PRIVACY IMPACT ASSESSMENT

Preliminary Report

TELECOMMUNICATIONS (INTERCEPTION AND ACCESS) ACT 1979 REFORM

For: Attorney-General's Department

December 2011

Table of Contents

1 EXECUTIVE SUMMARY

1.1 INTRODUCTION

The Attorney-General's Department (AGD) commissioned Information Integrity Solutions Pty Ltd (IIS) to undertake a privacy impact assessment (PIA) in the context of its current review of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

The TIA Act has provided a basis for the lawful interception regime since 1979. However, significant changes in technology, industry practice and consumer behaviour are challenging the effectiveness of the regime. In response to these challenges, and also in the interests of simplifying the legislation and making it more consistent and coherent, the Government has given in-principle agreement to the development of reforms to the TIA Act. The reforms will consider the operation of the Act from the perspective of its law enforcement and national security objectives. However, the possible privacy impact of any changes will also be an important consideration.

The TIA Act already recognises that the interception of essentially private communications, and the gathering of data related to communications processes, is inherently privacy intrusive. Its primary objectives are to protect privacy and to set out a strict framework for interception. The framework limits interception to serious offences, requires its use to be justified and provides a range oversight and accountability measures.

This privacy assessment comes at an early stage in the review of the TIA Act, prior to any wider public consultation. An early stage review means that privacy issues can be considered and addressed where possible in the development process and IIS commends this approach. It also welcomes the proactive consideration of privacy risks and protections that are already evident in the drafting instructions.

1.2 PRELIMINARY FINDINGS

The report sets out IIS's preliminary findings and recommendations in relation to AGD's current proposals for amendments to the TIA Act as set out in drafting instructions provided to IIS in October 2011. The findings and recommendations are primarily based on the proposals as set out in the drafting instructions, but also take into account other briefing material provided and meetings with agency and industry stakeholders.

The analysis has focussed on areas of significant change, and in particular on the key themes and proposals that IIS considers are most likely to have privacy impacts or raise privacy issues, rather than a line-by-line analysis of the drafting instructions. The preliminary findings and recommendations are also based on IIS's understanding at this point and may change following feedback and/or clarification from AGD or further stakeholder consultations.

The process of finding an appropriate balance for the exercise of intrusive powers while taking account of the community's interest in privacy is complex and raises difficult questions. IIS commends the approach taken so far in the AGD material and in the drafting instructions; privacy issues are squarely on the agenda and are being given careful consideration. IIS also acknowledges that the existing TIA Act, as well as the other laws, including the Privacy Act, provides a rigorous framework of accountability and oversight by independent bodies.

In considering the proposals, IIS has taken account of this framework and it has also considered the following matters.

Community expectations about a safe society, the use of intrusive powers and about privacy is clearly an important consideration but is also a complex area. There will be a range of views about what is expected or appropriate, including: those who think community safety and protection is paramount; those who feel in the digital age there can be no expectation of privacy; and those who value privacy strongly or who appreciate the need for intrusive powers but are concerned about how the powers are exercised. Ultimately, in Australia the community expects the Parliament to decide on the extent of intrusive powers and what safeguards are needed including for privacy. For the purposes of this analysis, IIS assessed the proposals against the balance currently set by the TIA Act and has also considered views expressed by the agencies participating in consultations and issues that have been raised in the past by privacy advocates and oversight bodies.

IIS has also considered the changing environment in which the telecommunications interception will take place. Of particular significance is the changing and exponentially expanding nature of the information that is collectable including:

- old types of data that has been useful may no longer even be created
- new types of data which are not necessarily accessible via carriage service providers and other traditional sources and
- very significantly, the emerging importance and richness of data.[1]

In thinking about privacy specifically, IIS has focussed on the range of matters addressed in the Information Privacy Principles (IPPs) in the Privacy Act as well as broader privacy concerns.

Often privacy principles are described as giving individuals control, to the extent possible, over personal information about themselves. In the context of the TIA Act individuals have little control over their personal information – they will not have a choice, and in most cases will not be advised, about whether their communications are intercepted or data about them disclosed and generally they will not have the usual access and correction rights. In such an environment the privacy protection focus moves from individual control, via notice and the ability to exercise informed to consent, to a focus on others, government agencies in particular, keeping personal information under control. The most relevant privacy principles here are:

- collection limitation (IPP 1)
- transparency (IPP 2 and IPP 5)
- security (IPP 4)
- use and disclosure controls (IPPs 10 and 11). [2]

[1] The term data is widely used and has a range of meanings. For the purposes of this report, IIS has used the following terms: content means the substance of a communication (see section 172 of the TIA Act) and non-content data means information about a communication not including the content of a communication. The latter can be Information about individuals held by telecommunications providers including subscriber name, address and date of birth, call routing details, and call charge records. It can also be information about a device or a computer.

Finally, IIS also considered its 'layered defence' framework, particularly in relation to the law and to governance, and the Office of the Australian Information Commissioner's (OAIC's) '4As' framework, in its analysis and in developing recommendations.

Overall, IIS considers that a number of the changes proposed are positive from a privacy perspective. In particular, it welcomes the new objects clause. On the other hand, some of the proposals do seem to shift the balance to a greater privacy impact. In its recommendations IIS has suggested that more evidence or justification would be helpful in some cases and it has also made a range of other recommendations for options to mitigate possible privacy impacts.

1.3 Preliminary Recommendations

Preliminary Recommendation 1 – Objects clause

IIS recommends that in developing the proposals further, the AGD should ensure the objects clause conveys the clear message that the TIA Act is primarily aimed at protecting privacy of communications with interception occurring only in limited, justified and proportional circumstance. It therefore recommends that in addition to the current elements in the drafting instructions the objects clause include that interception should proceed only where it is limited and proportional, and is justified and accountable to an independent authority.

Preliminary Recommendation 2 – Warrant Processes for Access to Content and TIA Act Guidance, Training and Community education

IIS recommends that in developing the proposals further, the AGD should:

- ensure that where interception is permitted on the basis of knowledge or consent of a party to the communication, this should be on the basis of knowledge or consent of all parties to communication not just one or some
- retain the 7 year threshold for interception other than in specified circumstances where a lower threshold is already permitted
- if the threshold is lowered to 5 years, the exposure draft of the legislation must be accompanied by:
    - a clear justification that explains how this is consistent with the objects clause as proposed in IIS preliminary recommendation 1
    - and an estimate of the impact of the measures, in terms of the nature of crimes or offences brought in and an estimate of the number of warrants that would be issued compared with the current law
- build in transparency about the nature and implications of the possible attributes that could be used to define warrant targets (replacing the current concept of warrants based on

[2] The Government is currently developing amendments to the Privacy Act based on the recommendations in the ALRC's report on privacy. The IPPs (and the private sector National Privacy Principles) will be replaced with the Australian Privacy Principles; these will have strengthened transparency provisions calling for the development and provision of privacy policies.

specified services, devices or named persons), and appropriate limits, both in the drafting of the legislation and in consultations undertaken on the exposure draft including by:

  - developing a detailed description of the nature of possible attributes
  - developing criteria to assist issuing authorities to consider the privacy implications of attributes, for example
    - the extent of communications to be intercepted
    - the extent to which they may result in the capture of non-target communication including B parties
    - strength of association of the attributes to a suspect or suspects
    - prohibition on 'fishing expeditions' for example, as noted in the drafting instructions, where a word or string of words in communications is targeted and
  - providing that permitted attributes will be listed in regulations

- ensure that the issuing authorities have access to advice about the privacy implications of attributes from independent, expert third parties, as well as from the requesting agency, that might include:
  - the establishment of an appropriately resourced federal level public interest monitor and/or a panel of experts available to offer advice
  - the availability of training or educative material based on ongoing monitoring of, and research into the nature of attributes
- build in a requirement for detailed reporting on the nature of attributes used and the impact on nature of communications intercepted (similar to the current requirement to report on the number of services intercepted)
- ensure that any streamlining of the matters that an issuing authority must take into account, as well as the proposed new requirement for proportionality, retains the need to consider the conduct being investigated, the potential intrusion on privacy, and the likely usefulness of the material to be gathered
- as flagged in the drafting instructions, explore additional pre and post accountability measures for warrants which an agency exercises without third party involvement – these measures might include:
  - a requirement to include the proposal, and rationale, in the warrant application
  - criteria and expert advice available to issuing authorities to assist them to understand the implications of the applications

    - ensuring that the IGIS and the Ombudsman have a particular obligation to examine all aspects of the interception processes undertaken without third party and to report to the Attorney-General on any underlying issues or trends
    - interception undertaken without third party involvement to be specifically reported in the TIA Act annual report and
- as flagged in the drafting instructions, provide that decryption notices are authorised by issuing authorities and that additional justification is required where the agency seeks encryption keys as well as or instead of decrypted content and
- ensure that resources are available and responsibility is allocated for the development of information and guidance material about the TIA Act, for example as identified by the ALRC Report 108, and for the development and delivery of regular community education programs about the Act.

Preliminary Recommendation 3 – Authorised access to Non-content data

IIS recommends that in developing the proposals further, the AGD should:

- in recognition of the increasing volume and sensitivity of non-content data, provide that access to non-content data other than subscriber data (particularly prospective data but preferably all) is only available under a warrant
- if a warrant approach to access to non-content data, other than subscriber data, is not adopted, specify more sensitive classes of non-content data that would require independent authorisation – these might include:
    - prospective data
    - historical data about a number of people in order to counter any argument that such collection might be a 'fishing expedition' and
    - historical or prospective geo-location data
- if a warrant approach to access to all non-content, non-subscriber data is not adopted, consider including appropriate minimum penalty requirements as pre-requisite for all authorisations as well as requiring that the access is 'reasonably necessary' and proportional (as proposed in the drafting instructions)
- provide that agency internal authorisations are based on detailed documentation of the grounds for the decision, including the nature and extent of non-content data required, the purpose of the access, for example whether it is needed to assist in targeting a warrant or for direct investigative purposes, and the likelihood that it will assist the purpose
- provide in the legislation for detailed guidelines on the factors that might affect the privacy and proportionality of an authorisations to assist authorising officers
- if access to non-content data is authorised internally, ensure that the Commonwealth Ombudsman (CO) (and the Inspector General of Intelligence and Security (IGIS) against the

separate Australian Security and Intelligence Organisation (ASIO) processes) is given specific responsibility to monitor and report on the decision making process, taking account of:

  - determinations made under s.183(1)(f)
  - liaison with the Privacy Commissioner about any findings or trends in relation to service providers compliance with their record keeping obligations
  - a systemic assessment of the impact of authorisations to identify any issues in process or accountability that should be addressed

- provide that the Attorney- General's annual report required under the TIA Act to include numbers of voluntary disclosures, that is those made without an authorisation (these were reported when the Australian Communications Authority and then ACMA had the reporting function).

