Submission by

Guardian Australia

to the

Parliamentary Joint Committee on Intelligence and Security
(the Committee)

Inquiry into the National Security Legislation Amendment Bill (No. 1) 2014
(the Bill)

Summary

Guardian Australia is part of Guardian News and Media, which through its editorial operations in the United Kingdom, United States and Australia publishes its journalism at www.theguardian.com and in daily, Sunday and weekly newspapers.

The Guardian shared the 2014 Pulitzer Prize for public service for its reporting on the surveillance activities of governments disclosed by the whistleblower Edward Snowden.

In essence, Guardian Australia submits to this inquiry that,

in light of

international developments relevant to this inquiry,
the significance of the powers and immunities being contemplated, and
the weighty public interests to be balanced in this Bill,

the Committee -

- **require from Executive Government and its agencies a higher level of evidence and explanation to demonstrate the necessity** of the powers and immunities being sought,

- **find that the powers and immunities currently sought are disproportionately strong and the safeguards currently proposed disproportionately weak**, and

- **recommend a mix that better balances for Australia's democratic society the public interests** in security, freedom of expression and freedom of the press, privacy, freedom of association and accountable government.

It is not easy to comprehend all that is intended by the Bill because of its inherent complexity, the need to cross-reference the Bill with the several statutes it would amend, the vagueness of some of the language, and the fact that the Committee's 2013 Report[i], on

which the Bill is said to be based, did not explore in detail all that the Bill appears to incorporate.

As the Committee's then chairman wrote in his foreword to the 2013 report, that inquiry was seriously hampered. Its terms were very wide, there was no draft legislation to consider, and there was a dearth of information about the controversial topic of data retention –

> Importantly the Committee was very disconcerted to find, once it commenced its Inquiry, that the Attorney-General's Department (AGD) had much more detailed information on the topic of data retention. Departmental work, including discussions with stakeholders, had been undertaken previously. Details of this work had to be drawn from witnesses representing the AGD.[ii]

It helps at the outset to summarise in plain language what Parliament is being asked to endorse. The Bill would strengthen agencies which already necessarily work in secret and with limited oversight, which utilise increasingly invasive technologies of surveillance, and which work in the company of Five Eyes partners, some of whom have recently put in doubt their fidelity to law and their candour in accounting to oversight entities, including elected representatives.[iii]

If passed in its current form, it appears the Bill would –

> **increase significantly the extent to which intelligence and security agencies could intrude into and disrupt the lives of others**, including people who are not targets but whose computers are connected to networks which targets' computers may share;
>
> **increase the capacity** for the domestic intelligence agency, Australian Security Intelligence Organisation (ASIO), to co-operate with the foreign intelligence agency, Australian Secret Intelligence Service (ASIS), **to collect intelligence about Australians** – the immediate context is concern about Australians fighting in foreign conflicts, but the powers potentially have wider application;
>
> **facilitate more formal exchanges between personnel** from intelligence and security agencies and personnel from other parts of the Australian Public Service, with the risk, identified by the Inspector-General of Intelligence and Security, that existing safeguards may be circumvented;[iv]
>
> **immunise operatives of intelligence and security agencies from the usual consequences of breaking the criminal and civil law in certain circumstances;**
>
> **criminalise acts which enhance accountability** and which are of proven value in a democratic society, in particular the cultivation by journalists of sources and disclosures that can augment the oversight work of Executive Government, Parliament and the Judiciary;
>
> **expose to heavy jail terms persons engaged in legitimate acts of democratic scrutiny**, including whistleblowers, journalists, academics and civil society organisations concerned with liberty, government accountability and the rule of law.

To acknowledge that the powers and immunities proposed in the Bill have some limitations and are accompanied by some oversight is not the same as concluding that the powers, immunities, limitations and oversight would together result in what is both necessary and proportionate in a democratic society.

Guardian Australia submits that this Committee should apply rigorously the tests of necessity and proportionality to every element of the Bill.

