theguardian
GNM Australia Pty Ltd
Lvl 2, 19 Foster St
Surry Hills, NSW 2010
Telephone: +61 (02) 8076 8400
ABN 50 161 165 242
theguardian.com

Submission by

Guardian Australia

to the

Parliamentary Joint Committee on Intelligence and Security
(the Committee or PJCIS)

Inquiry into the Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014
(the Bill[i])

Contents of this submission

Introduction

The day after this Committee held its first public hearing into the Bill in Canberra on 17 December 2014 Reuters reported –

> UNITED NATIONS — The United Nations General Assembly expressed concern on Thursday at digital spying and said unlawful or arbitrary mass surveillance and the interception and collection of online data are "highly intrusive acts" that violate privacy rights.
>
> The 193-member General Assembly adopted a resolution, drafted by Germany and Brazil, by consensus as a follow-up to a similar text approved last year after former U.S. National Security Agency contractor Edward Snowden exposed a spying programme by the NSA, sparking international outrage.
>
> Resolutions passed by the General Assembly are non-binding but can carry political weight.
>
> A reference to metadata surveillance as an intrusive act was removed from the resolution during negotiations to appease the United States, Britain, Australia, Canada and New Zealand, known as the Five Eyes surveillance alliance, diplomats said.
>
> Metadata is communications detail such as which telephone numbers were involved in a call, when calls were made, how long they lasted, when and where someone logged on to email or the Internet, who was emailed and what Web pages were visited.
>
> The resolution still mentions metadata for the first time, warning that "certain types of metadata, when aggregated, can reveal personal information and give an insight into an individual's behaviour, social relationships, private preferences and identity."
>
> It also calls on states to provide an effective remedy when a person's right to privacy has been violated by unlawful or arbitrary surveillance and encourages the U.N. Human Rights Council to consider establishing a special procedure to identify and clarify standards protecting privacy rights.[ii]

The article usefully encapsulates how, in our interconnected digital era –

- the issues involved in this Bill are part of an international debate of great significance;
- the disclosures by Edward Snowden are relevant to that debate;
- metadata about communications matters as much as the contents of communications;

- the Bill inevitably requires a balancing of values dear to democratic societies, particularly privacy and accountable security and law enforcement - to conduct the debate by minimising the importance of either value would be parochial, artificial and likely to harm both values.

The Committee is urged to conduct this inquiry with these four factors uppermost. While Guardian Australia is not persuaded that the necessity of a mandatory data retention scheme has been established, the PJCIS appears in its 2013 Report to have concluded otherwise, so this submission concentrates mostly on safeguards.

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 online at www.theguardian.com , through mobile applications 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.

Guardian Australia made a submission to the Committee on the National Security Legislation Amendment Bill (No 1) in 2014.[iii] Among other things, that submission drew attention to the debate surrounding the data retention legislation which the UK Parliament passed in July 2014. We also 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 (TIA Act).*[iv] *We* will not unnecessarily repeat here the arguments and sources presented in those two earlier submissions.

We again urge that the work of this Committee in its current inquiry and of the Senate Committee in the TIA Act inquiry be co-ordinated. This would reduce a recurring difficulty in ensuring appropriate scrutiny of legislation affecting freedoms. Intrusive powers tend to be expanded in an incremental and dispersed way. Their combined impact may not be fully appreciated. Scrutiny and safeguards may be fragmentary and, because of that, inadequate. (See later under the sub-heading 'Larger themes').

Debate about interception, storage and use of Australians' communications for security and law enforcement purposes is longstanding, not a product of relatively recent concerns about a particular strain of terrorism.[v] In examining data retention proposals this Committee is revisiting territory it covered in chapter five of its 2012-13 inquiry into potential reforms to national security legislation.[vi] The Committee is requested to look afresh at the issues, mindful of the limitations of its previous inquiry, one of which was described by the Committee's then chairman –

> ...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.[vii]

Trust in government agencies which are empowered to spy on people can never be blind trust.

Trust is granted in good faith according to an evidence-based assessment of the willingness of such agencies to co-operate in good faith with the various entities that are supposed to hold the agencies to account. The foremost accountability body is Parliament.

Since the Snowden disclosures and more recently since the disclosures about torture by Australia's Five Eyes partner, the United States, people are entitled to be more wary of further empowering government agencies to infringe established rights and freedoms. The evasiveness displayed in accounting for what Snowden revealed and for the torture ought to give pause to parliamentarians weighing the competing interests.

Where it is judged that on balance rights and freedoms must yield to other public interests, such as security from terrorism and the investigation of serious crime, people are entitled to insist on better safeguards against abuse of power, especially power exercised secretly.

People are entitled to insist on the creation - at the same time as powers are increased - of adequate methods to gather and make public the evidence that shows whether safeguards are working or not working. History shows that intrusive powers exercised secretly are prone to abuse and that public inquiry and reporting are necessary.[viii]

The reasons privacy is a right recognised expressly in the leading international human rights instruments and implicitly in several common law doctrines are too well known to repeat here.[ix] Also well known, or well described by other submitters to this inquiry, is the growing potential for privacy intrusion using digital technologies to sift and analyse big datasets. Described, too, are the ways access to the contents of communications and their metadata can assist in intelligence, security, counter terrorism and investigation of serious crime.[x]

The current Bill will compel an as-yet-unknown variety of communications service providers (CSPs)[xi] to gather and store for up to two years an as-yet-unknown range of data[xii] about the communications of all Australians – phone calls, texts, emails, social media, web use up to a point still unclear - whether or not they are suspected of involvement in any wrongdoing. Location data and download volumes appear to be included.

A variety of government agencies – and perhaps, necessarily, some private entities which are contracted to provide services to government agencies – will potentially have authorised access to the vast amount of data that will be compulsorily collected and stored.

The value of the data will ensure that pressure gradually develops for newly authorised uses and users, a phenomenon known as function creep.

Unauthorised leaks from such valuable stores of data are inevitable, whether through corruption, honest-but-arrogant disregard for limits, or mistake.

It is apparent that this inquiry relates to interests far broader than securing the public from terrorism and other serious crime.[xiii] The blending together under a national security/counter terrorism badge of legislative measures with more commonplace policing and revenue collection policy purposes is misleading and, to that extent, may be itself corrosive of trust.

A far-reaching step is being contemplated through this Bill. In the contemporary world in which most of us use digital communications in many aspects of our lives, what seems to be happening is the formal creation of what the Snowden disclosures suggest was being created informally: constantly refreshed storehouses of data that would allow every person's digital communications to be surveilled. The debate is about the how, not the if.

Communications service providers (CSPs) are to be compelled to facilitate surveillance more systematically and comprehensively than in the past. Yet the trend in their sector is for them to collect in the course of running their businesses less personal data about their customers than in the past. The Bill does not have only cost implications for the CSPs. It undermines the trust between CSPs and their customers. Snowden's disclosures showed the extent to which the co-operation of CSPs is necessary to surveillance of the public by the state. That

co-operation may be obtained by legal compulsion, inducement or persuasion. It may be reluctant, dutiful or avid. It has its tensions, vividly shown by the current debate over encryption.[xiv] But what seems clear is the heavy reliance customers must place on the effectiveness of safeguards to keep the state and the CSPs within authorised limits.