Preliminary Recommendation 4 – Use, Disclosure and Destruction of Accessed Content and Non-content Data

IIS recommends that in developing the proposals further, the AGD should:

- prohibit the re-use of non-content data acquired on the basis of authorisations for intelligence
- if use for intelligence purposes is permitted, in recognition of the increasing volume and sensitivity of non-content data, ensure that the draft legislation only permits retention, use and disclosure of this data for intelligence in limited, specified circumstances such as proposed in the Blunn Report and also considering IIS' preliminary recommendation 3
- if agencies are permitted to retain non-content data for specified intelligence purposes, records should be kept on the nature of the data retained, when it is used or disclosed and when it is destroyed and the CO should have responsibility and powers to monitor and report on the extent of, and trends, in data retained for intelligence purposes
- if non-content data is retained for Intelligence purposes but is not admissible in court the legislation should provide that it should be not be used to make decisions that would significantly affect an individual without providing them a right of hearing or reply
- provide in the legislation for the development of standards or guidance on what would constitute reasonable steps for destruction of content and non-content data as soon is it can no longer be legitimately retained.

Preliminary Recommendation 5 – Reporting, Accountability and Oversight

IIS recommends that in developing the proposals further, the AGD should:

- ensure that reports on the operation of the TIA Act include sufficient information to allow the Parliament, interest groups and the community to understand and assess the impact of the TIA Act, in particular the reports should:

- include information about the 'shape' of the industry, including:
  - estimates of industry parameters as a whole such as number of fixed line calls, mobile calls, VOIP calls, SMS messages, emails and instant messages that are exchanged in Australia annually
  - the number of participants in social networking activities and
  - indicators of the average levels of activity and the types and numbers of service providers that have been requested to provide assistance to agencies

  so that the number interceptions can be considered as proportion of all call as well as in absolute terms, giving a clearer indication of the growth or otherwise in interceptions and authorised disclosures
- retain information about the cost of interception
- ensure that any changes to the reporting of outcomes on interception allows understanding of the attributes used to target warrants and does not otherwise reduce the transparency and accountability of reports, particularly in relation to the extent to which interceptions capture information about innocent third parties (B parties)
- provide more detail on access to non-content data on matters such as the purpose for access, the nature of the data accessed, how many people are affected by a request and the outcomes
- use measures, in addition to numbers of accesses, to give an indication of the extent to which accesses may be increasing or decreasing as a percentage of overall communications
- provide information about the use of encryption notices
- provide details about interception without third party involvement
- report on the role of issuing authorities, including for example the number of warrants where attributes are withdrawn and the extent to which external advice on privacy implication of attributes, or how to assess proportionality was sought and was available and any difficulties identified
- provide for the Attorney-General to report on resourcing for monitoring functions and the extent to which concerns are expressed by the CO, or other stakeholders or commentator and
- to the extent that the changes aim for consistency with reporting under Surveillance Devices Act 2004 changes do not reduce current level of TIA Act transparency

- ensure that, as is proposed in the drafting instructions, the CO's monitoring role is defined broadly covering compliance with the law, how the system is operating overall, and any emerging issues with an impact on privacy
- provide for the IGIS to have a specific responsibility to incorporate into his or her regular inspection program oversight of the use of powers to obtain prospective telecommunications data by ASIO
- require that the CO's reports are made public to the extent possible, allowing for the excision of sensitive material
- ensure that permitted data exchanges between State Ombudsman and the CO are sufficient to allow cooperation for joint investigation or multi- jurisdiction investigations
- provide for regular surveys or research on issuing authorities and how competent they feel to make decisions on impact on privacy, proportionality and a requirement for the Attorney-General to respond to any issues identified and
- consider the resources required to ensure that the TIA Act oversight, accountability and complaint handling functions are effective and make this known to decision-makers.

Preliminary Recommendation 6 – Industry Obligations

IIS recommends that in developing the proposals further, the AGD should ensure that:

- all organisations that will have obligations under the TIA Act should be subject to the Privacy Act, whether or not the organisation might otherwise by exempt from the Privacy Act because of the small business operator provisions
- there will be transparency about the role of the industry in assisting with interceptions and in providing access to non-content data – measures might include:
    - providing regular public information about industry obligations and
    - requiring industry service providers to advise their customers, in general terms, about their obligations under the TIA Act, and in particular obligations to provide decrypted documents or encryption keys
- in addition to TIA Act provisions relating to the security of the interception process that the legislation address the security of information about individuals who have been subject to interception or data access and provide for data breach obligations on service providers, whether directly to individuals or to a regulator on their behalf
- the approach to cost sharing between agencies and the industry operates as a signal that interception is an exceptional rather than routine investigative tool.

Preliminary Recommendation 7 – Non-Content Data Retention

IIS recommends that in developing the proposals further, the AGD should:

- to the extent possible, include provisions relating to non-content data retention in the primary legislation rather than in regulation
- support the exposure draft of the legislation with detailed and concrete evidence on the issues and problems the proposals address
- apply the provisions only to non-content data that service providers would otherwise collect for their particular business model – in other words there should be no requirement to collect/generate data if it is not required for business needs
- limit the non-content data retention requirement to a short period (6 months) unless there is strong evidence relevant to Australia of the utility of a longer period
- require the prior approval of an independent body for access requests for older non-content data or for particularly sensitive data such as geo-location data
- provide that the obligation to retain non-content data is subject to prior notice to individuals that this will occur
- include measures to protect retained information from misuse, loss or other unauthorised (or new) uses such as security requirements and data breach notification (as proposed in preliminary recommendation 6
- subject to consultation on the exposure draft, prohibit the central storage of retained non-content data on the grounds that the 'honey pot' effect is likely to outweigh other concerns
- clearly define the nature of the non-content data that can or cannot be retained, for example does this include location data or the content of web pages.

2 INTRODUCTION

The Attorney-General's Department (AGD) commissioned Information Integrity Solutions Pty Ltd (IIS) to undertake a privacy impact assessment (PIA) in the context of its current review of the *Telecommunications (Interception and Access) Act 1979* (TIA Act).

The TIA Act has provided a basis for the lawful interception regime since 1979. However, significant changes in technology, industry practice and consumer behaviour are challenging the effectiveness of the regime. In response to these challenges, and also in the interests of simplifying the legislation and making it more consistent and coherent, the Government has given in-principle agreement to the development of reforms to the TIA Act. The reforms will consider the operation of the Act from the perspective of its law enforcement and national security objectives. However, the possible privacy impact of any changes will also be an important consideration.

The TIA Act already recognises that the interception of essentially private communications, and the gathering of data related to communications processes, is inherently privacy intrusive. Its primary objective is to protect privacy and it then sets out a strict framework for interception. The framework limits interception to serious offences, requires its use to be justified and provides a range oversight and accountability measures.

This privacy assessment comes at an early stage in the review of the TIA Act, prior to any wider public consultation. An early stage review means that privacy issues can be considered and addressed where possible in the development process and IIS commends this approach. It also welcomes the proactive consideration of privacy risks and protections that are already evident in the drafting instructions.

IIS has identified a range of matters that, if addressed, will further mitigate many of the potential privacy risks. Addressing these matters should allow the TIA Act framework to be safely modernised in a way that allows vital access for law enforcement/other interests and retains community trust.

2.1 PURPOSE AND SCOPE OF THE PIA

The purpose of the PIA is to:

- provide input to the development of proposed amendments to the TIA Act
- complement broader project risk management processes, and
- assist Government decision-making.

The scope of works is to

- undertake all necessary research and analysis, drafting, consultations and present the material in a suitable format
- review proposals for the TIA Act amendments as they are developed and map information flows, identify privacy issues, high level privacy risks, and possible mitigation strategies

- provide input to implementation planning including advising on strategies for public consultation on privacy matters
- provide input to the development of legislative proposals commenting on drafting instructions and draft legislation
- prepare draft and final PIA reports
- brief senior AGD management summarising development of impact assessment and outcomes

2.2 Assumptions and qualifications applied to the PIA

IIS applied the following assumptions to the PIA:

- it is not necessary or efficient to focus on every possible privacy risk, rather it is better to focus on the most critical issues and
- the information and documents made available will have provided IIS with the information that would be most critical to the privacy analysis.

The PIA is intended as general policy advice. It is not intended to be and should not be regarded as constituting legal advice.

2.3 Methodology

The PIA involved the following steps

- consultation with AGD and finalisation of work plan – in this phase, IIS discussed the project approach and confirmed the project plan to deliver the work
- information gathering – in this phase IIS gathered information about the project, in particular from AGD's drafting instructions for the proposed amendments and discussions with stakeholders, as well as other research – Appendix 2 lists the material reviewed
- analysis – in this phase IIS developed an understanding of the current TIA Act regime, and related personal information flows and identified privacy risks and benefits associated with the proposals set out in the drafting instructions taking into account of the Information Privacy Principles (IPPs) in the *Privacy Act 1988* (Cth)(the Privacy Act) and other more general risks and community concerns that tend to arise in the context of the use of intrusive powers as well as IIS's layered defence framework and the Office of the Information Commissioner's (OAIC's) '4As' framework
- draft report – IIS then prepared its draft preliminary report and provided this to AGD for comment
- finalisation of report – IIS finalised the report following comment and feedback from AGD.

As noted, in developing its recommendations IIS drew on its 'layered defence' approach. This applies a number of possible 'tools' to arrive at practical solutions that fit the particular circumstances. These tools include:

- **'business as usual'** good policy and practice, including education, process and culture change regarding the expectations about the way things are done by staff, and the actions that users need to take to protect themselves
- **additional law** where risks are particularly high (for example specific use and disclosure limitations, criminal penalties, special measures to ensure review before critical changes are made)
- **technology**, including design limits on information collected, what can be connected and who can see what
- **governance**, including transparency and accountability
- **safety-net** mechanisms including easily accessible complaint mechanisms for affected citizens when failure or mistakes occur.

