Submission No 117

Inquiry into potential reforms of National Security Legislation

Organisation: Mr Bernard Keane

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

Dear Secretary

Inquiry into potential reforms of National Security Legislation

Please find enclosed a submission to the committee's inquiry into potential reforms of National Security Legislation.

I make this submission in a private capacity and in no way intend to reflect the views of my employers, Private Media.

Yours sincerely

Bernard Keane
Canberra

20 August 2012

1. INTRODUCTION

The Attorney-General and the Joint Committee on Intelligence and Security (the Committee) are to be commended for providing an opportunity for public discussion of amendments to Australia's surveillance and intelligence-gathering laws.

For too long Australian governments, including the current government, have introduced into Parliament bills significantly strengthening those laws or providing additional powers to intelligence and law enforcement agencies with minimal public discussion except via Senate committee processes. These processes have themselves often been curtailed, providing little opportunity for the public and key stakeholders to bring different perspectives to committees' consideration of bills. It is to be hoped that this inquiry establishes a precedent for future governments contemplating amendments to our surveillance and intelligence-gathering laws.

A characteristic of Senate committee processes, too, has been the inability or unwillingness of the Attorney-General's Department (AGD) to publicly provide evidence or verifiable justification for the often significant extensions of agency surveillance, intelligence-gathering and enforcement powers proposed in bills. Instead, it has preferred to rely on mere assertion about the need to modernise or standardise the surveillance and intelligence-gathering laws.

This was most vividly illustrated in hearings in relation to the Intelligence Services Legislation Amendment Bill 2011, when AGD officers were directly asked to provide examples of what specific failing in ASIO's then-current powers the Bill was intended to remedy and in response provided one that was, some months later, directly contradicted and dismissed by the director-general of ASIO.[1]

Unfortunately, while the AGD discussion paper *Equipping Australia Against Emerging And Evolving Threats* (the paper) provided for the inquiry is welcome as a supplement to the terms of reference and a guide to the department's thinking, it again fails the basic test of providing evidence or verifiable justification for many of the proposals under consideration in this inquiry. What explanation there is relates to some of the minor proposals, for example the updating of the *Australian Security Intelligence Organisation Act 1979* to bring it into line with current Australian Public Service terminology.

For more significant proposals, however, there is minimal explanation; of great concern is that two of the most controversial proposals (albeit not at this stage supported by the government), to retain user data for 2 years, and to criminalise refusal to assist with decryption, are entirely omitted from the paper beyond the terms of reference. Indeed, the paper bears the appearance of having been in

[1] http://www.crikey.com.au/2011/10/20/asio-reels-in-a-g-line-on-illegal-fishing-hook-line-and-sinker/

effect stitched together from input from different areas of AGD, with no attempt made to ensure any sort of consistency of treatment across varying issues.

The AGD approach is instead to justify the overall approach outlined in the paper on the basis that

> *[T]he interception regime provided by the current Act reflects the use of telecommunications and the structure of the telecommunications industry that existed in 1979 when the Act was made. Many of these assumptions no longer apply, creating significant challenges for agencies in using and maintaining their investigative capabilities under the Act. In the absence of urgent reform, agencies will lose the ability to effectively access telecommunications, thereby significantly diminishing the collective ability to detect, investigate and prosecute threats to security and criminal activity.*

However, the broad argument that a change in communications technology and consumer usage of technology justifies the extension of the surveillance laws established for telecommunications to the internet is deeply flawed. The specific problems with this claim will be address in section 4.3, but more fundamentally, the justification in effect places opponents of the proposals contained in the paper in the position of proving a negative *i.e.* why shouldn't the same rules apply to the internet as to telecommunications?

But the burden of proof must rest with those advocating any amendments to the surveillance and intelligence-gathering laws that will give more power to law enforcement, intelligence and security agencies and reduce the rights and privacy of citizens. There should be no automatic assumption that, in effect, 'what is good for telecommunications is good for the internet'.

On that basis, AGD should explain exactly what features of the current laws are problematic – in effect, what agencies cannot now do that they wish to be able to do – how the proposed measure would remedy this failing, what risks are associated with the measure and an assessment of the trade-off between the benefits of greater surveillance and intelligence-gathering versus the costs of the personal privacy and civil rights. Such explanation and justification need not breach the confidentiality of intelligence or law enforcement operations

The paper comprehensively fails to make such a case except in relation to a few limited proposals. In short, AGD has not made the case for change.

In sections 2-4, some comments on specific proposals identified in the terms of reference and discussed in the paper are offered.