If the data retention scheme has fully disclosed and explained by Executive Government by the deadline for the PJCIS to report to the Legislature, and if the Committee concludes that the scheme is reasonably adapted to a legitimate purpose, is necessary and is proportionate, the Committee is urged to recommend safeguards that are commensurate with the risks inherent in such a scheme.

Metadata matters as much as the content of communications

The exact dataset to be compulsorily retained for access is unavailable at time of writing. The Attorney-General's Department has proposed a draft dataset[xv], but it was clear from the hearing on 17 December 2014 that this is by no means settled.

The potential for metadata to provide insights into what is reasonably expected to be private and confidential in a person's life is well documented. The potential exists for everyone, but in the context of this inquiry and this submission it is of particular concern to those whose professional lives require them to give and to receive confidences, such as journalists and lawyers.

Without repeating the sources cited in other submissions which demonstrate the power of metadata – and, incidentally, the misleading nature of the analogy of metadata with the name and address on the outside of an envelope - we note that the US Supreme Court has recently recognised the potency of data associated with mobile phones in its decision in *Riley v. California*. The court held that warrantless access by police to an arrested person's mobile phone violated the Fourth Amendment.[xvi] Delivering the ruling, Chief Justice Roberts said in part –

> Modern cell phones are not just another technological convenience. With all they contain and all they may reveal, they hold for many Americans "the privacies of life". The fact that technology now allows an individual to carry such information in his hand does not make the information any less worthy of the protection for which the Founders fought.

The emergency legislation hastily amending the UK data retention scheme in July 2014 is subject to a legal challenge by the UK Bureau of Investigative Journalism, and in summarising its claim the Bureau elaborated the potential impact of the retention of communications data on journalism -

> ...the interception, storage and analysis of data concerns not only communications *content* but also includes "*meta data*" (e.g. data about communications). Importantly, technological advances in recent years mean that such metadata can be used and exploited in a way that is every bit, if not more, intrusive of confidentiality or journalistic free expression as the interception of, for example, the content of journalistic communications. This is because metadata can be subject to hugely powerful computer programmes which collate, link analyse and synthesise masses of

> data, enabling a sophisticated picture to be developed of an individual or organization's network of contacts, sources, lines of enquiry as well as materials, subjects and persons of interest to them. Without rigorous and effective legal safeguards, it is plain that the use of these powerful technologies may now fundamentally undermine journalistic free expression in a way that could not previously have been envisaged.
>
> The interception and exploitation of journalistic communications in this manner, in the absence of proper safeguards, may undermine the confidentiality of journalistic sources, materials and information, a necessary and basic precondition for press freedom in a democratic society.[xvii]

The issue is not hypothetical, as recent disclosures show.[xviii]

The confidentiality necessary to lawyers and their clients is similarly at risk from legislation such as this. We anticipate that other submitters to this inquiry will elaborate this aspect, which is broader of course than simply journalists' consultations with their own lawyers. We note, however, that it is usually at times when journalists are fulfilling their most significant democratic role – preparing to make and defend serious public-interest disclosures - that the journalists' need to consult lawyers confidentially is at its most consequential.

The issue of the impact of surveillance on journalism and law is examined in detail in a 2014 report by Human Rights Watch and the American Civil Liberties Union, 'With Liberty To Monitor All – how large-scale US surveillance is harming journalism, law and American democracy'.[xix] The report and its recommendations range wider than the current issue under discussion and naturally there are jurisdictional differences, but several of the recommendations are similar to those that journalists in the UK are urging on decision-makers responsible for implementing data retention. They include –

- independent judicial process, with notice, before the content or metadata of journalists' communications may be accessed
- opportunity to challenge an application for access and to appeal an unsuccessful challenge
- appropriate 'shield law' protections
- where access is granted, procedures that tightly target only the minimum data necessary.

Surveillance and Members of Parliament

Just like lawyers and journalists, MPs have a professional need for confidentiality. One way to illustrate the way MPs share everyone's vulnerability to insufficiently accountable surveillance is to focus on how it could disrupt their ordinary working lives just as much as the lives of others.

Consider, for instance, the power that would settle in the hands of anyone who could gather and analyse the metadata of the phone calls of members of a parliamentary party during the tensions and lobbying that typically surround a leadership challenge. Assume the data shows only who called whom, when, for how long they spoke, and who each of them called

next. Mobile phone metadata may also give the location of the user. With a little simple data matching, the location data may indicate who has been visiting whose home, office or weekender. Cabals in restaurants or airport lounges would become apparent to a reasonably informed analyst of the data. Coupled with the software that permits big datasets to be sifted and visualised in patterns, the metadata has obvious temptations and misuses for professionals in the political process. Presumably, the temptation would wax and wane according to government or opposition status.

Go beyond the metadata to the actual content of the phone conversations and texts among MPs as they decide whom to support as leader. The content would indicate the essence of the pitches being made, the undermining techniques, the promises, the blandishments and the threats. It would shed light on the number of times the same office or posting had been promised or even traded in exchange for votes, and how many times one person had committed their single vote to rival contenders. Depending on how soon the fruits of this surveillance could be obtained, it could empower the holders with knowledge about the plotters, loyalists, persuaders, waverers and double-crossers.

Committee members with gmail accounts may wish to investigate how much about their own lives can be revealed by the metadata of only their emails – by using just the to, from, cc and timestamp fields, not the subject field or the contents. They can do so by using the 'Immersion' program developed by the Massachusetts Institute of Technology.[xx]

Safeguards

The UK Parliament passed emergency legislation in July 2014 in response to a European Court of Justice decision to declare invalid the EU Data Retention Directive.[xxi] During that legislative process the House of Commons Library distilled from a range of expert analyses of the ECJ decision the following principles for a data retention scheme that probably would have been valid.[xxii] Guardian Australia commends the list, if suitably adapted to Australia's legal context, as a valuable guide to desirable safeguards –

- restrict retention to data that is related to a threat to public security and in particular restrict retention to a particular time period, geographical area and/or suspects or persons whose data would contribute to the prevention, detection or prosecution of serious offences

- provide exceptions for persons whose communications are subject to an obligation of professional secrecy

- distinguish between the usefulness of different kinds of data and tailor retention periods to the objective pursued or the persons concerned

- ensure retention periods are limited to that which is 'strictly necessary'

- empower an independent administrative or judicial body to make decisions regarding access to the data on the basis of what is strictly necessary

- restrict access and use of the data to the prevention, detection or prosecution of defined, sufficiently serious crimes

- limit the number of persons authorised to access and subsequently use the data to that which is strictly necessary

- ensure the data is kept securely with sufficient safeguards to secure effective protection against the risk of abuse and unlawful access
- ensure destruction of the data when it is no longer required
- ensure the data is kept within the jurisdiction

Generally speaking, the recommendations about the Bill of the Australian Parliament's Joint Committee on Human Rights (PJCHR) are consistent with this list. The importance of audit and record keeping, among other safeguards, is emphasised in an analysis relating to another of Australia's Five Eyes partners, Canada.[xxiii] Guardian Australia requests that the PJCIS give particular attention to the following safeguards -