Given the current stage of the AGD proposals, IIS' recommendations focus on amendments to the law, including as they relate to governance and safety-net. As noted, IIS has also drawn on the OAIC 4As framework, which offers a structure for the making decisions about the use of intrusive powers as follows:

- **Authority** – powers conferred expressly by statute subject to objective criteria, authority to exercise intrusive powers should be dependent on special judicial authorisation, intrusive activities authorised by an appropriately senior officer
- **Analysis** – to ensure proposal are necessary, effective, proportional, the least privacy invasive option and consistent with community expectations
- **Accountability** – transparent and ensure accountability processes including independent complaint handling, monitoring, independent audit, and reporting and oversight powers commensurate with the intrusiveness of the measures
- **Appraisal** – periodic appraisal of the measure to assess costs and benefits

2.4 MEANING OF TERMS AND GLOSSARY

The terms content and telecommunications data are critical to the application of TIA Act but are also used widely in a range of other circumstances. There have been calls, including by the Australian Law Reform Commission (ALRC) in its 2008 report of it inquiry into Australian privacy law and practice, for these and other terms used in the TIA Act to be defined or defined more clearly.[3] The drafting instructions recognise this issue and identify a number of terms, including telecommunications data, which need to be addressed.

[3] Australian Law Reform Commission (ALRC) Report 108 *For Your Information: Australian Privacy Law and Practice* available at http://www.alrc.gov.au/publications/73.%20Other%20Telecommunications%20Privacy%20Issues/telecommunications-interception-and-access- (Recommendations 73.14 and 73.121)

Pending the development of specific definitions and for the purposes of this report, IIS has used the following terms:

- content means the substance of a communication (see section 172 of the TIA Act) and
- non-content data means information about a communication not including the content of a communication. The latter can be Information about individuals held by telecommunications providers including subscriber name, address and date of birth, call routing details, and call charge records. It can also be information about a device or a computer.

2.4.1 GLOSSARY

Abbreviation or term	Expansion or meaning
AAT	Administrative Appeals Tribunal
ACMA	Australian Communications and Media Authority
AFP	Australian Federal Police
AGD	Attorney-General's Department
Agencies	Specified Commonwealth and State and Territory agencies able to apply for warrant or issue authorisation to obtain telecommunications data
ALRC	Australian Law Reform Commission
ASIO	Australian Security Intelligence Organisation
CAC	Communications Access Coordinator
CO	Commonwealth Ombudsman
Content	The substance of a communication (see section 172 of the TIA Act)
IIS	Information Integrity Solution Pty Ltd
IPPs	Information Privacy Principles in the Privacy Act
Issuing Authority	A person appointed by the Minister to issue warrants, a judge of a court of federal jurisdiction created by the Parliament, a federal magistrate, a magistrate, or a Deputy President or member of the Administrative Appeals Tribunal with relevant legal qualifications
Non content data	Data is information about a communication not including the content of a communication. It can be Information about individuals, associated with a telecommunications held by an industry participants including subscriber

Abbreviation or term	Expansion or meaning
	name, address and date of birth, call routing details, call charge records but could also be information about a device or a computer
NPP	National Privacy Principles in the Privacy Act
OAIC	Office of the Australian Information Commissioner
PIA	Privacy Impact Assessment
PIM	Public Interest Monitor
Privacy Act	Privacy Act 1988
Service provider	Telecommunications industry participants including carriers, carriage and other service providers
TA	Telecommunications Act 1997
TIA Act	Telecommunications (Interception and Access) Act 1979

3 BACKGROUND TO THE PROPOSED REFORMS

3.1 DRIVERS FOR REVIEW

As noted in the introduction, the TIA Act has provided a basis for the lawful interception regime since 1979. However, significant changes in technology, industry practice, consumer behaviour and even patterns of criminal activity are challenging the effectiveness of the regime. The TIA Act also has some inherent 'drafting' problems that IIS understands make it difficult to apply and to monitor. Some of the key challenges are noted below.

3.1.1 CHANGES IN TELECOMMUNICATIONS TECHNOLOGY AND USAGE

There have been some very significant changes in telecommunications technology in recent years that have made it increasingly difficult to conduct interception and for agencies to access non-content data. These changes include:

- a significant move from fixed-line to mobile telephones – at the end of June 2011, there were 9.7 million mobile handset subscribers in Australia representing an increase of 18.1% from just December 2010[4]
- a move to internet protocol based infrastructure away from the older 'circuit-switched' systems – increased network coverage and availability has resulted in an increase in voice over Internet Protocol (VoIP) usage from 14% of the population aged 16 years and over at June 2009 to 16% at June 2010[5]
- Australian consumers are increasingly accessing multiple technologies and services to communicate, with 58% of adults who use a fixed line service also using a mobile phone, a VoIP service and the Internet[6]
- an increase in the number of service providers in the telecommunications industry – from a time when there was a single provider, at June 2010 there were 306 fixed-line telephone service providers and three mobile network operators[7]
- increasing globalisation of services means that Australians may be using telecommunications providers that are based overseas for Internet or VoIP services
- a number of services, for example communications using a Blackberry are default- encrypted
- increasing difficulties in accessing telecommunications non-content data (details about subscribers and use of a telecommunication service as distinct from the content of the communications) arising from the following factors:
    - the increasing number of service providers also affect ability to access non-content data

[4] ABS Catalogue 8153.0 – Internet Activity Australia, June 2011
[5] ACMA Communications Report 2009-2010 at p 143
[6] As above at pp 143 and 146
[7] As above at p 146

- increasing fragmentation of the industry – carriers and carriage service providers are now not the only bodies that may carry content or generate non-content data because, for example, there may be a split between infrastructure owners, providers of services and information people obtain by using services (for example ISPs do not hold information about Facebook accounts)
- while carriers and carriage service providers keep relevant non-content data for business purposes such as taxation and billing for up to seven years, there is no uniformity about what data is kept and the length of time it is retained
- traditionally such information was generated and retained by industry for business purposes such as billing but the trend is now towards fixed price contracts or plans and so there is less need to keep detailed supporting information[8] and
- there are also changes in where non-content data is stored (carriers may use third parties, possibly in other countries, to undertake billing, account management).

3.1.2 CHANGES IN PATTERNS OF CRIMINAL ACTIVITY

The changes in the telecommunications industry described above are also leading to changing patterns of criminal activity and making the investigation and prosecution process more difficult.

Changes in telecommunications technology and services have supported and facilitated old forms of crime and allowed new forms of crime to emerge that are unique to the virtual space.[9] There is a range of evidence pointing to the increasing use of mobile and Internet technologies in drug related crime and to increasing risks of identity theft. These technologies also appear to be facilitating cross border criminal activity in drugs, pornography and cybercrime is also increasingly an organised, transnational and multi-dimensional threat.[10]

3.1.3 TIA ACT STRUCTURAL AND DRAFTING ISSUES

It is well recognised that TIA Act is lengthy, opaque, overly complex and confusing in application. In its discussions with AGD and stakeholders IIS was advised that the changing environment and complexity of drafting makes it increasingly difficult to know if and when the TIA Act may be used.

The simplifying and streamlining aims of the reform process align with the Government's broader interest in improving the clarity of Commonwealth legislation. This 'Clearer Laws agenda' forms part of the Government's Strategic Framework for Access to Justice, which was announced by the Attorney-General on 17 May 2010.[11]

[8] This seems to be an international trend – the European Commission's evaluation report of its Data Retention Directive (see 3.2.1 below) noted that 'trends in business models and service offerings, such as the growth in flat rate tariffs, pre-paid and free electronic communications services, meant that operators gradually stopped storing traffic and location data for billing purposes thus reducing the availability of such data for criminal justice and law enforcement purposes (page 3)

[9] UN Office of Drugs and Crime 2010, *Globalisation of Crime,* at p 31

[10] Organised Crime in Australia, ACC report 2011 p 18

[11] The Attorney-General's speech, and references to the strategic framework are available at http://www.ema.gov.au/www/ministers/mcclelland.nsf/Page/Speeches_2010_17May2010-SpeechattheLaunchofNationalLawWeek-ImprovingAccesstoJustice

3.2 Related Australian and International developments

3.2.1 European Union – Data Retention Directive Review

As will be discussed in section 6 below, the proposed amendments to the TIA Act include the introduction of a data retention regime. The European Union (EU) has had a data retention regime since 2006. Directive 2006/24 requires Member States to oblige providers of publically available electronic communications services or of public communications networks to retain traffic and location data for between six months and two years for the purpose of the investigation, detection and prosecution of serious crime.[12]

The European Council has recently reviewed the Directive. It is undertaking some further work to assist it to refine the provisions of the Directive but it concluded that 'overall, the evaluation has demonstrated that data retention is a valuable tool for criminal justice systems and for law enforcement in the EU'. [13] Areas that have been identified for further examination include:

- more harmonisation of, and possibly shortening, the periods of mandatory data retention
- ensuring independent supervision of requests for access and of the overall data retention
- limiting the authorities authorised to access the data
- reducing the data categories to be retained
- guidance on technical and organisational security measures for access to data including handover procedures
- guidance on use of data including the prevention of data mining and
- developing feasible metrics and reporting procedures to facilitate comparisons of application and evaluation of a future instrument.

3.2.2 Cybercrime Bill

Australia has been invited to accede to the Council of Europe's Convention on Cybercrime (the Convention). Before Australia can accede, relevant Australian laws must comply with the Convention. Most laws already comply and areas that are not fully compliant have been addressed in the Cybercrime Legislation Amendment Bill 2011. A key measure contained in the Bill is the creation of a stored content preservation regime that will ensure that evidence is not deleted by telecommunications carriers through normal business practices before a warrant can be issued. If enacted, this measure would enable agencies, on a case-by-case basis, to ask carriers to preserve stored communications, such as SMS messages, that might otherwise be destroyed before a warrant is issued.

The Bill also:

- builds on the existing framework for Australian agencies to have greater co-operation with overseas partners in the investigation of cybercrime and

[12] Available at http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2006:105:0054:0063:EN:PDF
[13] Evaluation report on the Data Retention Directive (Directive 2006/24/EC) available at http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf

- extends the scope of existing Commonwealth computer offences to fully meet the requirements for such offences under the Convention on Cybercrime, while preserving existing state laws.

3.3 PREVIOUS REVIEWS

The TIA Act has been reviewed on a number of previous occasions and these reviews have shaped the current form of the Act and also raised matters that relevant in this current review. A brief overview of the previous reviews is at Appendix 1.