2. "MATTERS THE GOVERNMENT WISHES TO PROGRESS"

2.1 Safeguards and privacy protections

1. *Strengthening the safeguards and privacy protections under the lawful access to communications regime in the Telecommunications (Interception and Access) Act 1979 (the TIA Act). This would include the examination of:*
   a. *the legislation's privacy protection objective*
   b. *the proportionality tests for issuing of warrants*
   c. *mandatory record keeping standards*
   d. *oversight arrangements by the Commonwealth and State Ombudsmen.*

The paper is unclear about exactly what "strengthening" is intended beyond a review and consideration of "a privacy focused objects clause". Strengthening privacy laws and reviewing checks and balances is of course unobjectionable; but AGD has failed to even clearly describe its thinking on this important issue.

In relation to record-keeping standards and oversight by Ombudsmen, far from strengthening protections, the paper appears to advocate watering them down. AGD has imported the language of private sector critics of regulation, claiming current requirements represent "a one size fits all approach, resulting in a lack of flexibility for each agency to determine the best way to record and report on information having regard to individual practices, procedures and use of technology."

An alternative view is that "inflexible" and "one size fits all" provisions ensure that agencies cannot try to avoid reporting obligations and report in a manner that will enable meaningful comparisons over time and with other agencies. For relatively minor regulatory requirements, a "co-regulatory approach" such as that proposed by AGD might be appropriate, but given the serious nature of the issues on which law enforcement and intelligence agencies are being asked to report, it is wholly inappropriate to leave it up to agencies themselves to determine exactly how and what they report within a general remit. This would represent a significant weakening of accountability in an area where there is already too little scrutiny.

2.2 Reforms to lawful access

2. *Reforming the lawful access to communications regime. This would include:*
   a. *reducing the number of agencies eligible to access communications information*
   b. *the standardisation of warrant tests and thresholds*

Again, the paper does not discuss these proposals in detail; curtailing the number of agencies able to intercept data is a positive, but in the absence of an explanation of the basis for the revised approach (*i.e.* who will henceforth be

eligible, and why), hard to assess. On the other hand, the "standardisation of warrant tests and thresholds" is an unsubtle attempt to *lower* warrant tests and thresholds. Judging by the paper, which approvingly cites a 3 year minimum for some current warrants, the intention is to reduce the threshold for all interception and storage warrants to 3 years from, in many cases, 7 years. This is not "standardisation", this is a significant widening of current powers.

The only examples evinced by AGD in justification of this relates to the inevitable "child exploitation offences" and computer crime. Simple logic would suggest that either these offences are considered serious enough to justify interception measures, or they're not; if the former, the penalties associated with them should be appropriately severe, rather than using them as the basis for dramatically increasing the number of offences for which law enforcement and intelligence agencies can violate the privacy of Australians.

2.3 Streamlining and reducing complexity

> *3. Streamlining and reducing complexity in the lawful access to communications regime. This would include:*
>
> *a. simplifying the information sharing provisions that allow agencies to cooperate*
>
> *b. removing legislative duplication*

The argument that information should be more easily shared between agencies is a glib one, and the only justification advanced in the paper is that "effective co-operation within and between agencies is critical." This of course is assertion rather than argument; no effort is made by AGD to explain what failings are currently occurring because of the legislative restraints on his intercepted data can be shared.

This also appears to contradict the goal of "reducing the number of agencies eligible to access communications information" and further undermines the argument for a "co-regulatory" approach to record-keeping and oversight arrangements in which different agencies would be able to determine different standards and approaches in relation to their compliance obligations. AGD has offered no justification for violating the long-standing philosophy that intercepted information should only be used for the purposes for which it was collected, rather than becoming a common treasure trove to be dipped into by all law enforcement and intelligence agencies at will.

2.4 Cost-sharing

> *4. Modernising the TIA Act's cost sharing laws to:*
>
> *a. align industry interception assistance with industry regulatory policy*
>
> *b. clarify ACMA's regulatory and enforcement role*

In relation to the clarification of ACMA's regulatory role, the committee would benefit from consideration of paper commissioned by the then-Australian

Broadcasting Authority in relation to its broadcasting regulatory powers, by Professor Ian Ramsay.[2] While obviously limited to a portion of ACMA's powers, *Reform of the broadcasting regulator's enforcement powers* is a valuable analysis of regulatory theory that should provide the basis for an effective regulator's suite of tools for achieving effective industry regulation.

Prof Ramsay's report formed the basis for the Howard Government's 2006 amendments to the *Broadcasting Services Act* that extended ACMA's powers. In particular, it addressed the issue of a lack of "mid-tier" powers, which is a similar issue to that raised by AGD in the paper in relation to powers to enforce compliance with the TIA Act. On this issue, a power to accept enforceable undertakings, and a power to issue infringement notices, would appear to be two mid-tier powers worth considering to enable ACMA to enforce compliance without resorting to litigation.