Clear and precise legislation with minimal use of regulations

This should go without saying, but a troubling feature of the gestation of the data retention scheme has been the recurring failure to provide clear information about what, precisely, Parliament is to be asked to enact. A previous PJCIS chairman commented about the initial withholding of relevant information by the Attorney-General's Department; the current Attorney-General was unclear in some of his public comments about what constitutes metadata; Ministers and the Commissioner of the Australian Federal Police have appeared to contradict each other about the range of purposes for which the retained data is to be used; and the Bill and its Ex Mem lack fundamental information, for example, about the detail of the dataset that is to be compulsorily collected and stored.[xxiv]

Guardian Australia acknowledges that this Committee has pointed out these shortcomings – as does the PJCHR – but, taken together, these problems do not instil confidence in what is a balancing process involving weighty public interests. The Committee is requested to insist that the scheme be in detailed legislative form, so that the appropriate degree of scrutiny and, when eventually enacted, legitimacy, attaches to it. While it is understandable that the agency experts working on the scheme would want the flexibility that comes from putting detail into regulations rather than legislation, the stakes that surround this issue, and the damage done to trust by disclosures about past surveillance, make such a course not only insufficiently democratic, but also counter-productive. The relevant agencies have important work to undertake on behalf of the public, and properly authorised and accountable surveillance is part of it. If the powers they use and the scheme they administer come to be perceived as illegitimate their effectiveness will be hampered.

No relevant regulation or instrument to be immune from disallowance by Parliament

To the extent that aspects of the scheme must be left to regulation, everything should be capable of review and disallowance by Parliament. Nothing relevant should be immune from disallowance, whether through certification by the Attorney-General under the section 10 procedure of the *Legislation Instruments Act* in its current form or as it may be amended by the Acts and Instruments (Framework Reform) Bill 2014; it seems that the proposed new notifiable instrument procedure would preclude parliamentary scrutiny/disallowance. The datasets to be retained, in particular, should be in the form of amendments to the Bill. However, if the details of the datasets are to be in regulation then that regulation should be released for consultation as an exposure draft.[xxv] The same process should be followed for all regulations associated with the data retention scheme.

Automatic sunset after two years and public review

The Attorney-General has promised a review of the scheme by the PJCIS after three years. Given the significance of the issue, the speed with which technologies move, and the fact that the scheme seems to be a work-in-progress at this time, Guardian Australia submits that the enabling legislation should sunset and the scheme be reviewed after two years. By 2017, the results of the 2016 UK review of its similar scheme should be available to inform the Committee's work. To the greatest extent possible, the review and the Committee's report should be public.

Access to be obtained with prior approval from independent judicial authority

At the 17 December hearing several Committee members and agency witnesses expressed scepticism about the practicability of requiring agencies to obtain warrants from an independent judicial authority before getting access to retained metadata.

The following excerpts give the flavour of the exchanges. For clarity: during these exchanges the terms 'unwarranted' and 'non-warranted' are used when warrantless access is being discussed –

> **Mr NIKOLIC:** …I will move on to my next question, which is about some of the criticisms around non-warranted access to metadata. Some see it as exceptional and troubling. Indeed, some of the public commentary in the submissions I have seen almost tries to invest in the metadata the same sort of privacy sensitivity as you would find in the content of some of the data that is produced. So I am wondering to what extent you consider non-warranted access to metadata exceptional. Where else in law enforcement do we already find non-warranted access to records and information which would reasonably attract similar sorts of privacy concerns?
>
> [A-G's Dept rep] **:** Agencies can probably comment from an operational perspective on their practices for the range of information that they access. But, while there are warrants for access to some types of information and tools, warrants are typically reserved for those tools that are most intrusive. The committee has already commented today on telecommunications interception warrants, but there are a range of other warrants for more intrusive steps—search warrants et cetera. However, access under alternative mechanisms is certainly by no means unprecedented. Indeed, it is common through 'notice to produce' authorisation processes et cetera to access more routine ranges of information that are less intrusive. Telecommunications data, as we said, is a basic data point. It is typically used at the beginning of investigations to commence inquiries, to identify inquiries and to pursue those. It is a relatively less intrusive range of information. It is also often required to progress investigations quickly and to provide the information that is then required to support something like an interception warrant. So it then supports warranted access to other tools.
>
> [ASIO rep] **:** I will just add to that….metadata is often used as our first point in an investigation. So we see it as the least intrusive stage. It is as much to rule people in as to rule people out of investigations so that we do not then need, in many cases, to go to another higher level of intrusion. But I would not want the committee to think that there are no checks and balances for the data we collect. ASIO officers have to collect information using the most effective means. It has to be proportionate to the gravity of the situation. It has to take into account the level of intrusiveness. That is done under the Attorney-General's guidelines and in accordance with our own codes of conduct. As the level of intrusion increases, the level of delegation of an individual signing off on it goes higher. So it is proportionate, if you like, to that level of intrusion.

If there was a warranted regime for the sort of metadata that we are talking about here it would have a grave impact on our operational response and agility in these areas and would impose a sort of overlay and consequential delay in being able to assess and respond to emerging security threats that we think is beyond the level of intrusiveness that is involved.

[AFP rep] **:** It is the same with us in terms that I do not want anybody to be under the illusion—I think I have used the words 'willy nilly' with the committee before. We are very careful about the authorisations and the type of information we want and when we want it. The authorisations in the AFP are up to commissioned officer level, so only a commissioned officer can authorise the access to the communications data. We do not do it all the time; we do it when we need it because we actually have to pay for it as well, as it is at the moment. It is not free.

It is a point worth making that to move to full warranted application to do so is a very long and onerous process, and rightfully so, for intrusive actions. Whether we are doing telephone intercepts or whether we are using the metadata to form the basis of information to do a search warrant on someone's house, all those authorities have to be done in some form judicially. So we believe that it is most appropriate that we have the checks and balances in place. The AFP last year—and again recall that it is only a small percentage of what all law enforcement agencies do across the country—had 25,000-odd authorisations for 56,000 actual pieces of data or different services. If we were to get a warrant for each one of those, and it is roughly eight hours an application to put a search warrant together—that is how onerous they are to do these days—you are talking about 200 people taking a year to put that together. That is 20 per cent of my investigative capacity in the AFP.

[ASIO rep] **:** I should also say that, in ASIO's case, the IGIS has oversight and full royal commission powers to look over the way that we collect and use data. [IGIS] said that she 'did not identify any concerns with ASIO's access to prospective and historic telecommunications data. My officers' oversight of this particular technique decreased during this reporting period due primarily to changes in our inspection program and the high rate of compliance in this area.' So there are checks and balances there and warranted activity provides another level of intrusion and another level of checks and balances over the top of that.

Mr NIKOLIC: In those areas where there is already a precedent for unwarranted access—be it banking, finance or health records—can anyone on the panel tell me whether there has been an upsurge of complaints or criticism that there has been a free-for-all in accessing that material, as some are suggesting might be the case for metadata access?

[ACC rep] **:** Mr Nikolic, I am not aware of any other sectors that are complaining about a civic duty that has been put upon them, and the example you just referred to in terms of the financial sector is a good example. We have notices to produce that get served on financial sectors from all police and law enforcement agencies across the country—

Mr NIKOLIC: Unwarranted.

Unwarranted. And those investigations are generally over a regime which requires those institutions to hold those records for seven years, not two. So they are a necessary way of discovering and understanding what is the nature of the allegation. If I could refer back to the data issue that was just raised, the Australian Crime Commission has only 20 authorised officers who have oversight and have the delegated authority to require such information, and it is under a regime again by numerous oversight agencies. We have got about five or six that oversee the Australian Crime Commission in one form or another.