4 OVERVIEW OF THE TIA ACT INCLUDING PERSONAL INFORMATION AND OVERSIGHT AND ACCOUNTABILITY

4.1 OVERVIEW OF TIA ACT, INDUSTRY PARTICIPANTS AND PERSONAL INFORMATION FLOWS

The TIA Act protects the privacy of communications by making it an offence to intercept a communication passing over a telecommunications system without the knowledge of the maker of the communication, or to access a 'stored communication' without the knowledge of the sender or intended recipient of the communication.[14]

The TIA Act then provides a framework for the lawful interception of communications by telecommunication providers (carriers, and carriage service providers including Internet Service providers) in certain limited circumstances and by law enforcement and national security agencies if they have obtained a warrant. It also requires telecommunications providers to ensure that their services are 'interceptable' and to assist with interception in the context of an authorised warrant. The TIA Act also sets out stringent rules for the handling and use of intercepted material (content) and a range of oversight and accountability mechanisms (discussed below).

The TIA Act provides for separate warrant processes for:

- the Australian Security Intelligence Organisation (ASIO) where warrants are issued by the Attorney-General at the request of the Director-General of Security and
- Australian Government agencies other than ASIO, including the Australian Federal Police (AFP), State and Territory police forces and other bodies such as the Queensland Crime and Misconduct Commission where warrants are issued by a judge or a nominated member of the Administrative Appeals Tribunal (AAT)

The TIA Act also sets out a warrant process for access to stored communications; these are communications such as email or SMS that are not passing over a telecommunications system but are held by a carrier or carriage service provider and cannot be accessed without the assistance of a carrier or carriage service provider.

Warrants for access to stored communications are available to a much wider range of agencies; essentially all those responsible for administering a law imposing a pecuniary penalty or administration of a law relating to the protection of the public revenue. This includes the Australian Customs Service, the Australian Tax Office, and the Australian Securities and Investments Commission. However, stored communications warrants are only available to these agencies when investigating defined serious contraventions. This means that most of the agencies that are an enforcement agency cannot use the provisions, as their investigations do not meet the penalty thresholds. In 2010-2011 the only non-interception agencies that used this regime were Customs and the ACCC for a total of 12 warrants out of 298 issued warrants (in the previous reporting year ASIC made 10 applications).

The TIA Act also provides a framework for access to telecommunications, or 'non-content', data. As noted in section 2.4, this term is not defined in the Act but is information that telecommunications

[14] The information from this section has been drawn in part from ALRC Report 108

providers generate and hold about individuals in the course of providing services. It includes information or documents such as subscriber details, call charge records and call routing information. Telecommunications providers are permitted to disclose non-content data to ASIO or specified enforcement agencies where the disclosure has been authorised and they may also make 'voluntary' disclosures if satisfied on reasonable grounds.

The framework distinguishes historical non-content data, which was already in existence, and prospective non-content data, which come into existence during the period for which the authorisation is in force; the level of authorisation required for access to prospective data is higher than that required for historical data and also there are time limits on the authorisations and some additional criteria.

The framework sets out separate requirements for ASIO and enforcement agencies, which include: criminal law enforcement agencies (for example, the AFP and state and territory police), the CrimTrac Agency and any body whose functions include administering a law imposing a pecuniary penalty or relating to the protection of the public revenue. In summary these are as follows:

- the Director-General of ASIO can allow any officer or employee of ASIO to authorise access to historical data but in the case of prospective data, authorisation is limited to Senior Executive Service (SES) Band 2 or above - the authorisation commences at the time the person from whom the disclosure is sought receives notification of the authorisation, and must end within 90 days, unless revoked earlier

- an authorised officer of an enforcement agency can authorise a telecommunications provider to disclose historical data if he or she is satisfied that the disclosure is reasonably necessary for the enforcement of the criminal law, or a law imposing a pecuniary penalty or protection of the public revenue and

- an authorised officer of a 'criminal law-enforcement agency' can authorise the disclosure of prospective telecommunications data if satisfied that the disclosure is reasonably necessary for the investigation of a Commonwealth, state or territory offence that is punishable by imprisonment for at least three years and having regard to how much the privacy of any person or persons would be likely to be interfered with by the disclosure – the authorisation period is half that allowed for ASIO investigations—45 days.

4.2 SAFEGUARDS AND ACCOUNTABILITY

In addition to setting strict rules on the circumstances in which warrants can be obtained or non-content data accessed, the TIA Act sets out a range of accountability and safeguard measures, that as mentioned above, include independent decision-makers for warrant issuing, and record keeping and record destruction requirements, limits on use and disclosure of material, public reporting on certain matters and independent monitoring of compliance with the requirements of the Act. In addition, all the participants in the interception and non-content data access regime are subject to a range of legal requirements, including the Privacy Act for federal law enforcement agencies other than ASIO and telecommunications providers (unless exempt) and the *Telecommunications Act 1997* (TA) for telecommunications providers, and also to their own internal processes and accountability requirements.

Key aspects of the safeguards and accountability measures are noted below.

4.2.1 RECORD-KEEPING, DESTRUCTION OF CONTENT MATERIAL, ANNUAL REPORT AND PENALTIES

Law enforcement agencies are obliged to keep records relating to interception and stored communication warrants, and to provide the responsible Minister (currently the Attorney-General) with an annual report containing information about these warrants. The Minister is required to compile information received from law enforcement agencies into a report that must be tabled in Parliament. In addition, the TIA Act requires that records of intercepted or stored communications be destroyed in certain circumstances.[15]

The TIA Act makes it an offence to record, use or disclose intercepted information, stored communication information (in this report 'content'), or information about an interception or stored communication warrant, except in certain circumstances. For example, this type of information can be recorded, used or disclosed for the purpose of applying for a warrant or for investigating certain offences. Civil remedies also are available for unlawful interception of communications.

4.2.2 LAW ENFORCEMENT AGENCIES – LEGAL FRAMEWORK AND INTERNAL PROCESSES

As noted, in addition to the requirements of the TIA Act, telecommunications interception and access to non-content data takes place in the context of a range of other legal requirements and processes. In the course of preparing this PIA, IIS was briefed on the processes by ASIO and the AFP and was also given to the opportunity to observe non-confidential aspects of the management of interception processes.

IIS notes that State agencies can only exercise interception powers if they are declared by the Commonwealth Attorney General under section 34 of the TIA Act to be an agency. Once declared, all the requirements for obtaining an interception warrant apply. IIS understands that similar frameworks exist for these agencies utilising the provisions of the TIA Act according to the agency type and jurisdiction. There are some variations, for example, Western Australia and South Australia do not have a privacy laws and some of the other states and territories give full or partial exemptions in their privacy laws for law enforcement.

The briefings were very helpful in giving IIS a deeper understanding of the rigour of the processes surrounding interception and data access. While the details of the processes are confidential they include:

- detailed manuals and guidelines
- ensuring that access to intercepted material is available only to those who require it
- specialised staff to manage interception and compliance with TIA Act obligations
- a process of prioritising applications to fit within the resources available – not all warrant proposals proceed
- explicit consideration of issues relating to privacy

[15] The ALRC Report 108 mentioned previously raised some issues about data retention and destruction and called for published guidelines (Recommendations 73.90 and 73.104, 73.119)

- an internal chain of approval that includes a high level committee that makes the final decision
- stringent security safeguards and
- internal monitoring and audits.

4.2.3 ISSUING OF WARRANTS

The role of independent bodies in the issuing of warrants is an important plank in the TIA Act safeguards framework.

As noted, ASIO warrants are issued by the Attorney-General and other warrants are issued by an 'issuing authority' appointed by the Attorney-General and may include judges of courts exercising federal jurisdiction, a Federal Magistrate, or a magistrate. The Attorney-General also may appoint AAT members who are legal practitioners of at least 5 years standing.

The most recent report on the operation of the TIA Act notes that the number of eligible issuing authorities is as follows:[16]

- 12 federal court judges
- 12 family court judges
- 39 federal magistrates
- 46 nominated AAT members.

The report further notes that approximately 85% of telecommunications interception warrants were issued by AAT members and that the number of warrants issued by authorities is influenced by an agency's operational needs and the availability of an issuing authority at the time of application.

Both ASIO and other agency warrants must be documented and must be appropriately justified. In the case of ASIO the test is the proper use of its statutory powers. In the case of other agencies, with some variations for stored communications, the TIA Act provides that the issuing authority must consider:

- how much the privacy of any person or persons would be likely to be interfered with
- the gravity of the conduct constituting the offence or offences being investigated
- how much the information would be likely to assist in connection with the investigation by the agency of the offence or offences
- to what extent methods of investigating the offence or offences that do not involve so intercepting communications have been used by, or are available to, the agency

[16] Telecommunications (Interception and Access) Act 1979 Report for the year ending 30 June 2011 available at http://www.ag.gov.au/www/agd/rwpattach.nsf/VAP/(9A5D88DBA63D32A661E6369859739356)~Final+TIA+Act+Annual+Report+2010-11+-+amended+after+publication+-+v5+(3).pdf/$file/Final+TIA+Act+Annual+Report+2010-11+-+amended+after+publication+-+v5+(3).pdf

- how much the use of such methods would be likely to assist in connection with the investigation by the agency of the offence or offences and
- how much the use of such methods would be likely to prejudice the investigation by the agency of the offence or offences, whether because of delay or for any other reason.

4.2.4 Inspector General of intelligence and security

The Office of the Inspector-General of Intelligence and Security (IGIS) has been established under the *Inspector-General Of Intelligence And Security Act 1986* to assist government in the oversight of the activities of Australian intelligence and security agencies, including ASIO. The IGIS has broad inquiry and inspection powers in relation to ASIO activities, including ASIO's compliance with the law in respect of its collection and use of telecommunications data and intercept. The IGIS conducts inspections of ASIO's use of powers under the TIA Act, as well as more broadly under the ASIO Act, and includes information on the results of inspections in their annual report. The IGIS has substantial powers to conduct inquiries, obtain information and documents, and enter premises. ASIO works very closely with the IGIS, and will routinely report any administrative errors it makes to the IGIS.

4.2.5 Commonwealth Ombudsman

The Commonwealth Ombudsman (CO) is an independent statutory office established by the *Ombudsman Act 1976* (Cth). The Act provides that the Ombudsman is to investigate the administrative actions of Australian Government departments and prescribed authorities in response to complaints, or on the Ombudsman's own motion.

The CO inspects the interception records of Commonwealth bodies and the stored communications records of all enforcement bodies (including State and Territory agencies). Further, the CO has specific powers under the TIA Act to enter premises occupied by agencies, obtain relevant material, inspect records and prepare reports in relation to the interception of, or access to, communications.