The paper's proposal for a tiered model for cost sharing that distinguishes between large carriage and carriage service providers and medium and smaller ones is sound and accurately reflects fundamental changes in the communications industry in recent decades. However, a fundamental principle of any new model for cost-sharing should be the assumption that government bear *all* costs of interception, including capital costs, unless a case is proven to the contrary. Moreover, such costs should be fully transparent and publicly reported, to strengthen scrutiny of law enforcement and intelligence agencies.

2.5 Modernising the *ASIO Act 1979* and the *Intelligence Services Act 2001*

5. *Amending the ASIO Act to modernise and streamline ASIO's warrant provisions*
    a. *to update the definition of 'computer' in section 25A*
    b. *enabling warrants to be varied by the AG, simplifying the renewal of the warrants process and extending duration of search warrants from 90 days to 6 months.*

6. *Modernising ASIO Act employment provisions by:*
    a. *providing for officers to be employed under a concept of a 'level,' rather than holding an 'office.'*
    b. *Making the differing descriptions ('officer,' 'employee' and 'staff') denoting persons as an 'employee' consistent*
    c. *Modernising the Director•General's powers in relation to employment terms and conditions*
    d. *Removing an outdated employment provision (section 87 of the ASIO Act)*
    e. *Providing additional scope for further secondment arrangements*

---

2 http://www.acma.gov.au/webwr/aba/newspubs/radio_tv/investigations/documents/enforcementpowers.pdf

7. *Amending the Intelligence Services Act 2001 to clarify the Defence Imagery and Geospatial Organisation's authority to provide assistance to approved bodies.*

The relevant section of the paper articulates a strong, coherent case for this range of minor administrative reforms improving the functionality of current powers under the ASIO and Intelligence Services Acts. It is regrettable that a similarly strong case was not made in relation to more significant proposals.

3. MATTERS THE GOVERNMENT IS CONSIDERING

3.1 Extending the surveillance laws

> 9. *Modernising the Industry assistance laws –*
> a. *implement detailed requirements for industry interception obligations*
> b. *extend the regulatory regime to ancillary service providers not currently covered by the legislation*
> c. *implement a three-tiered industry participation model*

Bizarrely, it is under the rubric of "modernising cost sharing" that one of the most controversial proposals of the paper is offered – to extend surveillance and intelligence-gathering laws to social media providers. This would represent a dramatic extension of surveillance powers into an entirely new area of activity, with the sole justification that the current "exclusion" of social media providers "creates potential vulnerabilities in the interception regime that are capable of being manipulated by criminals".

There are a number of profound flaws with this proposal, and with the thinking of AGD officials that has evidently motivated it.

Firstly, if the goal of incorporating social media into surveillance systems is to capture networks being "manipulated by criminals" beyond the current reach of law enforcement and intelligence agencies, it is doomed to failure. There are a wide range of social media platforms, broadly defined, that can potentially be used for illicit communication. They include not merely the most obvious platforms such as Twitter and Facebook, or platforms that have recently come to prominence in the context of criminal justice overseas such as BlackBerry Messenger, but non-Anglophone equivalents of western platforms such as Sina Weibo, Skyrock or Cyworld; legacy platforms no longer widely used in Anglophone countries but still popular in non-Anglophone countries like Friendster (now a social gaming site, but with social network features); gaming platforms accessible via XBox 360 and PS3 that permit in-game chat and discussion on a global basis, innumerable chat applications and chat functions of communications platforms such as Skype; blogging applications like Wordpress and microblogging applications like Tumblr that allow text-based communication, collaborative tools like Pastebin and Google Docs, instant messaging clients, including ones with extensive encryption capabilities like Adium, and comparatively ancient communications platforms based on IRC.

All of those platforms are easily accessible by users for communication purposes and thus by the criminals about whom AGD expresses concern. They vary widely in function and operation. Moreover, they are constantly proliferating: Pinterest didn't exist before 2010 and by the end of 2011 was one of the top 10 social network sites. This creates two problems for legislators: one, how to define the "social networking providers" AGD wishes to bring within the surveillance laws without, in effect, bringing the entire internet within its definition, and two, how

to address the inevitable rapid proliferation of other platforms that may not fit within current definitions.

