zdnet.com/tit-for-tat-in-afact-iinet-final-submissions-1339325889/, *Roadshow Films Pty Ltd v iiNet Ltd* [2012] HCA 16. 2012 Judgment summaries *High Court of Australia*, 20 April 2012. Complete judgement at AustLII.

26 http://www.gpo.gov/fdsys/pkg/PLAW-107publ56/content-detail.html, “**U**niting and **S**trengthening **A**merica by **P**roviding **A**ppropriate **T**ools **R**equired to **I**ntercept and **O**bstruct **T**errorism (USA PATRIOT ACT) Act”

27 http://delimiter.com.au/2012/05/01/offshore-cloud-an-adoption-barrier-finds-kpmg/, report at http://www.kpmg.com/AU/en/IssuesAndInsights/ArticlesPublications/Documents/modelling-economic-impact-cloud-computing.pdf

by an Australian government agency reeks of sovereignty problems. Where do Australia's rights and interests become less important than handing out data which the USA requests (whether on the government's behalf or on the say-so of lobbyists)?

Agency competence

My final area of concern relates to proposals 5, 10, 11, 16 and 17 in the terms of reference.

The agencies wish to double the length of time they are allowed to have an active search warrant, from 90 to 180 days. The agencies claim that this would allow them to react more effectively to quickly changing operational circumstances and not spend time re-analysing the situation to apply for another warrant. I find it very curious that operational reaction times are given as a reason for allowing a longer period to have an active warrant. Since the discussion paper (and reported comments from the head of the High Tech Crime Center[28]) both make much of the need for a rapid response to changing circumstances, there is no justification for increasing the already extensive amount of time for which a search warrant is active. If the agencies cannot figure out how and when to execute a warrant within 90 days, why should we trust that giving them twice as much time will result in any more appropriate action?

The agencies wish to have the power to not only disrupt a target's computer(s) and network(s), to trespass through third-party computers and networks to do so, and to seize *any other computing device* that they might find when executing a warrant. This makes the entire operation a fishing expeditionn (bordering on harassment), not one based on evidence of illegal activity.

Simply, if the agency is unable to determine which computer(s) and network(s) they wish to seize, then they have not done their job. With the tools available for data mining from Open Source communities, from commercial software companies, other government agencies as well as whatever the agencies have written themselves, it should be well within the competency of the agencies to determine exactly what needs their attention.

The agencies also wish to be able to *dictate* to C/CSPs how to design their infrastructure, *force* the C/CSPs to use select commercially available components have the agencies' seal of approval, and *provide penalties for failing to do so*. This is engineering arrogance at its zenith. The agencies do not run the C/CSPs' businesses. The agencies do not have knowledge of what the C/CSPs' plans for the future are, or what problems they might need to solve.

28 http://www.brisbanetimes.com.au/opinion/political-news/roxon-questions-plan-to-track-users-web-history-20120720-22fp6.html; discussion paper p40.

I am more than happy for agencies to craft *suggestions* on security considerations which C/CSPs should take into account when auditing existing infrastructure and planning new infrastructure. However, telling C/CSPs what they may or may not use based on opaque justification is a completely unacceptable intrusion into commercial operations. It is completely at odds with the free market rhetoric which governments of both sides of the Australian political spectrum have been very happy to operate with for the last 30 years.

Conclusion

If we surrender our rights because a covert agency asserts that this is what is necessary in order to guarantee our safety, then every member of society becomes a criminal. Every member of a constantly surveilled society is subject to blackmail by that agency. The covert agencies are supposed to be our servants; we should not be in thrall to their unending appetite for information with which to protect them from us.

If the Committee allows these proposals to continue in to legislation it will be derelict in its supervisory role for the covert agencies. It will take many decades to retrieve our privacy from the ashes of the surveillance state.

Our society and government should be based on trust and respect, not on fear.

Yours faithfully,
James C. McPherson
—
Software engineer, system administrator, troubleshooter.