The CO reports on record keeping and accountability and can report on other provisions within the TIA Act. Ombudsman recently described their approach as taking a 'broader view' of the role and, for example, that its audit criteria include checking that:

- warrants are compliant with the Act
- any warrant conditions imposed by issuing officers are adhered to
- lawfully accessed information was only communicated to authorised officers
- warrants are validly executed, and
- the use of stored communications product is in accordance with the Act.[17]

4.2.6 State Ombudsman and other oversight bodies

The TIA Act provides that before the Attorney-General 'declares' that a state/territory agency is permitted to use the warrant provisions there must be State/Territory legislation complementing

[17] Ombudsman submission to the Senate Inquiry on the Cybercrime Bill

the TIA Act that imposes parallel supervisory and accountability provisions (including those relating to inspection and reporting requirements) on the State/Territory agency. State Ombudsman or other bodies including, in Queensland, the Public Interest Monitor, perform these oversight functions.

As noted above, the CO inspects the interception records of Cth bodies and the stored communications records of all enforcement bodies (including state agencies).

4.2.7 Office of the Australian Information Commissioner

The Privacy Commissioner (now part of the OAIC) does not have a direct role in the TIA Act oversight framework. The Information Commissioner does have the 'privacy' function of monitoring compliance with Part 13, Division 5 of the TA, which deals with telecommunications providers obligations to make a record of disclosures of personal information, including those that are authorised under the TIA Act.[18] In particular, the function conferred on the Information Commissioner includes monitoring:

- whether a record sets out a statement of the grounds for a disclosure and
- whether that statement is covered by the TA or the TIA Act.

The Information Commissioner may also give the Minister a written report about any matters arising out of the performance of the function.

[18] s.309 TA

5 STAKEHOLDERS CONSULTATIONS

In this course of preparing this report, IIS met with three groups of stakeholders. These were:

- State and Federal law enforcement agencies, including State police and the AFP, and ASIO
- telecommunications organisation or service providers and
- senior members of the AAT.

The AFP and ASIO also gave IIS further briefings and information on telecommunications interception activities and processes, and the frameworks and procedures under which they operate.

To date, IIS has not met with representatives of privacy or community advocacy organisations to discuss this PIA.

IIS found the discussions very helpful in clarifying its understanding of the current TIA Act the stringent and rigorous framework within which it is administered.

The issues raised in the discussions largely canvassed in the discussion in this preliminary report. A summary of the key points raised follows.

5.1 STAKEHOLDERS CONSULTATIONS

IIS asked both agencies and telecommunications organisations to consider common issues as follows:

- current practices for assisting agencies and managing data
- data collection and handling trends and
- oversight and accountability.

5.1.1 AGENCIES

The points made by agencies included:

- public expectation – recognition that thresholds for use and access need to reflect privacy considerations and the benefit to the community in information covered by the Act being accessed and used.
- definitions and assumptions:
    - concept of ‘serious offence’ and 7 year threshold too limited,
    - ‘authorised officer’ concept not workable for some agencies;
    - offence range not relevant to integrity agencies.
    - consistency needed in interpretation and use across jurisdictions

- some issues in understanding what is permitted under the TIA Act, for example, it is not always clear when agencies can share interception information in the context of joint investigations
- how best to target interceptions given the density of information and possible need to develop specific tools
- TIA Act accountability and reporting requirements tend to focus on process rather than substance; too much focus on process rather than on meaningful checks
- more accountability needed on needed on industry about how they handle information and the role of industry needs to be clearer and more obligations assigned and
- the role of CO and State Ombudsmen and other oversight bodies need to be simplified.

5.1.2 Telecommunications Organisations

The points made by agencies included:

- that requests for assistance or data from agencies are not always clearly defined
- definitions of 'traffic data' (in this report non-content data) and 'stored communications' are needed to clarify what can be released
- traditional phone carriers are becoming less important than content service providers
- the importance of ensuring that the general public has confidence that organisations are providing assistance and information within a limited and rigorous framework
- an interest in having more information about how agencies deal with information provided by carriers
- increased data volumes and encryption use means a combination of interception and surveillance will be needed to identify targets
- that carriers don't need as much information for billing and business purposes so once legacy systems go that information will not be retained.
- consider currently accountability focuses too much on process; consider that an auditing approach more useful than current reporting requirements
- accountability focus should be on agencies rather than industry and
- accountability will be important for data retention as would need to keep information safer than current systems allow.

5.1.3 AAT

IIS explored a number of issues with a Deputy President and the Sydney Registrar of the AAT. Issues discussed included:

- the role of the AAT in supporting its members, given that individual members, rather than the AAT as such, are given the role of authorising officer (which provides for the approving of warrant applications)
- an overview of the warrant application process from the AAT member's perspective
- how privacy issues are raised in warrants and how the AAT member considers the issues
- nature of changes sought to warrants and
- the AAT's views on the possible introduction of a proportionality requirement and the involvement of a public interest monitor (PIM).

IIS's impression was that privacy is very much on the agenda as warrants are issued. The AAT members noted that clarification or further information is often sought in the process. They expressed interest in more transparency on this aspect of the process and also on more community education to build confidence in AAT members' role in the process.

IIS understands that at this point AAT members do not receive specific training or guidance on considering privacy or other matters relevant to their authorising role. It also understands that the AAT is considering developing material and processes to support its members in this regard.[19]

[19] IIS did not speak to other issuing authorities but to the extent that specific training and guidance is not available, it presumes this would be relevant to them as well. Its recommendations on these matters apply to all issuing authorities. It also notes a number of the ALRC's recommendations in its report 108 call for additional published information and guidance on the TIA Act and its operation (in particular example recommendations 73.78 and 73.119)

6 TIA ACT REFORM PROPOSALS – PRELIMINARY FINDINGS AND RECOMMENDATIONS

This section of the report sets out IIS's preliminary findings and recommendations in relation to AGD's current proposals for amendments to the TIA Act as set out in drafting instructions provided to IIS in October 2011. The findings and recommendations are primarily based on the proposals as set out in the drafting instructions, but also take into account other briefing material provided and meetings with agency and industry stakeholders.

The analysis has focussed on areas of significant change, and in particular on the key themes and proposals that IIS considers are most likely to have privacy impacts or raise privacy issues, rather than a line-by-line analysis of the drafting instructions. The preliminary findings and recommendations are also based on IIS's understanding at this point and may change following feedback and/or clarification from AGD or further stakeholder consultations.

The process of finding an appropriate balance for the exercise of intrusive powers while taking account of the community's interest in privacy is complex and raises difficult questions. IIS commends the approach taken so far in the AGD material and in the drafting instructions; privacy issues are squarely on the agenda and are being given careful consideration. IIS also acknowledges that the existing TIA Act, as well as the other laws, including the Privacy Act, provides a rigorous framework of accountability and oversight by independent bodies.

In considering the proposals, IIS has taken account of this framework and it has also considered the following matters.

Community expectations about a safe society, the use of intrusive powers and about privacy is clearly an important consideration but is also a complex area. There will be a range of views about what is expected or appropriate, including: those who think community safety and protection is paramount; those who feel in the digital age there can be no expectation of privacy; and those who value privacy strongly or who appreciate the need for intrusive powers but are concerned about how the powers are exercised. Ultimately, in Australia the community expects the Parliament to decide on the extent of intrusive powers and what safeguards are needed including for privacy. For the purposes of this analysis, IIS assessed the proposals against the balance currently set by the TIA Act and has also considered views expressed by the agencies participating in consultations and issues that have been raised in the past by privacy advocates and oversight bodies.

IIS has also considered the changing environment in which the telecommunications interception will take place. Of particular significance is the changing and exponentially expanding nature of the information that is collectable including:

- old types of data that has been useful may no longer even be created
- new types of data which are not necessarily accessible via carriage service providers and other traditional sources and
- very significantly, the emerging importance and richness of data.

In thinking about privacy specifically, IIS has focussed on the range of matters addressed in the Information Privacy Principles (IPPs) in the Privacy Act as well as broader privacy concerns.

Often privacy principles are described as giving individuals control, to the extent possible, over personal information about themselves. In the context of the TIA Act individuals have little control over their personal information – they will not have a choice, and in most cases will not be advised, about whether their communications are intercepted or data about them disclosed and generally they will not have the usual access and correction rights. In such an environment the privacy protection focus moves from individual control, via notice and the ability to exercise informed to consent, to a focus on others, government agencies in particular, keeping personal information under control. The most relevant privacy principles here are:

- collection limitation (IPP 1)
- transparency (IPP 2 and IPP 5)
- security (IPP 4)
- use and disclosure controls (IPPs 10 and 11). [20]

Finally, IIS also considered its 'layered defence' framework, particularly in relation to the law and to governance, and the Office of the Australian Information Commissioner's (OAIC's) '4As' framework.

Overall, IIS considers that a number of the changes proposed are positive from a privacy perspective. In particular, it welcomes the new objects clause. On the other hand, some of the proposals do seem to shift the balance to a greater privacy impact. In its recommendations IIS has suggested that more evidence or justification would be helpful in some cases and it has also made a range of other recommendations for options to mitigate possible privacy impacts.

6.1 OBJECTS CLAUSE INCLUDING PRIVACY

IIS understands that the intent of the TIA Act is to primarily to protect privacy of communications as well as to set the framework for lawful interception and access to related data. Moreover, while interception is undoubtedly a useful tool for national security and law enforcement purposes, it is accepted as a tool that is not to be commonly used and in fact is deliberately not made available widely but only to a limited group of government agencies and then only under certain conditions. The use of interception requires analysis in each case of whether it is the right investigative tool for the job and whether the thresholds and other requirements of the legislation have been met. In other words, interception is a particularly sensitive method of investigation to which rigorous safeguards and accountability measures should always apply.

IIS therefore welcomes the inclusion of an objects clause for the legislation. The drafting instructions ask that the legislation should provide:

- a right to privacy in making a communication

[20] The Government is currently developing amendments to the Privacy Act based on the recommendations in the ALRC's report on privacy. The IPPs (and the private sector National Privacy Principles) will be replaced with the Australian Privacy Principles; these will have strengthened transparency provisions calling for the development and provision of privacy policies.

- that covert access to communications is necessary in limited circumstances to protect national security and to enforce the law but
    - must be for a purpose of complying with or fulfilling a statutory function
    - in accordance with this Act
    - must be 'reasonable, or proportionate'
- range of use limitations and protections mentioned including to comply with oversight, accountability and reporting requirements.