Secondly, virtually no significant social networking provider, to use the AGD term, is based within Australia. The proposal to bring social networking providers within Australian government surveillance laws thus would purport to extend Australian legal jurisdiction offshore to a wide variety of countries, a form of extraterritoriality much favoured by the US government but in our case without the economic power and critical internet role that the US plays. Moreover, how can Australian agencies guarantee appropriate evidence management or privacy control of intercepted information while operating extra-jurisdictionally?

Further discussion of this proposal is found at section 4.3.

3.2 Protection from criminal and civil liability for ASIO officers

> *10. Amending the ASIO Act to create an authorised intelligence operations scheme. This will provide ASIO officers and human sources with protection from criminal and civil liability for certain conduct in the course of authorised intelligence operations.*

Again, AGD has failed to establish the case for such an amendment. Australians have a legitimate expectation that all public officials will act with honesty and integrity at all times in the discharge of their responsibilities. While plainly undercover intelligence operations, being based fundamentally in deception, differ significantly from most public service roles, the paper proposes to permit ASIO officers to engage in all criminal behaviour short of inducing a person to commit a criminal offence not otherwise intended, homicide or serious injury, or sexual offences. This would, accordingly, permit ASIO officers to engage in crimes that may injure others, or major property crimes, in the course of their duties. At no point does AGD explain what ASIO is currently unable to achieve in the absence of a scheme enabling its officers to breach the law.

Moreover, there are concerns that ASIO officers already enjoy a form of immunity from prosecution. For example, the officers responsible for the kidnapping and false imprisonment of Izhar ul-Haque in 2003 have never been brought to justice or even exposed to public scrutiny. The ability of ASIO officers to hide behind legislative prohibitions on the revelation of their identity means that they need never fear justified public obloquy if they offend community standards or break the law during the course of their work. There is also precedent that such authorisations can be abused: an undercover police officer is alleged to have planted and detonated a bomb in a London department store in 1987 merely in order to prove his *bona fides* to an extremist animal rights group.[3]

[3] http://www.dailymail.co.uk/news/article-2158725/Undercover-police-officer-planted-firebomb-department-store-animal-rights-protest.html

If the Committee is of a mind to seriously consider the AGD proposal in the absence of any public justification for it, its attention is drawn to the Canadian government's 2000 proposal in relation to providing immunity from criminal liability for police committing acts during an investigation that, in ordinary circumstances, would be illegal.[4] The Canadian government proposal was highly circumscribed and conditional, and reflected the following principles:

- Distinguishing between acts or omissions with less serious consequences and more serious ones, that may require a higher level of approval or different form of approval.

- Ministerial authorization for more serious offences (rather than, as proposed in the paper, approval by the Director-General of ASIO.

- Causing bodily harm not to be permitted except if "on reasonable grounds that it is necessary to preserve the life or safety of any person, or to prevent the compromise of the identity of a public officer acting in an undercover capacity, a confidential informant or a person acting covertly under an officer's direction, or the loss or destruction of evidence of an indictable offence"

- No authorisation for failing to comply with requirements relating to surveillance or gathering of evidence.

- Providing authorisations for human sources who are not officers only for acts under the direction and control of an officer.

3.3 Permitting disruption of computers

> *11. Amending the ASIO Act to modernise and streamline ASIO's warrant provisions to:*
>
> *…*
>
> *c. Enable the disruption of a target computer for the purposes of a computer access warrant*

The proposal to permit ASIO agents to "disrupt" computers identified in warrants is deeply concerning. While ostensibly limited to "activity proportionate to what is necessary to execute the warrant", the proposal opens the door to a range of problems. More cynical observers might suggest ASIO agents may use "disruption" to plant evidence on targeted computers, or destroy information unrelated to the warrant; more plausibly, defendants will be able to claim that such behaviour has occurred.

However, there is already an example of what can go wrong when state agencies place material on computers designed to facilitate surveillance. In 2011, malware developed for German police was reverse-engineered and analysed by

[4] http://www.ulcc.ca/en/criminal/index.cfm?sec=4&sub=4g

the Chaos Computer Club.[5] The malware, designed to enable surveillance of target computers, was developed and used in accordance with German laws. It allowed keystroke logging, remote control of computer cameras and microphones and back-door functionality to enable authorities to add additional functions to the malware.

But due to poor design and encryption from the software company that manufactured the "Bundestrojaner" for German police, the malware had significant flaws: it could be exploited by any unauthorised third party, not just the federal agencies using the program, potentially enabling third parties to place material on companies infected with the malware (thus, "planting" of evidence) or use of the computers for cybercrime, and might even have allowed third parties access to agencies' IT infrastructure as well. The malware also routes information through a server located in the US, to avoid identification of the source of external commands, thereby exposing the data to US *Patriot Act* control.