Again there have not been any instances that I have been made aware of that have complained about the nature of those requirements for a telco to produce such data.

...

Mr RUDDOCK: On this same matter, I am very concerned about the extent to which agencies dealing with terrorism investigations, for instance, are impeded by unnecessary and very complex and costly processes that limit their capacity to go after the crooks. I ask myself the question: for the 30-odd thousand that you say the police needed of authorisations to get access to metadata, what is the cost of each authorisation? What would be the average cost of getting a warrant for every one of those authorisations? What would it do to the capacity of the organisation to carry out its functions?

I just get the impression that we are being totally unrealistic, and I would like to have some objective data that just demonstrates that it would impede the effectiveness of the organisations that we are relying upon to deal with these very significant investigations.

[AFP rep] **:** As I said, I only did it just on the back of the envelope, but I know how long it takes for our investigators in this day and age, in 2014, to put a search warrant together. They are very complex documents now. It was a lot different when I put one together 25 or 30 years ago.

Mr RUDDOCK: Opportunity cost—$1,000 for each warrant?

[AFP rep] **:** More than that. It is going to take at least eight hours a person—56 times eight. I am talking about 200 people in addition that it would take.

Mr RUDDOCK: So each warrant might cost $10,000.

[AFP rep] **:** Easily. At least a thousand bucks—a day's worth of work for each single one. You are talking millions. It is the back of an envelope here: the additional cost or the opportunity cost to our organisation would be at least $25 million a year.

Mr RUDDOCK: And there would be 30,000 judges who have to make their time available. Have we included the cost of that.

[AFP rep] **:** No, that is just our cost.

[ACC rep]**:** I might add that the national figure is in excess of 300,000, because the vast volume is done by law enforcement through the state and territory police, in addition to the 25,000 that the AFP spoke to earlier. So it is not only the preparation of affidavits and the attendance. Most of the warranted information is required to be represented by a legal practitioner, not a police officer, so you have to engage lawyers to go before the AAT and/or a judge, and they must be backed up by affidavits that often range anywhere from 20 pages to in excess of 200 pages—I have seen affidavits of that length. So the laborious nature of it is one point.

These exchanges, which incidentally demonstrate the scale and routine nature of current access to metadata by police and security agencies and others, contain a contestable assumption. They assume is that metadata is bland, and that the information or knowledge that can harvested from it is inconsequential compared to the contents of communications. Guardian Australia submits that metadata is not bland, that it can be as revealing as content of communications, that it can be very consequential for the people whose private and professional lives it relates to, and that the scheme that is being proposed is likely to result in more systematic access to metadata than in the past.

If metadata were bland, it seems doubtful that so many agencies would be seeking so much of it.

The contradiction is worth expressing: on the one hand it is argued that metadata is a vital tool for intelligence, security, investigating crime and securing revenue and that is why it must be compulsorily collected, stored and accessed; on the other hand metadata is said to be of such a non-revelatory nature that common processes such as persuading an independent decision-maker that intrusion is warranted are unnecessary.

While it is natural for agency representatives to reassure the Committee about the integrity and reliability of their internal processes for getting access to the data, having regard to the significance of the interests at stake, the reassurances from the users of the data are not enough.

The audit-style oversight after the event by the Ombudsman, and the potential for the Inspector-General of Intelligence and Security to examine matters in response to complaints or on her own initiative, are welcome safeguards, subject to the adequacy of the powers and resources that those accountability bodies may be given.

Citing low complaints statistics may not be useful in this context; few people whose data is accessed are likely to be aware of the surveillance. General public awareness of these kinds of metadata surveillance is low. It is awareness that can create customer pressure on the commercial organisations that routinely supply data, pressure which may then lead those organisations to complain about having to do so. This sequence was evident after the Snowden disclosures showed the extent of the secret supply of customer data by commercial organisations such as Facebook, Google and Yahoo.

Guardian Australia submits that it is reasonable for the public to expect that authorisation from an independent, appropriately qualified person ought to be required before metadata is accessed. Independent authorisation is such a commonly occurring feature of the safeguards used by democratic societies in the context of surveillance schemes that the Committee is requested to investigate further, to test seriously the agencies' claims about cost in time and money, and to recommend an appropriate process for independent authorisation prior to access.

Public Interest Monitor, to be heard before access decision is made

Of necessity, procedures to assess whether surveillance of a person's communications are warranted will ordinarily occur without the knowledge of the target. Yet this means that the person who must make the decision – whether a senior officer of the agency, the Minister, or a judicial officer – lacks one side of the argument.

The Committee is requested to recommend the creation of an independent Public Interest Monitor role. A suitably qualified and experienced person should have the primary function of testing the arguments of agencies which seek to conduct surveillance and of articulating the privacy and others interests which ought to be weighed by the decision-maker.

A PIM would be a valuable additional safeguard, not just for the data retention scheme but for amended communications interception scheme which will presumably result from the current inquiry by the Senate Legal and Constitutional Affairs References Committee into the comprehensive revision of the Telecommunications (Interception and Access) Act 1979 (Cth).

Queensland and Victoria[xxvi] have established statutory Public Interest Monitors as part of the safeguards for their schemes to combat corruption, terrorism and organised crime. The

Australian Law Reform Commission recommended the creation of a PIM in the telecommunications interception context in 2008.[xxvii]

In the US Congress, reforming legislation in the wake of the Snowden disclosures has included a PIM equivalent: 'special advocates' to assist the closed courts that consider surveillance applications from agencies.[xxviii]

The Committee is requested to consider adapting and applying to the current context the rationale for the role of a PIM set out in the Queensland Parliament at the time preventive detention was being enacted as part of anti-terrorism measures in 2005 -

> These laws are tough. They are almost unprecedented in our legal system. They may result in people being locked up for 14 days without charge or trial and with very limited rights of communication with the outside world. I do not wash my hands of the responsibility to act against terrorism where that is needed. In proposing draconian laws, however, I take seriously my responsibility and the responsibility of my government and my colleagues to ensure that every reasonable safeguard is in place.
>
> ...In a civil society, law enforcement powers are strengthened, not compromised, by improving their public accountability and credibility. The PIM, or Public Interest Monitor, is a nationally unique mechanism for doing this at the 'front end' of the process. Other jurisdictions use reactive mechanisms that only apply after the event, such as complaints, inspections and reports. There is no doubt a role for those 'back end' accountability measures, but they are immeasurably enhanced by proactive safeguards like the Public Interest Monitor at the front end. I am sure those opposite will join me in calling on other states to use public interest monitors in their corresponding procedures in the future. I hope one day that we have a national system of public interest monitors operating in our legal systems around Australia.[xxix]

Mandatory disclosure of independently verified information about scale, uses and security of retained data. Maximum possible transparency.

Committee members will be aware that currently the available statistical data about the extent of lawful surveillance of communications data is limited and can be confusing. Proposed amendments would reduce it further.[xxx]

One of the consistent lessons from accountability systems in many areas, not just security and policing, is that routine gathering, analysis and publication of statistics, independently verified, is a valuable way to keep track of the use of strong powers, particularly powers which of necessity must be exercised and may be authorised primarily in secret.