IIS anticipates that these points would convey that the sense that interception is available in limited circumstances and that its use would not be permitted just because it would be useful. However, it is not convinced that the current objects clause by itself conveys the sensitivity of the tool. It suggests that the objects clause should convey clearly that telecommunications interception is intended to be "limited" as well as proportional and moreover that it is justified and accountable to independent authority

Preliminary Recommendation 1 – Objects clause

IIS recommends that in developing the proposals further, the AGD should ensure the objects clause conveys the clear message that the TIA Act is primarily aimed at protecting privacy of communications with interception occurring only in limited, justified and proportional circumstance. It therefore recommends that in addition to the current elements in the drafting instructions the objects clause include that interception should proceed only where it is limited and proportional, and is justified and accountable to an independent authority.

6.2 WARRANTS – ACCESSING CONTENT OF COMMUNICATIONS UNDER THE TIA ACT

The drafting instructions propose a range of significant changes to the warrant provisions of the TIA Act. Some of the proposed changes clearly strengthen the current regime from a privacy perspective. These include:

- the removal of the distinction between live and stored communications warrants – both are to be considered 'content' and subject to the same processes – this change is in recognition of factors such as:
    - stored communications becoming increasingly common
    - the volume of stored communications, particularly if the practice is not to delete the communications
    - that it is no longer realistic to assume that the content of stored communications is more 'considered' (which was in part the basis for the original distinction) and
    - the fact that if documents stored in the cloud are considered to be stored communications 'this will open up a much broader range of data that is stored on carriers' networks (drafting instructions paragraph 247)

- a new requirement for issuing authorities to have regard to whether the proposed interception is proportional taking account of factors such as the likely privacy impact, the seriousness of the matter and the likely effectiveness of the interception.

IIS welcomes the removal of the distinction in the warrant process for live and stored communications. This change is also likely to addresses concerns other stakeholders have raised about the operation of the TIA Act, for example:

- by the ALRC that a warrant for access to stored communication is not needed if a party to the communication has been notified, rather than all parties [21]
- reporting and accountability variations for live and stored communications and
- as noted in the drafting instructions, the extensive range of agencies that could seek a warrant for stored communications (the agencies able to seek a warrant for live communications is more limited than that currently able to make an application for a stored communications warrant).

Other changes that may be of concern to some stakeholders include the discussion of prohibitions and penalties, adding judges in state/territory courts as possible issuing authorities and providing more generic descriptions of the level of seniority for agency officers exercising functions under the TIA Act.

Changes that are likely to have a direct affect on privacy or which raise significant issues for consideration are discussed below.

6.2.1 Thresholds for obtaining a warrant

The threshold for warrants may affect the extent of interception that is permitted and undertaken (IPP 1 – collection limitation) and whether it is proportionate (the 'Analysis' point of the 4 As). The drafting instructions propose lowering the general penalty threshold for interception warrants from 7 years to 5 years. There would also be a power to make regulations for a lower threshold in a range of circumstances. The thresholds for ASIO warrants are noted for further instructions at a later point.

IIS considers that this change will need to be carefully explained and to be supported by detailed information about the impact of the change; it is likely to be perceived as a fairly significant lowering in privacy protection.

The rationale for the changes appears to hinge on the current complexity of the threshold provisions in the TIA Act and the need for a simpler approach that more accurately reflects the current scope of the threshold. The drafting instructions identify that the current 7 year threshold is not absolute and there are a range of offences that fall under 7 year threshold. These include where telecommunications services, for example computing related, are the means on commission of offence, where there is a linkage to more serious offence and because of the 'general view' that

[21] See ALRC Report 108 mentioned previously at http://www.alrc.gov.au/publications/73.%20Other%20Telecommunications%20Privacy%20Issues/telecommunications-interception-and-access-

certain offences, such as child exploitation warrant telecommunication interception regardless of the actual penalty. IIS notes that the law enforcement agencies attending the stakeholder consultation advocated a lowering of the threshold. IIS understands that AGD considers the 5-year threshold more neatly and accurately describes the range of offences currently triggering the ability to seek a warrant and that in any event it anticipates that resourcing and warrant issuing processes mean that the lower threshold would not automatically expand the extent of interception undertaken. However, IIS also understands that the 5-year threshold would introduce a significant range of new offences into the TIA regime.

IIS appreciates that there is a case for clarifying the application of the TIA Act thresholds and that there will be a need for a range of exceptions to the general threshold. IIS suggests that the exposure draft of the legislation should provide more detailed information about the current arrangements and difficulties and evidence about the impact of the change on the extent to interception that could occur, as well as is likely to occur.

6.2.2 WARRANT PROCESSES – DEFINING WARRANT SCOPE AND TARGETS

The drafting instructions propose a new way to describe the scope or target of a warrant. The proposal is to remove the current separate provisions for warrants targeting specific services, named persons and multiple services, or devices and replace this with a single approach based on the communications of interest, and person to whom communications relate; a warrant would specify 'identifying attributes', that isolate the targeted communication from a stream such as:

- the source of communication
- known service identifiers used by the person of interest (such as mail user addresses, phone numbers, service, device and Facebook IDs) or their computer terminal device identifier
- date and time of communications, based on 'pattern-of-life analysis and/or
- the destination and the type of communication. [22]

The rationale for the changes is partly to allow the warrant processes to respond to rapid changes in technology, and also to address the current complexity and level of bureaucracy in having a number of differing sets of warrant requirements. The drafting instructions note a further aim, which is to allow ASIO and the agencies to target warrants with greater flexibility and precision. IIS understands that attribute interception would also provide a means of focussing interception on the target and excluding all non-relevant intercepts at the point of network access rather than at the monitoring stage; a benefit from a privacy perspective.

The drafting instructions also note that the new provisions would have some restrictions on attributes. For example, it would not be permissible to target all emails that contain particular content, such as 'Wednesday' and 'destruction'. On the basis of the information in the drafting instructions it is hard to know if this limitation, which appear to be intended to avoid fishing expeditions, is sufficient and if it should be the only prima facie limitation.

[22] Existing warrant types would also be attributes

IIS considers that it will be difficult for interested parties (including community interest groups) to assess the impact of the proposed change overall; the concepts are fairly technical, there is no experience from current warrant processes to draw on and the possible attributes are open-ended. They may result in a more efficient process, which results in less non-material content but there also might be potential for the change to result in more interceptions in more circumstances.

While the IIS understands the intention is to modernise, rather than expand, the existing approach, it considers the changes have at least the potential to have an impact in terms of collection limitation (IPP 1) and the 4As 'Analysis' and 'Accountability limbs'.

The drafting instructions do note that the 'fluidity of the technology in the current environment means that it is hard to allocate a level of intrusiveness to a particular identifying attribute' (paragraph 252). The proposed solution here is a greater role for the issuing authority to consider the privacy implications of attributes at the application stage and to have the capacity to remove particular attributes from an application in order to promote a more proportionate exercise. There are also proposals to allow issuing authorities to ask agencies for more information on the privacy implications.

An issue to consider is whether the changes could mean that it is harder for issuing authorities to assess the privacy implications of a warrant and whether it is in the circumstances proportionate. IIS notes that the drafting instructions anticipate that it might be necessary for issuing authorities to have access to expert advice in making these assessments and suggests this would be available from agencies. IIS suggests that the process is likely to be seen to be more independent and rigorous if advice is available from an independent third party, for example, a PIM such as already operates in Queensland and is proposed in Victoria, or other independent expert advice. IIS suggests such a role would be needed at the federal as well as state/territory levels.

IIS understands that the attribute warrants would also replace B party warrants. As recognised in the Blunn report, B party warrants have potential to have a significant impact on privacy; it emphasised the need for privacy protections to accompany such provisions. When B party warrants were introduced, the notion was that prior to issuing a telecommunications service warrant for B-party intercepts, the issuing authority would need to be satisfied that the interception agency has exhausted all other practicable methods of identifying the telecommunications service used or likely to be used by the person of interest or that it would not possible to intercept the telecommunications used or likely to be used by the person of interest. As noted above, a possible benefit of attribute interception will be to reduce the collection of information about B parties at source. However, IIS considers that it will be important to make sure that warrants still make it clear to the issuing authorities either that the interception will involve B parties and that they need to give this aspect of a warrant particular consideration.

6.2.3 WARRANT PROCESSES – TESTS AND HOW APPLIED

The drafting instructions propose a new requirement for issuing authorities to be required to consider if a warrant application is proportional (taking account of the privacy impacts as well as other circumstances) and also includes provision for PIMs[23] where a jurisdiction has this role (paragraph 231 and 232).

IIS welcomes these proposals – they are consistent with the 4As framework – and it also expects that other stakeholders would be supportive; the Law Council and the CO have raised these issues in submissions.

The drafting instruction also propose that the criteria that a warrant application must address be defined more broadly as themes, including proportionality, rather than a list of requirements. If this proposal is developed further, IIS suggests caution is needed to ensure that sufficient information is available to allow issuing authorities to make appropriate assessments.

IIS suggests that this change, together with the move to attribute defined warrants, could affect the ability of issuing authorities to take privacy into account or could at least add to the perception in some quarters that issuing authorities simply 'rubber stamp' applications.

The drafting instructions note this perception and attribute it this to the fact that only a handful of applications are ever rejected. They challenge this by pointing to the number of occasions when issuing authorities seek amendments to warrant applications (currently this information is not included in the TIA Act annual report). IIS was also advised, in the stakeholder consultations, that the low number of rejections can be attributed to agency (and ASIO) rigorous internal processes, which ensure warrants are needed and that the application covers the matters required by the TIA Act. The AAT members consulted were also confident of the agency internal processes but reported that they nevertheless sought clarification or more information where necessary before issuing a warrant.

IIS understands that at present AAT members do not have specific training or information available to them to assist them in undertake responsibilities as issuing authorities. It also understands the AAT is considering what might be possible and appropriate support without compromising the individual members' responsibility.

It also notes that the ALRC identified that intelligence and law enforcement agencies, telecommunications service providers, regulators, oversight bodies, and the community should have a clear understanding about when communications may be intercepted and accessed, and how that information is subsequently handled; in short it seemed to be advocating a wide community education campaign as well as specific training and guidance.[24]

Overall, there seem to be questions of perceptions and trust here, in addition to the possible need for expert input. IIS suggests that there might need to be a combination of responses, which go in part to the need for community education about the issuing authority processes and to more transparent reporting, including about additional information sought or conditions imposed on a

[23]

[24] ALRC Report 108, Recommendation 73.119 and 73.120

warrant, as well as to options such as a PIM or other education or support strategies for issuing authorities.