Aware of the expertise of other likely submitters to this inquiry, particularly in relation to the warrant powers, Guardian Australia will focus on the implications of the proposed new special intelligence operations scheme and its associated powers, immunities, offences and penalties – new Division 4 Part III, sections 35A-35R of the Bill.

Before doing so, the Committee's attention will be drawn to the international context in which this legislation is being proposed.

Guardian Australia made a submission to the Senate Legal and Constitutional Affairs Committee inquiry into the comprehensive revision of the *Telecommunications Act (Interception and Access) Act 1979* and will not repeat its arguments and sources.[v] We simply note that this Parliamentary Joint Committee on Intelligence and Security has in the past recommended a review of oversight arrangements to ensure effective accountability under the TIA Act and we urge that the work of this Committee in the current inquiry and of the Senate Committee in the TIA Act inquiry be co-ordinated. A recurring difficulty in ensuring appropriate scrutiny of legislation affecting freedoms can be the fragmented, incremental way in which formal processes empower agencies whose operations have the potential to compromise freedoms.

International context

Guardian Australia believes that this Committee shares the view that any national measures to increase the powers of intelligence and security agencies need to be considered in an international context.

This belief follows not only from Australia's membership of the Five Eyes group of nations - US, UK, Canada, Australia and New Zealand - which for many decades have co-operated on intelligence matters and which, it is reasonable to infer from the Snowden revelations, have shared in the fruits, if not the implementation, of projects of questionable legitimacy conducted mainly by the US National Security Agency.

This Committee's awareness of the international context is evidenced by its consultation, during the inquiry that led to its 2013 Report, with the British Intelligence and Security Committee. As your Report stated (para 1.12), the UK Data Retention and Investigatory Powers Bill had similarities to the potential Australian reforms.

On 15-17 July 2014 the UK Government fast-tracked a version of that legislation through the House of Commons and House of Lords over protests that haste undermines the legitimacy of security measures which have the potential to undermine liberty. A sunset clause was negotiated and a fuller inquiry was promised. During the debate the Liberal Democrat, Dr Julian Huppert, summarised previous iterations of the UK legislation and made comments that could equally be put to the Australian Parliament and its committees:

> All that was before the Snowden period, when we found out what was happening. What has the House done to reflect the concerns that people have about privacy, data and surveillance?....This House has failed to have the discussions and debates that have happened in the US, Germany and many other places. That leads directly to the scepticism about the bill that many people feel. There is a track record and people have developed concerns over many years. For decades we have had claims from the Government, again and again, about what is needed for security. So

> many clichés – the old lines: if we have nothing to hide we have nothing to fear. Every reference to everything is justified by a reference to terrorists or paedophiles. Of course these matter and are serious, but they are not the same as proper evidence-based arguments about what is needed and is proportionate.[vi]

In the US, in response to the Snowden revelations, President Obama commissioned an expert panel which in December 2013 recommended reform. His Review Group on Intelligence and Security Technologies highlighted the importance of an international perspective, stating -

> ...rapid changes include unprecedented advances in information and communications technologies; increased globalization of trade, investment, and information flows; and fluid national security threats against which the American public rightly expects its government to provide protection. With this larger context in mind, we have been mindful of significant recent changes in the environment in which intelligence collection takes place. For example, traditional distinctions between "foreign" and "domestic" are far less clear today than in the past, now that the same communications devices, software, and networks are used globally by friends and foes alike. These changes, as well as changes in the nature of the threats we face, have implications for the right of privacy, our strategic relationships with other nations, and the levels of innovation and information-sharing that underpin key elements of the global economy. In addressing these issues, the United States must pursue multiple and often competing goals at home and abroad. In facing these challenges, the United States must take into account the full range of interests and values that it is pursuing, and it must communicate these goals to the American public and to key international audiences.[vii]

The US Congress is currently negotiating amendments to intelligence and security legislation, with proposals sponsored by Senator Patrick Leahy[viii] winning considerable support[ix]. They include safeguards which the Committee may wish to consider, both in this inquiry and when the foreshadowed data retention legislation emerges.