The Committee is urged to give particular attention to this issue as the communications surveillance scheme of Australia is revised. Detailed requirements should be enshrined in legislation. The responsibilities of the relevant agencies, the Attorney-General's Department, the Ombudsman, the Privacy Commissioner, the Inspector-General of Intelligence and Security, the CSPs and other relevant public or private sector bodies should be spelled out. They should have the resources to undertake the work adequately.

No agency or corporation should be permitted to withhold or to mislead in relation to any statistical data about itself, and there should be penalties for doing so.

The fact of any decisions by a Minister, or any of the oversight bodies, to suppress any data should be made public (with appropriate language to protect any necessarily secret operations or techniques).

Reliable data about the occasions of authorised access to the contents and to the metadata of Australians' communications, of occasions on which access was sought and denied, of the uses and the users, and of mistakes, leaks or complaints and what was done about them, will be vital to the proper conduct of future reviews, especially the review at the time the sun sets on the scheme currently under construction.

Part of accountability is transparency. In this field it is not always possible to be as transparent as in others, but the Committee is requested to keep transparency to the fore and to establish whether the Australian Government proposes something similar to the UK in relation to the secrecy of sources of the retained data.

It appears that the UK system will operate secretly in the sense that only the Home Office would know which communications service providers are being required to retain data. Para 1.9 of the draft code states –

> The Home Office does not publish or release identities of CSPs subject to a data retention notice as to do so may identify operational capabilities or harm the commercial interests of CSPs under a notice.[xxxi]

The implication is that the customers of the CSP will not be informed that the CSP is under a notice to retain the customers' data. Leaving to another day the issue of whether a Privacy Commissioner would regard a similar approach here as acceptable under the Australian Privacy Principles[xxxii], an inference from the reasons given for secrecy is that disclosure of the fact that a CSP is being required by law to retain the data of its customers may harm the CSP's commercial interest, presumably because customers may take their business elsewhere. Customers may also begin to encrypt their communications.

Minimum necessary retention period and a prohibition on hoarding

One lesson from the Snowden disclosures is the size of the appetite of some government agencies for collecting and hoarding very large stores of personal information about the public's communications. The capacity and sophistication of programs that can sort and sift digital data to produce information about people and their relationships, or to allow inferences about them, seems to improve rapidly.

The clichéd rationale is about haystacks and needles: to find the needle – that is, terrorists and other serious criminals – it is argued that you need to gather and stack much more hay – that is, personal information, especially communications data. An alternative view is that you need to develop better magnets, but that is a separate discussion.

The point for now is that the amount of data collected will be determined partly by the length of the mandatory data retention period. This matters from a privacy perspective, of course, but also because the larger the stores of data the greater their attractiveness to unauthorised users so the greater the need to keep the data secure.

The Bill proposes a retention period of two years, which is lengthy by international standards and longer than the period that generally yields the most useful data, as Committee members demonstrated by their questioning at the 17 December hearing –

Mr CLARE:… international experience I think shows that about three-quarters of the data that is sought is usually six months old or less, and around 90 or 95 per cent of the data is one year old or less. I am wondering whether the department or agencies could comment on that.

[ASIO rep] **:** We have certainly included some detailed information in our classified submission on this, but, as I think I mentioned in my opening statement, it is true that 90 per cent of the data that we obtain is in that 12-month period, which leaves 10 per cent that is longer than that, and obviously a smaller percentage as you go out. But the difficulty in that is that you cannot compare to say that that 10 per cent is the least important and that 90 per cent the most important, because in dealing with particularly complex and long-running cases and plots it may well be that the 10 per cent or the two per cent outside, at the longest length of retention, is actually the most crucial information that you are looking for in terms of networks and, as I think I said earlier, in terms of particularly espionage cases and cyber cases. Those sorts of things can go out for very long periods of time.

Mr CLARE: But it appears almost without exception that countries around the world have opted for 12 months or six months.

[A-G's Dept rep] **:** And I think—and I cannot speak for other countries—it is about trying to find that compromise between the security and privacy concerns. If you asked any intelligence organisation around the world whether they wanted to have access to data for a longer period of time or for a shorter period of time, I think I could say with great confidence that it would be for a longer time.

Guardian Australia urges the Committee to endorse the recommendation of the Joint Committee on Human Rights, to test the Attorney-General's Department further on whether a two-year retention period is necessary and proportionate, and to incline to a shorter period in the absence of a compelling case for the two-year period.

In light of the Snowden disclosures, the Committee is requested to consider whether further steps are necessary to guard against the potential for data to be harvested from CSPs prior to the retention deadline and hoarded by one or more agencies.

Specific criminal offences to cover wrongful access and misuse

Assurances have been given about the rigour with which internal safeguards are applied by agencies which are allowed access to communications metadata and contents. The Attorney-General's Department has advised that the range of agencies permitted access to metadata is to be significantly limited.

These assurances are welcome, but Guardian Australia submits that more is required.

It is envisaged that the Attorney-General may declare entities eligible for access if they are engaged in the enforcement of the law or protection of public revenue. The 17 December hearing established that applications for expanded uses of the data are likely, if not expected. ASIC was mentioned, for example.

It was also noted that retained data about the volume of downloads would be useful in tracking torrenting. The following exchange fleshed out the issue –

Q: ...Once the data is retained, what are its implications for the purposes of civil litigation, particularly this sticky issue of piracy?… With civil litigation there is a discovery order, people want to find out—a bit like the speculative invoicing we have seen in the case of the Dallas Buyers Club. You now have all of this data available

> that a content producer can use in order to try to dig a bit deeper and find out who is illegally downloading their material. Under the existing law, they would have the right and ability to pursue that in court. This additional data that is being preserved that otherwise might disappear over the course of the next five years or so would be available to pursue through those court orders. Does the department think that there needs to be some change there to the way in which civil litigation might operate?
>
> A**:** It is the case, obviously, that data that is already available and data that will become available in accordance with data retention is available and amenable to other lawful process, including in the civil space whether that be through subpoena or other orders for production. Production in other contexts itself raises a number of challenges and the ability for persons in those proceedings to adduce such evidence as is relevant to their proceedings, and of course it extends into such matters as family law, other commercial situations other than the rights space, which has been the subject of some coverage. It is the case that that data would be available and it has been for some time and is amenable to that process.

The answer is broadly consistent with the UK, where the data retention is also being revised and a draft code, issued by the Home Office, is currently under discussion. The draft code states that retained data may be used –

- in the interests of national security;
- for the purpose of preventing or detecting crime[6] or of preventing disorder;
- in the interests of the economic well-being of the United Kingdom so far as those interests are also relevant to the interests of national security;
- in the interests of public safety;
- for the purpose of protecting public health;
- for the purpose of assessing or collecting any tax, duty, levy or other imposition, contribution or charge payable to a government department;
- for the purpose, in an emergency, of preventing death or injury or any damage to a person's physical or mental health, or of mitigating any injury or damage to a person's physical or mental health;
- to assist investigations into alleged miscarriages of justice;
- for the purpose of assisting in identifying any person who has died otherwise than as a result of crime or who is unable to identify himself because of a physical or mental condition, other than one resulting from crime (such as a natural disaster or an accident); and
- in relation a person who has died or is unable to identify himself, for the purpose of obtaining information about the next of kin or other connected persons of such a person or about the reason for his death or condition.[xxxiii]

This list is wide, and not exhaustive. The draft code states –

> In circumstances where a CSP identifies a specific purpose where access to retained data is in the interest of their customers, the company should discuss this issue with the Home Office on a case-by-case basis. This could include an investigation into fraudulent use of their services, where historical data retained under a notice might be crucial to that investigation. The agreement of the Home Office may relate either to individual requests or categories of request.[xxxiv]

It would be reasonable for Australians to enquire, and for this Committee to establish, whether the Government has any similar mechanism in mind under which, for example, the owners of copyright in digital entertainment products would be able, at the discretion of a Minister or Department, to use retained data to investigate the communications activities of members of the public and to attempt to enforce intellectual property rights.