A recurrent theme in 2011 was the ease with which the IT infrastructure of governments, their agencies, the firms to which they outsource functions and large corporations could all be penetrated by even relatively inexperienced hackers intent on causing embarrassment, let alone those engaged in criminal or espionage activities. On this basis, one can have little confidence that an Australian government agency will be able to develop a fully secured piece of malware that would address the types of concerns immediately raised by the Bundestrojaner.

3.4 Publication of the identity of an ASIO officer

> *12. Clarifying ASIO's ability to cooperate with the private sector.*
> *13. Amending the ASIO Act to enable ASIO to refer breaches of section 92 of the ASIO Act (publishing the identity of an ASIO officer) to authorities for investigation.*

No well-informed comment on 12 is possible as no information is available about ASIO's relationships with the private sector. Public service agencies are routinely required to provide details of contracts with private sector providers. ASIO is not subject to this, and accordingly citizens and taxpayers have no idea of the extent of outsourcing, contracting or other forms of cooperation with the private sector that currently occurs.

In relation to referring breaches of s.92 of the ASIO Act, again, AGD has provided no justification or explanation of why the current prohibition on publishing the identity of an ASIO officer should be amended.

---

5 http://www.dailytech.com/German+Hackers+Govt+Trojan+Capable+of+Planting+Evidence+Cybercrime/article22966.htm

Indeed, the s.92 prohibition needs fundamental reconsideration, given the paper argues that technological change has created a need for updating the surveillance laws. A consequence of the proliferation of wireless internet access and smart phones is that governments no longer have a monopoly on surveillance. The "panopticon" has now been reversed, and the watchers and the watched are alike under surveillance: police and many government officials as well as the public may now be filmed at any time in the course of the performance of their duties by the public.

Australian police forces, including the AFP, have generally indicated no concerns about being under permanent public surveillance in this manner; indeed, one Australian police force explicitly welcomed the idea that its officers would always potentially be under surveillance.[6] Given ASIO officers have repeatedly been found monitoring legal protest actions, ASIO and AGD must give serious thought to how they handle the likelihood that at some point ASIO officers will be filmed and the footage posted online, thereby in effect "publishing the identity of an ASIO officer". Perhaps this has already occurred and is the motivation for the proposed amendment. Regardless of whether the amendment ultimately proceeds, consideration must be given to this issue rather than a simple assertion of a command-and-control approach.

[6] http://www.crikey.com.au/2011/11/01/reversing-the-panopticon-police-officially-relaxed-about-being-filmed/

4. MATTERS ON WHICH THE GOVERNMENT IS SEEKING VIEWS

4.1 Telecommunications

14. Reforming the Lawful Access Regime
a. expanding the basis of interception activities

See comments under s. 4.3

4.2 Criminalising failure to assist in decryption

15. Modernising the Industry assistance laws
a. establish an offence for failure to assist in the decryption of communications

Any attempt to compel assistance in decryption, such as the provision of passwords, is a clear violation of two core principles of the Australian criminal justice system, the right to silence and the privilege against self-incrimination. These principles have been held by the High Court to be "integral to the protection of the natural legal person in a criminal justice system in which inquisitorial methods have no place."[7] In this case, there is no basis to make the distinction, which the High Court has considered in the past, between the right to silence and the privilege against self-incrimination, and the production of documents that may reveal guilt; clearly "assisting in decryption" constitutes a separate communication (most likely, of a password or cryptographic key) in addition to whatever materials may be revealed by decryption.

The right to silence has already been abrogated in the name of counter-terrorism by the Howard government's draconian 2002 terrorism laws. However, that abrogation related only to terrorism and associated offences. The AGD proposal would in effect extend an already profoundly troubling curtailment of basic rights across *all* offences.

Under Commonwealth law, the privilege against self-incrimination may only be overridden for witnesses if a certificate is provided guaranteeing evidence will not be used against them in other proceedings. Establishing an offence in relation to refusal to assist in decryption would, in a manner similar to the 2002 terrorism laws, extend an existing exemption, in this case one pertaining to criminal trials, to pre-trial investigations.

Moreover, AGD has yet again publicly failed to make the case for such a profound attack on basic rights. Indeed, there is no justification or discussion of any kind whatsoever for this proposal. The committee is urged in the strongest possible terms to reject it.

[7] http://www.austlii.edu.au/au/journals/MqLJ/2001/3.html

4.3 Data retention

> *c. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts*

As with the proposal to criminalise the right to silence and privilege against self-incrimination in relation to decryption, AGD fails to even discuss the basis for one of the paper's most draconian and far-reaching proposals, let alone articulate a case for it.