Trust, legitimacy and safeguards

This international context is highly relevant to laws under which Australia's intelligence and security agencies operate, so it is puzzling to find no substantial reference to it in materials associated with the Bill.

While it is true that many of the Bill's proposals pre-date the first Snowden disclosures in June 2013, in the present international context it is not just artificial, but also counterproductive, to present legislation which significantly increases the powers and immunities of Australia's intelligence and security agencies, and severely penalises disclosures about them, as if the legislation were merely an act of modernisation.

The Snowden disclosures have shaken public trust in intelligence and security agencies which operate alongside Australia in Five Eyes. It has been shown that safeguards, many of them instituted because of earlier breaches of trust by such agencies, did not work as reasonably expected.

Australia is not isolated from the serious and urgent debate happening in many countries about the proper balance between liberty and security under which people in democratic, technologically rich societies may consent to live.

The Explanatory Memorandum to the Bill states, without elaborating, that the Bill is 'compatible with the human rights and freedoms recognised or declared in the [relevant] international instruments' and lists eight:

> the right to work
>
> the right to just and favourable working conditions
>
> the right to freedom from arbitrary detention and to liberty of the person
>
> the right to freedom of movement
>
> the right to a fair trial, presumption of innocence and procedural guarantees
>
> the right to protection against arbitrary and unlawful interference with privacy
>
> the right to freedom of expression
>
> the prohibition on cruel, inhuman or degrading treatment or punishment.

This substantial list suggests that the stakes are high for the balancing process in which this Bill involves the Committee and Parliament.

To the extent that the Attorney-General's Department is conflicted in its roles as servant of the intelligence and security agencies' legislative agenda and assessor of compliance with human rights obligations, Guardian Australia submits that the Committee should review for itself the Department's assessment of the Bill's compliance. Before the Legislature enacts law of this Bill's significance the public should hear the results of such a review from a committee of the Legislature, not mere bald assurances from the Executive about compliance.

The Ex Mem states that the Bill 'does not have a financial impact'. Leaving to one side queries about the expenditure which seems inherent in the use of some of the new powers, the statement begs the question whether the proposed safeguards will be effective if they are cost neutral.

It is a common complaint about watchdogs for Executive Government agencies that the watchdogs lack the resources necessary to carry out effectively the multiple oversight tasks which legislation gives them as a way of balancing the powers conferred on the agencies they watch. They must monitor, audit, handle complaints, conduct own-motion inquiries, assemble data and make reports.

The Committee is urged not only to ensure that safeguards are meaningful in law, but that they are meaningful in practice insofar as resources can ensure it.

Commitment to safeguards can be assessed in other ways.

Until recently it had been the current Australian Government's intention to abolish the office of the Independent National Security Legislation Monitor.[x] The term of the previous INSLM Mr Bret Walker SC ended in April 2014 and no replacement had been announced by the end of July.

In the recent UK parliamentary debate on legislation with similarities to this Bill, Lord Carlile of Berriew said –

> ...as a veteran of dealing with the Anti-terrorism, Crime and Security Act 2001 when I was independent reviewer of terrorism legislation, I remind your Lordships that Ministers who introduce legislation in haste are later left to repent it in panic.
>
> ...One of the things that were announced yesterday was the abolition of the independent reviewer of terrorism legislation, who is currently the brilliant David Anderson QC. We have heard much entirely justified praise of him in this debate, but he is being abolished. Can we have an explanation of why? Will the Minister please tell the House when Mr Anderson himself was first informed of the intended abolition of his post? How much earlier than yesterday was it? How long was he given to respond to the proposal? What arrangements exist for a full and proper consultation on the proposal to abolish the independent reviewer...?
>
> Will members of the board [to replace the independent reviewer] enjoy developed vetted access to be able fully to scrutinise counterterrorism activity by the services? It is crucial that, if his post is abolished, someone should have that access. It is important to have a positive assurance of that, otherwise what has been announced is a seriously retrograde step in terms of scrutiny.[xi]

Scheme for special intelligence operations (SIO) – new Division 4 Part III

Has the scheme been shown to be necessary?