Personal data, and the information which can be mined from it, is useful and valuable for reasons that are not always foreseeable. This was always a given, but it is of special significance in the digital era when so much data can be generated, collected and processed. Function creep is highly likely in any data retention scheme.

Once it is clarified precisely what the retained data may be used for, consideration should be given to making it a criminal offence, with appropriate defences, to use it for any other purpose. Consideration should be given to making data that has been obtained or used in an unauthorised way inadmissible as evidence in a criminal or civil proceeding.

Any expansion of the authorised uses should require a transparent process, involving prior notice, an obligation to consult, and parliamentary approval.

Justifiable exceptions, such as a use of the data in response to an emergency, should nevertheless require, at least, endorsement afterwards by a judicial officer and publication of the fact of the use (in appropriately circumspect language) during the reporting process.

Such safeguards are part of ensuring that what is done with the data is necessary and proportionate. Meaningful safeguards are part of rebuilding trust.

Independent oversight, adequately empowered and funded

Trust can also be engendered by the activities of independent oversight bodies that are visible and effective. To be effective, they need resources.

In the data retention scheme, the roles of the Inspector-General of Intelligence and Security, the Commonwealth Ombudsman and the Australian Privacy Commissioner have been emphasised.

The Committee is urged to satisfy itself that these agencies have the powers and resources necessary to undertake effectively the new oversight duties that the data retention scheme, and any other changes to communications surveillance, may entail.

The growth since 11 September 2001 in the powers and resources of the Australian intelligence and security community are regularly noted. ASIO had 1490 full-time staff and about $406 million in 2013-14, according to its latest annual report. Its chief independent overseer is the Inspector-General of Intelligence and Security who, says the IGIS website,

> is an independent statutory office holder who reviews the activities of the six intelligence agencies referred to as the “Australian Intelligence Community”, namely:
>
> Australian Security Intelligence Organisation - ASIO
> Australian Secret Intelligence Service - ASIS
> Defence Signals Directorate - DSD
> Defence Imagery and Geospatial Organisation - DIGO
> Defence Intelligence organisation - DIO
> Office of National Assessments - ONA

> The purpose of this review is to ensure that the agencies act legally and with propriety, comply with ministerial guidelines and directives and respect human rights.

The Inspector-General had income of $2.38 million and 12 staff, according to her 2013-14 annual report.[xxxv]

The Ombudsman and Privacy Commissioner have responsibilities that embrace not just the intelligence and policing community but the whole of the Commonwealth public sector and, for the Privacy Commissioner, a substantial chunk of the private sector as well.

In the US after 9/11 a Privacy and Civil Liberties Oversight Board was created as a check and balance to the enormous growth in the powers and resources of the intelligence and security community of that country. In its recent semi-annual report, the PCLOB noted that –

> The Board has jurisdiction to review all existing and proposed federal counterterrorism programs, to ensure that they include adequate safeguards for privacy and civil liberties. Most of these programs are conducted by the 17 different agencies that comprise the Intelligence Community, whose cumulative budget for FY 2013 was $49 billion. By contrast, the Board's FY 2013 budget was only $0.9 million and its FY 2014 budget was appropriated at $3.1 million.[xxxvi]

Notwithstanding its meagre resources, the PCLOB has made some contribution to the scrutiny and understanding of the surveillance that the Snowden disclosures revealed.[xxxvii] President Obama's expert review group, which inquired and reported after the Snowden disclosures, recommended replacement of the PCLOB with a board with a wider mandate that embraced not just foreign intelligence but counter terrorism.[xxxviii]

The Committee is urged to consider imbalances between what accountability bodies are expected to do and the resources they have to do it, especially when compared to the size and resources of the agencies they oversee.

The risk in leaving oversight bodies so obviously dwarfed by the entities they are supposed to hold accountable is that instead of building trust the accountability structure looks like threadbare windowdressing and trust ebbs further. This can happen regardless of the integrity and efforts of the accountability bodies themselves.

Experience suggests that poor accountability mechanisms miss problems, which then grow in the dark. They fester and cause greater harm and loss of trust when they are eventually revealed - often by a whistleblower - than they would have caused in embarrassment had they been revealed earlier through an effective accountability process. The phenomenon is not confined to intelligence and policy, nor to the public sector – the UK phone hacking scandal is a private sector example – but the phenomenon is worthy of this Committee's attention in this inquiry.

Three reforms

Help rebuild trust: repeal section 35P of the ASIO Act

This Bill is the fourth in a series which the Attorney-General has described as the most comprehensive rewrite of national security laws in 30 years.[xxxix] In the first, the *National Security Legislation Amendment Act (No 1)*, which took effect on 2 October 2014, a new

offence was inserted into the *ASIO Act* as section 35P. It exposes to criminal prosecution and prison terms persons, including journalists in the course of their legitimate work, who disclose information about a special intelligence operation. No public interest defence is provided.

During the passage of the legislation Parliament did not have the benefit of advice from the Independent National Security Legislation Monitor because the position was vacant.

In the period since, a significant range of diverse voices have raised concerns about section 35P and suggested that it goes too far.

In opposing the provision in its submission to this Committee in August last year, Guardian Australia pointed out that –

> 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. 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 also pointed to unintended consequences –

> 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 and Manning (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.

Guardian Australia submits that the Committee should take this opportunity of its report on the fourth of a related set of Bills to propose the repeal of section 35P before it does damage. In not repealed, at a minimum the section should be revisited and amended to improve the defences.

Enshrine the value of freedom of expression and the right to privacy

When, as in the current Bill, a legislature must strike a balance between values which are all of importance to a democratic society – here, privacy, security, law enforcement, freedom of expression – it helps if rights and freedoms are placed on a similar footing with security and law enforcement concerns. This is particularly important during times of heightened fear of terrorism.

The attack in Paris on 7 January 2015 on the satirical publication *Charlie Hebdo*, reminds us that democratic societies must both secure themselves against terror as far as possible whilst upholding values which characterise the society as democratic. One of those values is freedom of expression, another is privacy.

In the US this balancing tends to be achieved through the Bill of Rights in which the First Amendment and Fourth Amendment ensure that, respectively, freedom of expression and privacy can be properly considered during a balancing process. In the UK, something similar occurs through the operation of the *Human Rights Act 1998* and the way this has led to conscious consideration by UK courts of values enshrined in the European Charter of Human Rights.[xl]

In Australia, the *Human Rights (Parliamentary Scrutiny) Act 2011* is a step towards these mechanisms.[xli] But the statements of compatibility which accompany proposed legislation, including this Bill, are provided by the architects of the legislative measures which may be in tension with rights.