In particular, AGD has failed to explain why a 2 year data retention regime is required beyond the existing regime in which data is temporarily retained for business purposes and intelligence and law enforcement agencies can request data storage via warrant.

Indeed, AGD is currently in the throes of expanding the existing laws for data storage via the draconian Cybercrime Legislation Amendment Bill 2011, currently before Parliament, which proposes to permit foreign governments to request data storage and for Australian citizens' user data to be handed over to foreign governments. That is, AGD has put forward for discussion a dramatic and far-reaching expansion of the existing data storage regime before its most recent expansion has even passed Parliament.

There are four issues that illustrate why data retention should be rejected outright by the committee and in the strongest terms.

<u>The internet is not a phone</u>

The first goes to the broader issue raised by the paper, and other proposals, that an expansion of the "telecommunications era" surveillance laws to the internet is required because communications have shifted from a single, easily-controlled platform – the phone – to a wide range of online platforms.

The analogy that forms the basis of this argument, between analog-era telecommunications and the internet, is profoundly flawed.

Australians, like citizen around the world, do not use online communications in the same way, or for the same purposes, as they used phones. They did not commit huge amounts of personal information to permanent storage on the phone. They did not leave crucial financial details on the phone. The phone was not their primary tool for interacting with communities that are important to them. The telephone did not enable contact with communities around the globe that are of critical importance to citizens.

Australians now live significant portions of their lives online in a way impossible with the phone. Personal relationships, recreation, media consumption, political activity, civic participation (including, potentially, voting), economic activity and employment all occur online.

Any attempt therefore to impose the telecommunications interception laws on the internet represents not a logical extension of that laws to "keep up with technology" on a like-for-like basis but a dramatic extension of surveillance into citizens' lives far beyond that enabled by telecommunications interception.

Australians have traditionally guarded against such surveillance in their day-to-day lives. They expect, and the state has accepted, that their personal lives, recreation, employment and civic engagement will be free of routine monitoring by government, that there is no threat great enough to justify routine intervention in and surveillance of Australians' day-to-day activities by the state.

The tenor of the paper, and a number of its specific proposals, most particularly in relation to data retention, seeks to clearly overturn this tradition and impose state surveillance on huge areas of Australians' everyday lives.

Nor is it relevant to argue that the data targeted by a data retention regime is only traffic data rather than content data. Traffic data, particularly when it includes data derived from mobile phones enabling geographical tracking, is sufficient to extensively profile an individual citizen, their habits, relationships, interests and movements.

No threat justifies such a fundamental rejection of the historic tradition that we do not permit the state to monitor our lives. That AGD has failed to even attempt such a justification is of a piece with its long history of convincing parliament to pass ever-more draconian surveillance laws with minimal scrutiny or public accountability.

Impacts on C/CSPs

Despite the sections of the paper devoted to cost-sharing in relation to surveillance, an emerging theme in AGD's proposals for ever-greater extensions of the surveillance laws is a blithe assumption that data storage is somehow cost-free and straightforward for affected companies such as ISPs and telecommunications companies.

This emerged in the rushed, inadequate Senate committee consideration of the Cybercrime Legislation Amendment Bill 2011 and subsequent discussions between key stakeholders such as Telstra and AGD, in which AGD's simplistic assumptions about the ease and inexpensive nature of data retention were found to be false.[8] As Telstra told the committee examining the bill in relation to data preservation for 180 days, "[i]n some cases, the existing networks may require significant modifications or even replacement to ensure compliance with such long information preservation periods."

[8] http://www.crikey.com.au/2011/09/21/cybercrime-bill-to-be-debated-in-senat/

Plainly that applies to a vastly greater degree to a two-year data retention scheme for all citizens. Such a huge cost logically must be borne either by C/CSPs or by taxpayers; if the former, it represents a vast imposition on the industry that would be likely to force smaller providers out of business, reducing competition. Even if borne by taxpayers, there would still be impacts on competition; the more elaborate infrastructure protection and national security obligations for the communications industry become, the higher the barriers to entry for new firms are raised, giving incumbents, with established networks and relationships with governments, a significant advantage.

None of these issues are broached by AGD in the paper. Assuming costs would be shared between industry and the government, there is no discussion of the likely fiscal impact. While the proposal's status as one on which the government is seeking views would make a full costing (presumably agreed with the Department of Finance) unnecessary at this point, and not require a Regulation Impact Statement, the lack of any detail in relation to the costs is an impediment to informed discussion.

Security of retained data

While large C/CSPs may be able to more effectively secure a large amount of data, as the paper acknowledges elsewhere, the surveillance and intelligence-gathering laws now includes a range of industry stakeholders including small and medium-sized firms.