In its 2013 Report the Committee noted that at least one submitter had challenged the necessity of the scheme and had argued that existing law enforcement agencies, using existing legal frameworks for controlled operations, could do what was necessary without Parliament further empowering the intelligence and security agencies. The Committee preferred the view of the Attorney-General's Department but did not provide much explanation for its recommendation. This may have been because, as noted above, the Committee lacked information and detail. A full explanation of the necessity of the scheme is overdue.

Why isn't authorisation kept at arm's-length?

The Bill envisages that the Director-General or Deputy Director-General of ASIO could grant an application for a special intelligence operation. This runs counter to the usual requirement for a person at arm's length from the agency to authorise invasive or intrusive conduct, for example, warrants to intercept communications. The evidentiary certificate process - proposed new section 35R – is further reason for the Committee to reconsider this proposal that ASIO sign off on its own special intelligence operations.

Reform proposals emerging in the post-Snowden environment tend to emphasise the need for more checks and balances into schemes which permit intelligence and security agencies to engage in seriously intrusive conduct.

Guardian Australia submits that, if the SIO scheme passes the necessity test and is retained in the Bill, authorisation for such an operation should be required to come from a judicial officer, and that an appropriately qualified, experienced and security-cleared Public Interest Monitor should be able to make submissions to the judicial officer before a decision is made.

Are the immunities necessary and proportionate?

The Bill proposes that in a Special Intelligence Operation agents may break the criminal or civil law and in certain circumstances be immune from the usual consequences. The Bill would also modify the judicial discretion to exclude evidence obtained through such criminal acts.

Parliament is being asked to erode what the High Court, in *A v Hayden [1984] 156 CLR 532*, described as fundamental to our legal system –

> ...the Executive has no power to authorize a breach of the law and that it is no excuse for an offender to say that he acted under the orders of a superior officer – Gibbs CJ
>
> ...For the future, the point needs to be made loudly and clearly, that if counter espionage activities involve breaches of the law they are liable to attract the consequences that ordinarily flow from breaches of the law – Mason J

The case arose from a training exercise run by ASIS in which operatives staged a mock hostage rescue in the Sheraton Hotel Melbourne. They wore masks and carried a pistol and two submachine guns. A hotel manager was manhandled. In the ensuing investigation, Victoria Police sought the identities of those involved. To be sure, it was a long time ago, but its echoes could be heard in the Inspector-General of Intelligence and Security's carefully worded public summary of her investigation into ASIS and weapons in November 2013.[xii]

The facts of *A v Hayden*, as much as the principle it emphatically reinforced, are relevant to the Committee's deliberations about whether the SIO powers and immunities sought in this Bill ought to be granted, and if so under what safeguards.

It is reasonable to ask what may have happened, and how much the Parliament or the public would have later come to know, had the proposed Special Intelligence Operation scheme been in force in December 2013 when ASIO raided the office and seized documents of the Australian lawyer who was at that time at The Hague to represent in the International Court of Justice East Timor in its dispute with Australia.

Guardian Australia acknowledges the various qualifications and limitations set out in proposed new Division 4 Part III. It urges the Committee to examine all of them with care.

Statutory schemes for controlled operations by police followed cases in which superior courts found some police methods amounted to entrapment.[xiii] The risks inherent in empowering and immunising police to break the law in order to investigate and prosecute other law-breaking are recognised, in part, by various purpose-built accountability methods.[xiv] Experience with controlled operations by police is mixed enough to be cautionary.