Guardian Australia submits that law reform aimed at enshrining fundamental rights would, if successful, ensure that balances would be struck more successfully not only when legislation is being enacted but also *when it is operating* within the democratic society it is intended to help to preserve.

Review the fast-growing intelligence and security community and the adequacy of its oversight and accountability

The Committee is urged to take the opportunity presented by this significant piece of surveillance legislation to begin a wider and longer-term review of the adequacy of the

oversight and accountability of the intelligence and security community, including those parts of police forces which do intelligence and security work.

Guardian Australia submits that a worthwhile starting point to wider reform is the set of proposals made by Senator John Faulkner, a respected parliamentarian, an experienced member of the PJCIS, and a former Defence Minister, in his paper 'Surveillance, Intelligence and Accountability: an Australian Story'[xlii] The paper is informed by history, conscious of the international context including the Five Eyes arrangement, measured in its judgments and methodical, detailed and practical in its recommendations. They include reforms to this Committee, including the extension of PJCIS oversight to the Australian Federal Police, which has significant counter terrorism and national security functions.

In concluding, Senator Faulkner writes:

> This article works from the simple proposition that enhanced power requires enhanced accountability. The greater the potential for that power to infringe on individual liberties, the greater the need for accountability in the exercise of that power. This is not to suggest that our security and intelligence agencies are acting perniciously or misusing their powers. I do not believe that to be the case. But in the relatively recent past those powers were used inappropriately, with a consequent erosion of public trust, and we must be conscious that enhancements we agree to now may lend themselves to future misuse in the absence of appropriate and effective accountability mechanisms.
>
> Of course, ultimately the constitutional duty to control executive conduct as to its lawfulness lies with the High Court of Australia. This is a fundamental but only partial aspect of the oversight of intelligence agencies. Australians need continuing assurance of much more than simply the absence of illegality. They need to be assured the agencies are serving the purpose for which they were created and that they are doing so in a cost effective way. It is the parliament to which the agencies are accountable, not the judiciary, and it is the parliament's responsibility to oversight their priorities and effectiveness, and to ensure agencies meet the requirements and standards it sets. There is no greater or more important focus of political activity in this country than parliament itself, and the Australian Parliament has no better or more authoritative forum than the PJCIS to do this job.
>
> It is the responsibility of Parliament, on behalf of the people, to balance individual liberty and national security. If the public are to have confidence that an appropriate balance has been struck and that the enhanced powers and capabilities of our intelligence and security agencies are being used only for the purposes for which they were granted, current accountability arrangements must be improved. The measures proposed in this paper will increase the accountability of our security and intelligence agencies and ensure ongoing public confidence in the integrity of these vital institutions.[xliii]

Submitted on behalf of
Guardian Australia
21 January 2015

Endnotes

[i] Telecommunications (Interception and Access) Amendment (Data Retention) Bill 2014 http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22legislation%2Fbills%2Fr5375_first-reps%2F0000%22;rec=0

[ii] New York Times online18 December 2014 http://www.nytimes.com/reuters/2014/12/18/world/europe/18reuters-spying-un.html?_r=0 ; PJIS Committee hearing transcript 17 December 2014 - http://parlinfo.aph.gov.au/parlInfo/search/display/display.w3p;query=Id%3A%22committees%2Fcommjnt%2Ff5e54f61-7ed2-4af4-a540-b83be0ae5307%2F0001%22

[iii] Submission No 12 http://www.aph.gov.au/Parliamentary_Business/Committees/Joint/Intelligence_and_Security/National_Security_Amendment_Bill_2014/Submissions

[iv] Submission 40 http://www.aph.gov.au/Parliamentary_Business/Committees/Senate/Legal_and_Constitutional_Affairs/Comprehensive_revision_of_TIA_Act/Submissions

[v] A snapshot of the debate from almost 10 years ago can be gleaned from submissions to a consultation by the Attorney-General's Department into access to communications, for example http://www.privacy.vic.gov.au/domino/privacyvic/web2.nsf/files/review-of-the-regulation-of-access-to-communications-2005 . The round of discussion that has led to the recent Bills can be traced to the Attorney-General's Department discussion paper *Equipping Australia Against Emerging and Evolving Threats*, July 2012 http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/n**sl2012/additional/discussion%20paper.pdf

[vi] http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/report.htm

[vii] Ibid. Foreword xiii-ix

[viii] In the UK and US respectively, recent reports into abuses of the *Regulation of Investigatory Powers Act 2000* (RIPA) and the US Senate Committee report into torture during the Bush Administration are sufficient illustrations of the general point. The UK Interception of Communications Commissioner's recent submission to the current Investigatory Powers Review implicitly demonstrates the point, but in a more practical sense it also includes detailed information about safeguards - http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf For a US analysis specifically relevant to this inquiry, see U.S. Department of Justice, Office of the Inspector General. (2010). "A Review of the Federal Bureau of Investigation's Use of Exigent Letters and Other Informal Requests for Telephone Records," *Department of Justice*, January 2010. Online:<http://www.justice.gov/oig/special/s1001r.pdf>.
Australia's history in this regard is usefully summarised in the October 2014 paper by Senator John Faulkner, 'Surveillance, Intelligence and Accountability: an Australian story' pp 3-25 – available at http://www.senatorjohnfaulkner.com.au/file.php?file=/news/TGRUOSECRG/index.html From a different angle, the issues are also gracefully analysed by Frank Moorhouse in his recent *Australia Under Surveillance* (Vintage Books, 2014).

[ix] The relevant reports into privacy by the Australian Law Reform Commission in 1983, 2008 and 2014 exhaustively cover that ground.

[x] The Attorney-General's Dept factsheet on data retention summarises these benefits - http://www.ag.gov.au/dataretention ; officials at this Committee's hearing on 17 December 2014 emphasised them – see transcript; the Ex Mem for the Bill outlines them; and they are also expressed in the European Commission Memo/14/269 on the Data Retention Directive, 8 April 2014 - europa.**eu**/rapid/press-release_MEMO-14-269_en.doc .

[xi] Responses given at the Committee's hearing on 17 December 2014 indicated that more CSPs than the major telecommunications providers will be involved.

[xii] The Bill's Explanatory Memorandum states that details will be in regulations. Attorney-General's Department has made public only a draft definition of the metadata to be gathered - http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/ProposeddatasetOctober2014.pdf The lack of precision about such a central element of the proposed scheme hampers all who need to make submissions before the deadline of 19 January 2015. At the 17 December 2015 hearing it was unclear whether a final definition of metadata would be available before the Committee itself was due to report in February. The issue is important because, generally speaking, access to metadata would

not require a warrant but access to the contents or substance of a communication would, Depending on how it is defined, metadata may be unexpectedly revealing. On one view, metadata may include the URL of a website visited and, as most will know, a URL will often include information indicative of the contents of the webpage (Parliamentary Library flagpost, 18 August 2014, *Access to and retention of internet 'metadata'* - *http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/FlagPost/2014/August/Access_to_and_retention_of_internet_metadata*).