It has become clear over the last 18 months that even large corporations with strong incentives to keep data secure are vulnerable to cracking by organised crime, other states or activists, or simply lazy about security of personal information. This has included the Australia telecommunications provider Vodafone, which was revealed in early 2011 to have allowed – not via cracking or illegal action by outside actors, but through its own poor internal processes – widespread access to personal information about its 4 million customers.[9]

The recent history of personal information security in Australia and overseas suggests that both citizens and law enforcement agencies, intelligence agencies and prosecutors can have little confidence that information compiled under data retention laws would be effectively secured by all companies required to hold it, either from a privacy or from a investigative/prosecutorial point of view. Even assuming a strong commitment to data security by providers and a statutory laws for data protection by government, such repositories of information would be highly-prized treasure troves for organised crime, corporations and even foreign governments, and inevitably targeted by crackers.

[9] http://www.smh.com.au/technology/security/mobile-security-outrage-private-details-accessible-on-net-20110108-19j9j.html

Offshore data retention?

The data retention proposal would inevitably require an attempt by the Australian government to impose data retention on foreign-based service providers. While the data retention proposal may not be intended for social media, as proposed in relation to other extensions of the surveillance and intelligence-gathering laws discussed in the paper, VOIP services such as Skype, Google Voice or FaceTime would clearly need to be included in the data retention proposal.

Not merely does this raise the problem of how Australia can purport to impose its legislative will on firms based offshore, and the problem of ensuring that all new VOIP services (such as, for example, mobile VOIP applications) are covered. It also deepens the problem of assuring that data is retained securely both from a privacy and from an investigative/prosecutorial point of view: what Australian court would accept the assurances of a small foreign firm that it had met data retention standards without independent verification, when the data forms part of the evidence for a criminal trial?

4.4 Government intervention in the telecommunications industry

> *16. Amending the Telecommunications Act to address security and resilience risks posed to the telecommunications sector. This would be achieved by:*
>
> *a. by instituting obligations on the Australian telecommunications industry to protect their networks from unauthorised interference*
>
> *b. by instituting obligations to provide Government with information on significant business and procurement decisions and network designs.*

These proposals represent a significant government intervention in the commercial operations of private businesses, and provide the federal government with a power to compel members of the telecommunications industry to operate their businesses according to government priorities, rather than commercial priorities, backed by the threat of fines. The imposition of a régime under which senior public servants can direct telecommunications companies to undertake potentially costly infrastructure upgrades or protective measures on the basis of non-commercial determinations made by bureaucrats would represent a significant commercial risk for companies, particularly given the track record of AGD in relation to the Cybercrime Legislation Amendment Bill 2011. It should not be considered without discussion of appropriate compensation for telecommunications companies that would in effect have their property partially expropriated.

4.5 Third party interception

17. *Amending the ASIO Act to modernise and streamline ASIO's warrant provisions by:*
    a. *Using third party computers and communications in transit to access a target computer under a computer access warrant.*
    b. *Clarifying that the incidental power in the search warrant provision authorises access to third party premises to execute a warrant*
    c. *Clarifying that reasonable force may be used at any time during the execution of a warrant, not just on entry.*
    d. *Introducing an evidentiary certificate regime*.

The extension of surveillance and intelligence-gathering laws to third party computers *i.e.* to place under surveillance the computer equipment of people who are suspected of no crime, is a significant infringement of privacy, and one for which AGD has yet again provided no justification. The proposal discussed in section 3.3 would also presumably apply to third party computers, opening up citizens suspected of no crime to spyware and other forms of malware. The point made in section 4.3 bears repetition: there is no analogy between telephone and online communications; the interception of online communications is a significantly greater infringement of privacy that interception of telephone communications, with far greater costs to citizens. The casual use of interception of the internet activities of a citizen purely because it will make the operations of law enforcement or intelligence officers more convenient is wholly unjustified.