Given the imprecise scope of offences relating to national security or terrorism, particularly compared to more common criminal offences for which police use controlled operations, creation of a SIO scheme for intelligence and security agencies requires thorough examination. Proposed new section 35K provides that 'a participant in an SIO who engages in conduct that satisfies the requirements of subsection 35K (1) is not subject to any criminal or civil liability in relation to that conduct.'[xv]

Subsection 35K (1) sets out six conditions. Condition (e) requires that –

> the conduct does not involve the participant engaging in any conduct that causes the death of or serious injury to a person, or involves the commission of a sexual offence against any person, or causes the significant loss of, or serious damage to, property

Qualifying 'injury' with 'serious' raises important issues. How much may operatives injure a person before they lose the immunity anticipated by s 35K (1) (e)? The question is not trivial. It brings into focus the kinds of issues that can arise when the State gives its operatives immunity from legal liability in relation to physical treatment of persons.[xvi]

The UK Home Secretary recently established an inquiry into the conduct of some undercover police and its impact on prosecutions[xvii]. Several women from groups infiltrated by police allege the police formed sexual relationships with them and have launched civil actions for deceit, assault, negligence and misfeasance in public office.[xviii]

It is reasonable to ask the Committee to enquire whether, if similar circumstances arose in Australia under Special Intelligence Operations, the women could get justice under law.

Harms to legitimate scrutiny and disclosure

A feature of several of the examples used so far throughout this submission to illustrate questionable activities of intelligence and security agencies has been the role of the media in first bringing matters to light.

Commonly, after journalists make initial disclosures other oversight entities take action within the limits of their powers and resources. It may be a responsible minister, a parliamentary committee or a purpose-built entity such as the Inspector-General of Intelligence and Security (IGIS).

Of the 20 public reports of the Inspector-General (as at 31 July 2014), nine appear to have been triggered directly or indirectly by media disclosures.[xix]

The unfortunate case of Dr Mohamed Haneef was largely brought to light by the media. The inquiry it spawned led to an apparent acceptance within government that some improvements were required, according to the formal response to its recommendations.[xx]

This Bill – specifically new section 35P if enacted in its present form - would chill this disclosure work. In some circumstances which are likely to occur it would punish it.

The Ex Mem states that the offences apply to 'persons who are the recipients of an unauthorised disclosure of information, should they engage in any subsequent disclosure.'

It is clear from the Ex Mem that the new offences and penalties are intended in part to have a deterrent effect. The Bill and Ex Mem neglect the critical role which intention and public interest may play in a just and proportionate assessment of a person who makes preparations to disclose information or does disclose information.[xxi]

The consequences of proposed new section 35P would do damage to one of the essential checks and balances in a democratic society. The work of journalists, co-operating sometimes with whistleblowers willing to take great risks to help expose unlawful or improper conduct in government and elsewhere, is one of democracy's great safety valves. Its public interest value is myriad.[xxii] It may force an end for the time being to corrupt or harmful practices; it may avert them; it may serve more generally to inform voters' in their judgments at the ballot box.

The existence of the *potential* for disclosure can itself be a potent deterrent to wrongdoing or negligence or the kind of strained self-justifications to which like-minded people in closed decision-making environments are prone. It is the importance of *potential* disclosure which makes the chilling effect of provisions such as proposed new section 35P so damaging. Lips may not be pursed to blow a whistle. Journalistic enquiries may not begin, may not reach far enough.

These processes of disclosure and potential for disclosure have proved their worth many times over many years for many societies. We will not heap them up here but would be glad to provide the Committee with examples beyond those mentioned in this submission.

On 28 July 2014, Human Rights Watch and the American Civil Liberties Union released a 120-page report, *With Liberty To Monitor All – how large-scale surveillance is harming journalism, law and American democracy*. It reviews the effects on journalism when the balance between security and privacy goes too far towards security. The jurisdictional details are of course different, but the fundamentals apply also to Australia.[xxiii] The report may assist the Committee in assessing the Attorney-General's assertion in the Ex Mem that this Bill is compliant with the rights and freedoms of various international instruments.