6.2.4 INTERCEPTION UNDERTAKEN BY AGENCIES WITHOUT THIRD PARTY INVOLVEMENT

The drafting instructions propose a change from requiring the actual interception to be done by a third party to give more flexibility to allow agencies to exercise a warrant themselves, or on behalf of another agency, if the circumstances warrant this. The rationale here is primarily the range of new telecommunication bodies (service providers) that will have obligations under the amended TIA Act (discussed in section 6.6.1 below) and that may not have the technical capability to assist with interception or that may pose more risks from a security perspective.

IIS acknowledges that agency interception activities are subject to rigorous internal processes and to oversight by the CO or other ombudsmen or the IGIS as appropriate. However, there is at least the perceived risk of greater potential for unauthorised interception and for trust in the regime to be affected. IIS therefore welcomes the proposals in the drafting instructions for strengthened accountability in the warrant application process and in post interception monitoring and accountability measures.

6.2.5 ASSISTANCE WITH DECRYPTION

The drafting instruction provide a new obligation for service providers to provide assistance with decryption, and also provide for agencies to apply for and serve notices on relevant persons requiring them to provide assistance to decrypt information (however protected including passwords, compression, steganography). A notice is only available in the context of a warrant but in these circumstances could apply to non-content as well as content; if there is an authorisation for disclosure of non-content data service providers do have obligations to assist if they can. A notice can be served on anybody who might be able to assist by providing an intelligible version of the material sought or the encryption key; subjects of a notice only have to comply with a notice if they can. The agency has to justify request for key on grounds such as:

- the reliability of the person holding the information
- the need to protect content if the person with the key does not know it
- the key is evidentiary
- practicality.

Notices will need to be authorised by issuing authorities and will attract similar protections and record-keeping obligations to warrants.

IIS considers that this proposal needs to be considered in terms of proportionality. It is likely to be controversial and its use will need to be transparent, justified and accountable. There may also need to be limits on the use or retention of a key and on access to any extraneous material exposed by a key.

Preliminary Recommendation 2 – Warrant Processes for Access to Content and TIA Act Guidance, Training and Community education

IIS recommends that in developing the proposals further, the AGD should:

- ensure that where interception is permitted on the basis of knowledge or consent of a party to the communication, this should be on the basis of knowledge or consent of all parties to communication not just one or some
- retain the 7 year threshold for interception other than in specified circumstances where a lower threshold is already permitted
- if the threshold is lowered to 5 years, the exposure draft of the legislation must be accompanied by:
    - a clear justification that explains how this is consistent with the objects clause as proposed in IIS preliminary recommendation 1
    - and an estimate of the impact of the measures, in terms of the nature of crimes or offences brought in and an estimate of the number of warrants that would be issued compared with the current law
- build in transparency about the nature and implications of the possible attributes that could be used to define warrant targets (replacing the current concept of warrants based on specified services, devices or named persons), and appropriate limits, both in the drafting of the legislation and in consultations undertaken on the exposure draft including by:
    - developing a detailed description of the nature of possible attributes
    - developing criteria to assist issuing authorities to consider the privacy implications of attributes, for example
        - the extent of communications to be intercepted
        - the extent to which they may result in the capture of non-target communication including B parties
        - strength of association of the attributes to a suspect or suspects
        - prohibition on 'fishing expeditions' for example, as noted in the drafting instructions, where a word or string of words in communications is targeted and
    - providing that permitted attributes will be listed in regulations
- ensure that the issuing authorities have access to advice about the privacy implications of attributes from independent, expert third parties, as well as from the requesting agency, that might include:

  - the establishment of an appropriately resourced federal level public interest monitor and/or a panel of experts available to offer advice
  - the availability of training or educative material based on ongoing monitoring of, and research into the nature of attributes

- build in a requirement for detailed reporting on the nature of attributes used and the impact on nature of communications intercepted (similar to the current requirement to report on the number of services intercepted)
- ensure that any streamlining of the matters that an issuing authority must take into account, as well as the proposed new requirement for proportionality, retains the need to consider the conduct being investigated, the potential intrusion on privacy, and the likely usefulness of the material to be gathered
- as flagged in the drafting instructions, explore additional pre and post accountability measures for warrants which an agency exercises without third party involvement – these measures might include:
  - a requirement to include the proposal, and rationale, in the warrant application
  - criteria and expert advice available to issuing authorities to assist them to understand the implications of the applications
  - ensuring that the IGIS and the Ombudsman have a particular obligation to examine all aspects of the interception processes undertaken without third party and to report to the Attorney-General on any underlying issues or trends
  - interception undertaken without third party involvement to be specifically reported in the TIA Act annual report and
- as flagged in the drafting instructions, provide that decryption notices are authorised by issuing authorities and that additional justification is required where the agency seeks encryption keys as well as or instead of decrypted content and
- ensure that resources are available and responsibility is allocated for the development of information and guidance material about the TIA Act, for example as identified by the ALRC Report 108, and for the development and delivery of regular community education programs about the Act.

6.3 AUTHORISED ACCESS TO NON-CONTENT DATA

The TIA Act currently permits ASIO, specified law enforcement agencies, and a range of other enforcement agencies to authorise access to non-content data held by telecommunications service providers. These authorisations are classed as 'internal authorisations' as there is no independent third party involvement in the decision-making. Service providers are permitted to make disclosures on the basis of such authorisations. They must make a record of authorised disclosures and the

Information Commissioner has the power to check if proper records have been kept.[25] Service Providers may also 'voluntarily' provide information without a formal authorisation, provided they can do this in accordance with the *Telecommunications Act 1997* (TA).

The framework for access to non-content data is an issue from a privacy perspective because:

- individuals have no control over the disclosures and will at best be given only very general information about the circumstances in which they might occur; there is no specific notice of disclosures provided (IPPs 2 and 5)
- there is potential for information to be inaccurate, for wrong inferences to be drawn or for the information provided to ASIO or agencies to be used for additional or new purposes (IPPs 4, 8 and 10)
- the increasing volume and detail of non-content data (analysis, proportionality) – IIS has for some time been watching the global debate in the area of 'big data' generally and what this means including for privacy and privacy protection. Its apparent that the volumes of data collected combined with increasing analytical power mean that even historical data, by itself or combined with other information, can reveal a very detailed picture of the way a person lives their life. Even more revealing is 'moving' data, such as geo-location, communications or purchasing patterns as opposed to stable data such as name, date of birth or other subscriber detail. A telling example is the level of detail could be ascertained about a German politician's life, courtesy of cellphone and online data.[26] The trends in data collection and analysis and also the resulting issues for society are also well canvassed in a recent OECD Roundtable. [27]
- there are a fairly substantial number of authorisations – over 240 000 in 2011 for law enforcement purposes (but this was down 40 000 over the previous year), over 8000 for laws imposing a pecuniary penalty or for protection of the public revenue and over 4800 prospective authorisations that effectively allow real time monitoring of a persons activities (IPP 1 – Collection limitation, necessity for collection).

The drafting instructions recognise the power/potential intrusiveness of non-content data and proposes a number of changes to the TIA Act to address the issues, which include:

- providing for two categories of non-content data:
    - subscriber data – available to wide range of agencies
    - non content data, non-subscriber data (billing, location, numbers called etc but not to include the content of web pages) that will only available to specified law enforcement agencies

[25] S.309 TA
[26] The example is found in article available at http://www.zeit.de/datenschutz/malte-spitz-data-retention
[27] The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines http://www.oecd.org/document/22/0,3746,en_2649_34255_46565782_1_1_1_1,00.html

- a new requirement for agency 'authorisers' to consider if the authorisations are 'proportionate' taking account of privacy of people whose data is accessed and the volume and nature of the data being accessed – again consistent with the 4As framework.

Other measures are being considered including a possible new requirement for authorisations to be in a specified format. IIS welcomes these measures particularly as other changes propose less process including freeing up who within an agency can 'authorise' the release of non-content data. However, while the changes do give greater protection to non-content data, the question IIS considers is if the changes go far enough.

6.3.1 BASIS FOR ACCESS TO NON-CONTENT DATA

In addition to the proposed requirements for authoriser to consider proportionality, the drafting instructions also flag the need to reconsider the criteria/threshold for access to subscriber data. The current requirement is that the authoriser to attest that the disclosures are ' reasonably necessary' for the enforcement of the criminal law or other permitted laws.[28] There is a stronger test for prospective data, which effectively allows real time monitoring; matters being investigated or enforced must carry a minimum penalty of three years.

The TIA Act provides for the Communications Access Coordinator (CAC) (within AGD) to develop guidance for authorisers in consultation with OAIC and the Australian Communications and Media Authority (ACMA).[29] A Determination was issued in 2007, following consultation with the Privacy Commissioner.[30] While it generally focuses on the form of authorisations it is also intended to give guidance to agencies on aspects of the provisions including how the impact on privacy should be considered. The Determination draws attention to the 'balancing' approach that it states is implicit in the relevant TIA Act provisions and suggests that in ensuring they have appropriately considered privacy an authorising officer could consider the gravity of the offence and how much the disclosure will assist the investigation of the offence.

However, its not clear that this measure is providing sufficient reassurance; the ALRC, in its 2008 report on privacy, and the Australian Law Council, in its submission on the Cybercrime Bill, expressed reservations about how the test might be being applied and sought assurance that there was detailed and clear advice available to agency authorisers.[31]

In the drafting instructions so far there are proposals for extra rigour in the process but not a new criterion. IIS considers there is a case for significantly stronger test or criterion, and indeed that there is a case for a warrant or warrant like process for non-content data (other than subscriber data for which the current test may be appropriate). Factors that IIS considers support the case are:

- the minimum penalty for prospective data seems low given the potentially increasing intrusiveness of the activity in the current technological environment

[28] TIA Act s.177-180

[29] The Communications Access Coordinator is a statutory position created under the *Telecommunications (Interception and Access) Act 1979*. An officer of the Australian Government Attorney-General's Department, currently the First Assistant Secretary of the Security and Critical Infrastructure Division fills the role and TIA Act s.183(1)(f) provides for a determination.