[xiii] The draft UK Data Retention code, out for consultation until 20 January 2015, contains a substantial list of potential uses of data retained under that country's analogous law - https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/383401/Draft_Data_Retention_Code_of_Practice_-_for_publication_2014_12_09.pdf
Attention is drawn to the recommendation of Parliament's Joint Committee on Human Rights, in its November 2014 report on this Bill, that on proportionality grounds access to the retained data be restricted to what is necessary for investigating specific serious crimes such as major indictable offences and specific serious threats – 'Report on examination of legislation in accordance with the Human Rights (Parliamentary Scrutiny) Act 2011', pp10-22 at para1.51

[xiv] Service providers, responding to customer disquiet, have indicated an interest in increasing encryption, but governments such as the Cameron Government in the UK discourage encrypted services to which government agencies cannot obtain access - http://www.theguardian.com/us-news/2015/jan/15/-sp-secret-us-cybersecurity-report-encryption-protect-data-cameron-paris-attacks

[xv] http://www.ag.gov.au/NationalSecurity/DataRetention/Documents/ProposeddatasetOctober2014.pdf

[xvi] *Riley v California* 573 US, decision June 2014, available at http://www2.bloomberglaw.com/public/desktop/document/Riley_v_California_No_13132_and_13212_US_June_25_2014_Court_Opini The Canadian Supreme Court recently affirmed the significance of the privacy interest in customer data held by Internet Service Providers and underlined the requirement that agencies seeking it must have lawful authority to do so: *R v Spencer* 2014 SCC 43

[xvii] Summary available at http://www.thebureauinvestigates.com/2014/09/14/a-summary-of-the-bureaus-application-to-the-european-court-of-human-rights/

[xviii] See http://www.theguardian.com/uk-news/2015/jan/19/gchq-intercepted-emails-journalists-ny-times-bbc-guardian-le-monde-reuters-nbc-washington-post

[xix] Available at http://www.hrw.org/reports/2014/07/28/liberty-monitor-all-0

[xx] The program is introduced at https://immersion.media.mit.edu/

[xxi] *Digital Rights Ireland and Seitlinger*, 8 April 2014, judgment available at http://curia.europa.eu/juris/document/document_print.jsf?doclang=EN&text=&pageIndex=0&part=1&mode=lst&docid=150642&occ=first&dir=&cid=314051

[xxii] Data Retention and Investigatory Powers Bill, Standard Note SNHA6934, 16 July 2014, at page 9 - http://www.parliament.uk/briefing-papers/sn06934/the-data-retention-and-investigatory-powers-bill

[xxiii] C. Parsons, Lawful Access and Data Preservation/Retention: present practices, ongoing harm and future Canadian policies (2012) - http://www.christopher-parsons.com/Main/wp-content/uploads/2012/02/Lawful-Access-Report-v.2.2Final.pdf More recent Canadian experience is summarised at http://www.giswatch.org/en/country-report/communications-surveillance/canada

[xxiv] See Ex Mem: 'While the detail of the dataset will be included in the supporting regulations, this Compatibility Statement addresses the data to be retained to the extent that the key attributes of retained data are reflected in this Bill.' - http://parlinfo.aph.gov.au/parlInfo/download/legislation/ems/r5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001/upload_pdf/14242b01EM.pdf;fileType=application%2Fpdf#search=%22legislation/ems/r5375_ems_e6cf11b4-5a4e-41bc-ae27-031e2b90e001%22

[xxv] As recommended by Parliament's Joint Committee on Human Rights, at paras 1.36-1.37 of its report on the Bill.

[xxvi] Victorian legislation is at http://www.legislation.vic.gov.au/Domino/Web_Notes/LDMS/PubStatbook.nsf/f932b66241ecf1b7ca256e92000e23be/A8643A46DC859F89CA25795E0009168A/$FILE/11-072a.pdfbookmarked.pdf
;Queensland's PIM annual report - http://www.parliament.qld.gov.au/Documents/TableOffice/TabledPapers/2012/5412T1635.pdf ; criminal organisation PIM has been more recently established http://governmentbodies.premiers.qld.gov.au/BodyDisplay.aspx?Parameter=743

[xxvii] ALRC Report 108, at para 71.71, 71-2e

[xxviii] http://www.leahy.senate.gov/download/hen14602

[xxix] Queensland, Parliamentary Debates, Legislative Assembly, 22 November 2005, Second Reading

Speech to the *Terrorism (Preventative Detention) Bill* (The Hon Peter Beattie, Premier), page 4064.

[xxx] Guardian Australia, 20 October, 22 October 2014 - http://www.theguardian.com/world/2014/oct/20/australian-government-metadata-requests-far-higher-than-disclosed; http://www.theguardian.com/australia-news/2014/oct/22/telcos-may-no-longer-be-required-to-publish-lists-of-metadata-requests

[xxxi] UK Data Retention – draft code – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/383401/Draft_Data_Retention_Code_of_Practice_-_for_publication_2014_12_09.pdf

[xxxii] People are usually entitled to known who is collecting their personal information and what it is being used for - http://www.oaic.gov.au/privacy/privacy-resources/privacy-fact-sheets/other/privacy-fact-sheet-17-australian-privacy-principles

[xxxiii] UK Data Retention – draft code – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/383401/Draft_Data_Retention_Code_of_Practice_-_for_publication_2014_12_09.pdf

[xxxiv] UK Data Retention – draft code – https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/383401/Draft_Data_Retention_Code_of_Practice_-_for_publication_2014_12_09.pdf para 8.7

[xxxv] IGIS annual report 2013-14 vailable at http://www.igis.gov.au/annual_report/13-14/pdfs/IGIS_annual_report_13-14.pdf; Canada's oversight body, the Canadian Security Establishment Commissioner, had $C2.28m and eight staff in 2012-13, according to that year's annual report - http://www.iocco-uk.info/docs/IOCCO%20Evidence%20for%20the%20Investigatory%20Powers%20Review.pdf – and 11 staff and almost $C2m in 2013-14 according to the new Commissioner's latest annual report - http://www.ocsec-bccst.gc.ca/ann-rpt/2013-2014/index_e.php

[xxxvi] US PCLOB semi-annual report, released 22 December 2014 - http://www.pclob.gov/library/Semi_Annual_Report-Sept2014.pdf page 7

[xxxvii] See, for example, its reports into section 702 of the Foreign Intelligence Surveillance Act http://www.pclob.gov/library/702-Report.pdf ; and into section 215 of the Patriot Act http://www.pclob.gov/library/215-Report_on_the_Telephone_Records_Program.pdf

[xxxviii] *Liberty and Security in a Changing World – report and recommendations of the President's Review Group on Intelligence and Communications Technologies*, December 2013 - http://www.whitehouse.gov/blog/2013/12/18/liberty-and-security-changing-world

[xxxix] Senator George Brandis, 'One more anti-terror tool', *The Australian*, 12 January 2015 page 10

[xl] For recent examples by the UK Supreme Court, see *Bank Mellat v Her Majesty's Treasury (No 2)* [2014] AC 700 and *R (Lord Carlile of Berriew QC) v Home Secretary* [2014] UKSC 60

[xli] Human rights acts exist in Victoria and the ACT. The Joint Parliamentary Committee on Human Rights uses an approach similar to the UK/European one in its analysis of this Bill.

[xlii] Op cit endnote viii - http://www.senatorjohnfaulkner.com.au/file.php?file=/news/TGRUOSECRG/index.html

[xliii] Ibid p 50-51