For a powerful reminder of the importance of the particular category of journalism which would be damaged by this Bill – the kind that scrutinises the intelligence and security community - we refer the Committee to a dissenting judgment in the case of James Risen, a *New York Times* reporter specialising in national security matters. Risen has been pursued to reveal his sources for a story which described a failed attempt by the Central Intelligence Agency to disrupt Iran's nuclear planning. In 2013 the US Court of Appeals overturned a lower court's ruling protecting Risen and his sources and ordered Risen to disclose. (He appealed again.) In dissenting, Judge Gregory said in part –

> The freedom of the press is one of our Constitution's most important and salutary contributions to human history....
>
> Democracy without information about the activities of the government is hardly a democracy....
>
> The public, of course, does not have a right to see all classified information held by our government. But public debate on American military and intelligence methods is a critical element of public oversight of our government....Public debate helps our government act in accordance with our Constitution and our values. Given the unprecedented volume of information available in the digital age – including information considered classified – it is important for journalists to have the ability to elicit and convey to the public an informed narrative filled with detail and context. Such reporting is critical to the way our citizens obtain information about what is being done in their name by the government.
> A reporter's need for keeping sources confidential is not hypothetical. The record on appeal contains affidavits proffered by Risen detailing the integral role of confidential sources in the newsgathering process. Scott Armstrong, executive director of the Information Trust and former Washington Post reporter, points to three ways in which investigative journalism uses confidential sources:
>
> "developing factual accounts and documentation unknown to the public,"
>
> "tak[ing] a mix of known facts and new information and produc[ing] an interpretation previously unavailable to the public," and

> "publiciz[ing] information developed in government investigations that has not been known to the public and might well be suppressed."
>
> "It would be rare," Armstrong asserts, "for there not to be multiple sources – including confidential sources – for news stories on highly sensitive topics."
>
> ...Such guarantees of confidentiality enable sources to discuss "sensitive matters such as major policy debates, personnel matters, investigations of improprieties, and financial and budget matters." ...The affidavits also recount numerous instances in which the confidentiality promised to sources was integral to a reporter's development of major stories critical to informing the public of the government's actions. See...Dana Priest noting, among many stories, her reporting on the existence and treatment of military prisoners at Guantanamo Bay, Cuba; the abuse of prisoners in Abu Ghraib, Iraq; the existence of secret CIA prisons in Eastern Europe; and the "systematic lack of adequate care" for veterans at Walter Reed Army Medical Center relied upon confidential sources.[xxiv]

These dynamics will not be new to Committee members, who as Members of Parliament are surely, to varying extents, participants in some of them from time to time.

The proposed offences and penalties in 35P are drafted in a way that would severely interfere with activities vital to the proper functioning of Australia's democracy. Journalists, public servants, lawyers, community groups, and others concerned with liberty, government accountability and the rule of law are likely to be affected in ways disproportionate to what is appropriate to balance security with other important public interests.

Unintended consequences – disabling the filters of responsibility means less security, not more

Legislation aimed at intimidating and punishing journalists and others who play legitimate roles in the checks and balances of democratic life is likely to have serious unintended consequences.

Disclosures by insiders will continue. Snowden followed Ellsberg[xxv] and Manning[xxvi] (notwithstanding what was done to his two predecessors). Others will follow Snowden. Communications technologies increasingly will empower them.

The question facing the intelligence and security community is whether they want to disable the filtering role that journalists have so far played. Most media professionals – like, we presume, most intelligence and security professionals - feel obligations to ethical behaviour and the public interest. Journalists test a source's motives and the accuracy of his or her proffered material. They weigh the potential for disclosures to put lives at risk or to imperil active lawful operations aimed at preventing substantial harms. They consider whether delay is appropriate. They understand the significance of compromises inherent in redaction.

To wreck with heavy-handed law this kind of subtle interaction – first between journalists and sources, and second between editorial decision-makers and government representatives – would be a net loss to the security of Australia.

Viewed as part of the balancing of the public interests implicated in this Bill, how is it proportionate to legislate in a way that ensures future Snowdens are more likely, not less likely, to publish by themselves - irretrievably and to the world - the information they believe ought to be known? Once would-be whistleblowers understand the effect that these proposed provisions would have on media outlets, they may feel that to approach a media partner increases the whistleblower's risk rather than reduces it.

So what is the probable result of new offences and penalties like those proposed? Not the eradication of whistleblowers but the rise of unfiltered disclosures with all their increased potential for live operations to be compromised, for the identities of operatives and perhaps sources to become known, and for exposure of lawful techniques which renders the techniques ineffective. In short, the probable result is more harm to national security, not less.