5. CONCLUSION

In a 2011 paper, US academic John Mueller and University of Newcastle's Mark G. Stewart discussed the cost of the US "war on terror" and how to determine whether the expenditure had been justified.[10] One of the key points made by Mueller and Stewart is that considerable – in fact truly extraordinary – expenditure has been justified by governments through inconsistent, illogical and plain deceptive use of statistics about the real risk of a terrorist attack and, in particular, how much that already very low risk is further reduced by additional expenditure. Their observations are worth quoting at length:

> *In assessing risk reduction, it is important first to look at the effectiveness of homeland security measures that were in place before 9/11 in reducing risk. The 9/11 Commission's report points to a number of failures, but it acknowledges as well that terrorism was already a high priority of the United States government before 9/11. More pointed is an observation of Michael Sheehan, former New York City Deputy Commissioner for Counterterrorism:*
>
> > The most important work in protecting our country since 9/11 has been accomplished with the capacity that was in place when the event happened, not with any of the new capability bought since 9/11. I firmly believe that those huge budget increases have not significantly contributed to our post-9/11 security....The big wins had little to do with the new programs.
>
> *As this suggests, police and domestic intelligence agencies have long had in place procedures, techniques, trained personnel, and action plans to deal with bombs and shootings and those who plot them. Indeed, according to 9/11's chief planner, Khalid Sheikh Mohammed, the greatest difficulty the plotters faced was getting their band of terrorists into the United States. It may be even more difficult now, but the strictures before already presented a considerable hurdle.*
>
> *There is another consideration. The tragic events of 9/11 massively heightened the awareness of the public to the threat of terrorism, resulting in extra vigilance that has often resulted in the arrest of terrorists or the foiling of terrorist attempts. Indeed, tip-offs have been key to prosecutions in many of the terrorism cases in the United States since 9/11.*

To summarise, each additional expenditure on counter-terrorism is in pursuit of ever-smaller reductions in already very low risk, and this must form part of a valid assessment of the benefits of such expenditure.

The same logic applies to each additional infringement of privacy and basic civil rights proposed by government.

The paper states that "[s]ince 2001, four mass casualty attacks within Australia have been disrupted because of the joint work of intelligence and law

[10] http://polisci.osu.edu/faculty/jmueller/MID11TSM.PDF

enforcement agencies. Since 2001, 38 people have been prosecuted in Australia as a result of counter-terrorism operations and 22 people have been convicted of terrorism offences under the Criminal Code Act 1995…" Putting aside that the description "mass casualty" is not verifiable given the publicly available details about the planned terrorist attacks to which the paper is presumably referring, plainly the current surveillance and intelligence-gathering laws have enabled a number of operational successes.

Any further amendments to those laws are therefore likely, even on the best-case scenario, to reduce the risk of a successful terrorist attack by a negligible additional amount beyond the reductions already achieved by existing laws.

The key challenge, which the department has comprehensively failed in the paper, is to explain what *additional* reductions in the risk of successful terrorist attacks will be achieved through the significant additional infringements in privacy and basic rights proposed in the paper, which will enable us to assess the net benefit or cost when that reduction is compared to the impacts.

Of course, the proposals in the paper are not exclusively targeted at terrorism. Espionage, organised crime and cyber crime are all mentioned. But claims about the impact of cyber crime are wildly overblown: a report purporting to estimate the impact of cybercrime in Australia last year was revealed to be heavily on including computer viruses and online bullying in its definition of "cybercrime".[11] A recent analysis has revealed the flawed nature of similar claims made overseas.[12] US academics Jerry Brito and Tate Watkins earlier this year exposed the thin justification for many claims made about cyber-espionage and the possibility of "cyber war".[13]

This routine inflation of the threat of cyber crime appears partly driven by IT security companies eager to extend the market for their IT security and anti-malware products, and partly by "cyberhawk" politicians eager to whip up concerns about a "digital Pearl Harbour".[14] The result is the evolution of what I have previously termed a cyber equivalent of the military industrial complex, with ever-growing budgets, even at a time of fiscal austerity extending to traditional military budgets, for cyber warfare.

The recent history of amendments to Australia's surveillance and intelligence-gathering laws is of constant expansion of the powers of government agencies at the expense of citizens, with limited or no justification advanced by proponents beyond broad invocations of external threats. There has been little debate about the trade-offs between the remorseless creep of surveillance powers and the

---

[11] http://www.crikey.com.au/2011/09/12/internet-shock-huge-cost-of-cybercrime-revealed-by-cyber-security-firm/
[12] http://www.propublica.org/article/does-cybercrime-really-cost-1-trillion
[13] http://mercatus.org/publication/loving-cyber-bomb-dangers-threat-inflation-cybersecurity-policy
[14] http://www.crikey.com.au/2011/08/03/digital-pearl-harbors-make-for-a-good-year-for-the-cyber-defence-industry/

privacy and basic rights citizens have lost as a consequence. The Committee, in undertaking a public inquiry, has the opportunity to begin correcting this long-term problem. Its priority should be to require AGD, its portfolio agencies and other member agencies of the Australian Intelligence Community to justify in detail each of the proposals advanced, to identify the specific benefits to the national interest from each, and enable citizens to consider the benefits versus the inevitable costs they will endure as a result of them.