The actual lived experience of publication of material from Snowden - and, earlier, material provided to long-established media entities by Julian Assange and Wikileaks - is that media outlets such as the Guardian, New York Times, Washington Post and Der Spiegel took responsible steps to ensure complex and competing public interests were weighed.

From a national security perspective their role was positive not negative.

Branding whistleblowers as traitors and criminalising acts of journalism do not assist in the reasoned balancing of liberty and security.

Conclusion

Official confirmation in recent days that the CIA broke into the computer system of the committee of the US Senate that oversees the CIA at the time the committee was conducting a sensitive investigation of the CIA is a timely reminder of the risks inherent in agencies which are entrusted with strong powers and large resources to invade the lives of others, including, potentially, their elected political overseers.[xxvii]

Guardian Australia urges the Committee to reaffirm through this inquiry the legitimacy of activity in a democratic society that tries to hold to account, under law and before the public, the intelligence and security agencies.

We urge that, if the Committee endorses a special intelligence operations scheme, its recommendations include a three-year sunset clause so that Parliament can review and if necessary reconsider the legislation in light of both its actual operation and the integrity with which Executive Government agencies respond to the balances made under law and the efforts to oversee them.

Emily Wilson

Editor-in-Chief

Guardian Australia

5 August 2014

Endnotes

[i] Parliamentary Joint Committee on Intelligence and Security *Report of the Inquiry into Potential Reforms of Australia's National Security Legislation*, May 2013,(the 2013 Report),
[ii] 2013 Report, Foreword xiii-ix
[iii] Based on the large amount of now public information in, or in response to, the Snowden materials, especially in the United States, it can reasonably be said that there is doubt about the lawful authority for some of the NSA activities which Snowden disclosed, and that there were serious inadequacies in what intelligence and security officials told oversight entities such as the Foreign Intelligence Surveillance Court, a Congressional Committee and the US Supreme Court.
[iv] 2013 Report, Chapter 4, para 4.90. Apart from noting that agencies had no intention of circumventing, no express safeguards appear to have been developed.
[v] http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act
[vi] Hansard, House of Commons, 15 July 2014 Col. 826
[vii] Liberty and Security in a Changing World – report and recommendations of the President's Review Group on Intelligence and Communications Technologies, December 2013, pp 10-11 http://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf

[viii] http://www.leahy.senate.gov/download/hen14602
[ix] Statement, Senators Ron Wyden and Mark Udall - http://www.wyden.senate.gov/news/press-releases/wyden-udall-will-work-to-strengthen-newly-unveiled-surveillance-reform-legislation ; *A stronger bill to limit surveillance*, editorial, New York Times, 28 July 2014 http://www.nytimes.com/2014/07/28/opinion/a-stronger-bill-to-limit-surveillance.html?partner=rssnyt&emc=rss&_r=0
[x] http://www.dpmc.gov.au/inslm/

[xi] Hansard, House of Lords, 16 July 2014, Col 630-631
[xii] Inquiry into the provision of weapons and the training in and use of weapons and self-defence techniques in the Australian Secret Intelligence Service - http://www.igis.gov.au/inquiries/index.cfm
[xiii] For example, *Ridgeway v The Queen* (1995) 184 CLR 19; *R v Loosely* [2001] UKHL 53
[xiv] For example, the jurisdiction of the Commonwealth Ombudsman - http://www.ombudsman.gov.au/pages/our-legislation/controlled-operations-and-surveillance-devices/ - and the annual reports of the NSW Ombudsman under the Law Enforcement (Controlled Operations) Act 1997 - http://www.ombo.nsw.gov.au/__data/assets/pdf_file/0010/14311/Law-Enforcement-Controlled-Operations-Act-Annual-Report-2012-2013.pdf
[xv] Ex mem para 532
[xvi] Although not a case involving Australian agencies, the case of Khaled el-Masri and the very recent acknowledgement by President Obama that, after 9/11, the US tortured some people, show that it is not fanciful to be concerned that intelligence and security agencies may overstep boundaries if they believe they are beyond the reach of the law: http://www.theguardian.com/world/2005/jan/14/usa.germany ; European Court of Human Rights, *El-Masri v former Yugoslav Republic of Macedonia*, 13 December 2012, news release summary http://hudoc.echr.coe.int/sites/fra-press/pages/search.aspx?i=003-4196815-4975517 . The concern was evident in October 2005 when the US Senate adopted an amendment by Senator John McCain aimed at preventing abuse in interrogations – Congressional Record, US Senate, Amendment #1977, 5 October 2005, begins page S11061
[xvii] Home Secretary's announcement https://www.gov.uk/government/news/home-secretary-announces-review-of-undercover-policing-cases. See also http://www.theguardian.com/uk-news/2014/jun/26/theresa-may-undercover-police-inquiry-campaigners-convictions -

[xviii] http://www.theguardian.com/uk-news/2014/jul/02/met-spy-undercover-police-damages-court
[xix] http://www.igis.gov.au/inquiries/index.cfm

[xx] http://www.ag.gov.au/NationalSecurity/Counterterrorismlaw/Documents/Government%20response%20to%20the%20report%20of%20the%20inquiry%20into%20the%20case%20of%20Dr%20Mohamed%20Haneef.pdf
[xxi] Ex Mem paras 553-562

[xxii] The US Senate formally designated 30 July 2014 as 'National Whistleblower Appreciation Day', linking it to the day in 1778 when the Continental Congress resolved to encourage the reporting of government wrongdoing by any person in the service of government who had knowledge of it.[xxii]

[xxiii] http://www.hrw.org/reports/2014/07/28/liberty-monitor-all

[xxiv] *US v. Sterling*, Court of Appeals, Fourth Circuit, No 11-5028, 19 July 2013, Gregory J, pp 86-90 (internal citations and brackets omitted).

[xxv] Provider of the Pentagon Papers to the New York Times – see Daniel Ellsberg, *Secrets: a memoir of Vietnam and the Pentagon Papers* (Penguin Books, 2002).

[xxvi] Chelsea, formerly Bradley, Manning, now in prison in the US for providing classified information to Julian Assange and Wikileaks. For accounts of other whistleblowers and their treatment see, for example, the cases of Thomas Drake http://www.newyorker.com/magazine/2011/05/23/the-secret-sharer and, in the UK, Clive Ponting, tried and acquitted after leaking information about the sinking by UK forces of the Argentine ship *Belgrano* during the Falklands War in 1982 – Richard Norton-Taylor, *The Ponting Affair* (Cecil Woolf: London 1985) and Clive Ponting, *The Right to Know* (Sphere: London 1985)

[xxvii] Summary by the Intelligence Community Inspector General, 31 July 2014 https://www.scribd.com/embeds/235569152/content?start_page=1&view_mode=scroll&show_recommendations=true ;'Inquiry by CIA affirms it spied on Senate panel', New York Times, 31 July 2014 http://www.nytimes.com/2014/08/01/world/senate-intelligence-commitee-cia-interrogation-report.html?hp&action=click&pgtype=Homepage&version=HpSum&module=first-column-region&region=top-news&WT.nav=top-news&_r=0 ; 'The CIA's reckless breach of trust, editorial, NYT, 1 August 2014 http://www.nytimes.com/2014/08/01/opinion/The-CIAs-Reckless-Breach-of-Trust.html?hp&action=click&pgtype=Homepage&module=c-column-top-span-region&region=c-column-top-span-region&WT.nav=c-column-top-span-region&_r=0 On 25 July 2014 McClatchyDC reported that the CIA appeared to have intercepted emails between officials of the oversight body, the Intelligence Community Inspector General, and Congress at a time the Inspector General was investigating claims of retaliation by the CIA against whistleblowers who has assisted a Senate Committee investigation into the CIA http://www.mcclatchydc.com/2014/07/25/234484/after-cia-gets-secret-whistleblower.html