[30] The authorised version is available from ComLaw at http://www.comlaw.gov.au/Details/F2007L04424/Download

[31] See for example, ALRC Report 108 Recommendations 73.35, 73.119, 73.120

- as discussed above, the generally increasing sensitivity of non-content data because of the increasing richness of this information and the increasing power to analyse and extract new information from the data
- the particular sensitivity of certain types of non-content data, for example, location data associated with mobile phones that have a surveillance like affect
- the possible introduction of provisions allowing agencies to re-use non-content data for intelligence purposes
- the possible introduction of blanket data retention requirements into the TIA Act
- the potential for authorisations for non-content data to amount to a fishing expedition – where data about a large number of people is obtained on the basis of some possible activity or characteristics
- while the European Council review of its Data Protection Directive concludes that data retention is valuable law enforcement tool and should continue, it is still considering options to tighten the regime
- the European Data Protection supervisor contemplates that access to data retained under the EU Data Retention Directive would be by way of warrant and not for general law enforcement purposes.

Preliminary Recommendation 3 – Authorised access to Non-content data

IIS recommends that in developing the proposals further, the AGD should:

- in recognition of the increasing volume and sensitivity of non-content data, provide that access to non-content data other than subscriber data (particularly prospective data but preferably all) is only available under a warrant
- if a warrant approach to access to non-content data, other than subscriber data, is not adopted, specify more sensitive classes of non-content data that would require independent authorisation – these might include:
    - prospective data
    - historical data about a number of people in order to counter any argument that such collection might be a 'fishing expedition' and
    - historical or prospective geo-location data
- if a warrant approach to access to all non-content, non-subscriber data is not adopted, consider including appropriate minimum penalty requirements as pre-requisite for all authorisations as well as requiring that the access is 'reasonably necessary' and proportional (as proposed in the drafting instructions)
- provide that agency internal authorisations are based on detailed documentation of the grounds for the decision, including the nature and extent of non-content data required, the

purpose of the access, for example whether it is needed to assist in targeting a warrant or for direct investigative purposes, and the likelihood that it will assist the purpose

- provide in the legislation for detailed guidelines on the factors that might affect the privacy and proportionality of an authorisations to assist authorising officers
- if access to non-content data is authorised internally, ensure that the CO (and the IGIS against the separate ASIO processes) is given specific responsibility to monitor and report on the decision making process, taking account of:
    - determinations made under s.183(1)(f)
    - liaison with the Privacy Commissioner about any findings or trends in relation to service providers compliance with their record keeping obligations
    - a systemic assessment of the impact of authorisations to identify any issues in process or accountability that should be addressed
- provide that the Attorney- General's annual report required under the TIA Act to include numbers of voluntary disclosures, that is those made without an authorisation (these were reported when the Australian Communications Authority and then ACMA had the reporting function).

6.4 Use, Disclosure and Destruction of content and accessed Non-Content Data

The drafting instructions propose a range of changes to the handling and destruction of content and accessed non-content data. The approach to these matters will have an impact on the extent to which personal information is considered to be 'under control' (IPPs 4, 10 and 11), and the transparency and accountability of the TIA Act regime (IPP 5 and the accountability arm of the 4As).

An underlying theme in these changes is removing unwarranted bureaucracy and in allowing more flexibility in the use or disclosure of data once it is collected. In some cases IIS considers these measures, if managed well, will be neutral from a privacy perspective.

For example, the drafting instructions address the agency record-keeping requirements, which are intended as an accountability measure. The drafting instructions propose removing prescriptive requirements and allowing an agency to keep records it thinks necessary to demonstrate it has complied with the law – a 'purposive approach' – but subject to possible regulations to set minimum requirements. The drafting instructions also provide that the CO can work with agencies to develop appropriate approaches and can comment on approaches and practices in their reports.

Other changes, although allowing greater use or disclosure of content and non content data, appear likely to be generally accepted, for example data would be able to be re-used in misconduct matters in more circumstances.

IIS considers that some of the proposals have the potential for a greater impact on privacy and therefore it suggests some modifications or additional mitigation. In particular, the drafting instructions propose rationalising the permitted uses and disclosures of intercepted information so

that it can be more freely used for the purpose for which it was obtained and also allowing non-content data to be used for any of the intercepting agencies' purposes, functions or investigations, including intelligence, and removing restrictions on the retention on non-content data.

6.4.1 USE OF NON-CONTENT DATA FOR INTELLIGENCE

The usual principle from a privacy perspective is to only use or disclose personal information for the purpose for which it was collected or related purposes unless an exception applies; the exceptions include where uses or disclosures are authorised by law. The drafting instructions propose to authorise the use and disclosure of non-content data for intelligence purposes. This is currently not permitted and IIS considers that permitting this use would be a significant change. The potential privacy risks include:

- the potential for agencies over time to hold extensive databases of information
- the potential for there to be data quality issues that lead to people being unnecessarily being investigated or getting extra attention, and
- as intelligence is generally not subject to court processes, limited ability for people to become aware of the information held or test the implications.

IIS queries if a wide mandate to use or disclose non-content data for intelligence purposes is consistent with the potential sensitivity of non-content data. It also notes a 1993 High Court case 'that held that information about an individual obtained by the corporate regulator through use of a statutory demand power could not be disclosed to another agency for another purpose, at least without giving the individual concerned an opportunity to argue against disclosure'. [32]

IIS also notes the 2005 Blunn report considered intelligence uses of non-content data.[33] It did conclude that the intelligence to be gathered from non-content data would be invaluable in detecting patterns of behaviour for example in relation to organised crime. However, it also saw a need to limit and control any intelligences uses. A suggestion was to prescribe the circumstances of use, for example in connection with certain classes of organisation or associations involving known suspects where it can be demonstrated that intelligence is likely to assist, and to make the provisions subject to warrant or other equivalent protections and to oversight.

6.4.2 DESTRUCTION OF CONTENT

IIS considers that the drafting instructions on the destruction of content are sensible, subject to proper implementation. It encourages AGD to consider the development of standards or guidance on what would constitute reasonable steps for destruction of content and data as soon is it can no longer be legitimately retained. The ALRC Report 108 Recommendations 73.90 and 73.104 also called for guidance in this area.

IIS queried earlier if the change to attribute interception might result in less transparency in the collection of material about non-suspect persons. The ALRC has also raised the issue of destruction

[32] JOHNS v. AUSTRALIAN SECURITIES COMMISSION AND OTHERS [1993] HCA 56; (1993) 178 CLR 408 F.C. 93/041 in N Waters *Government Surveillance in Australia* page 5

[33] A Blunn, Report of the Review of the Regulation of Access to Communications (2005) Australian Government Attorney-General's Department, paragraphs 9.5-9.7

of intercepted material, particularly in relation to stored communications and non-material content intercepted under B party warrants.[34].

Preliminary Recommendation 4 – Use, Disclosure and Destruction of Accessed Content and Non-Content Data

IIS recommends that in developing the proposals further, the AGD should:

- prohibit the re-use of non-content data acquired on the basis of authorisations for intelligence
- if use for intelligence purposes is permitted, in recognition of the increasing volume and sensitivity of non-content data, ensure that the draft legislation only permits retention, use and disclosure of data for intelligence in limited, specified circumstances such as proposed in the Blunn Report and also considering IIS' preliminary recommendation 3
- if agencies are permitted to retain non-content data for specified intelligence purposes, records should be kept on the nature of the data retained, when it is used or disclosed and when it is destroyed and the CO should have responsibility and powers to monitor and report on the extent of, and trends in, data retained for intelligence purposes
- if non-content data is retained for Intelligence purposes but is not admissible in court the legislation should provide that it should be not be used to make decisions that would significantly affect an individual without providing them a right of hearing or reply
- provide in the legislation for the development of standards or guidance on what would constitute reasonable steps for destruction of content and data as soon is it can no longer be legitimately retained.

6.5 ACCOUNTABILITY AND OVERSIGHT

As noted in the introduction to this section, individuals have little or no control over personal information about them that is collected and handled in the context of the TIA Act and therefore privacy protections should include a focus on transparency and accountability (the accountability and appraisal arms of the 4As). The earlier part of this report gives a brief overview of these measures in the TIA regime, which include:

- documented decisions
- rigorous internal agency processes, senior decision-making and monitoring
- warrants issued by independent bodies
- monitoring of record keeping and other compliance by the CO and the IGIS for agencies and ASIO respectively
- annual reporting on the operation of the regime and
- testing of processes via the courts (to extent brought into that process).

[34] ALRC Report 108 – Recommendation 73-1-3

The drafting instructions include measures that IIS considers will strengthen privacy protection. These include:

- some strengthening of oversight roles of the CO and State or Territory Ombudsmen, allowing the CO to consider and report on best practice not just compliance with the TIA Act
- refinement of TIA Act annual reports, including measures of effectiveness for non-content data
- the addition of a complaints function, for either the CO or the Privacy Commissioner to investigate complaints of illegal phone tapping by anybody other than ASIO or law enforcement agencies and
- a new requirement to consult people whose information is obtained in interceptions and may be aired in public hearings (which is currently not the case with anti-corruption type bodies).

Changes that are likely to have a direct affect on privacy or that raise significant issues for consideration are discussed below. Preliminary Recommendation 5 that follows this section also includes measures that are intended to mitigate reporting issues arising from discussion in other sections including in relation to industry obligations, encryption notices, interception by agencies without third party involvement, and the work of issuing authorities.

6.5.1 TIA Act Annual Reports

The TIA Act requires the Attorney-General to prepare an annual report setting out information about a range of matters including statistics on warrants issued for content, stored communications, and for authorisations for non-content data, and any matters raised by the CO. IIS considers the annual report requirement is an important privacy safeguard, providing some information about the operation of regime and supporting the accountability and appraisal aspects of the 4As framework.

The current report includes useful information. However its focus is somewhat narrow, reporting outcomes and processes in terms of statistics, and providing some information about costs. It includes information about recent policy and legislative changes but only limited commentary on the report subject matter, generally leaving interested parties to draw their own conclusions. In IIS' experience media coverage on the annual report does tend to focus on the overall numbers and the trends, which, particularly for authorisation for non-content data, involve fairly large numbers.[35] In this regard, the AAT members who briefed IIS on its members' role as issuing authorities suggested that the annual report could have more of an educational role, that is it could promote understanding of and trust in the regime – including how issuing authorities go about their business. IIS sees value in this proposal.

The drafting instructions notes a number of challenges in the current reporting requirements including:

[35] Interestingly, as far as IIS is aware, the fact that there were over 40 000 less authorisations by law enforcement agencies in 2010-11 did not attract media attention but the fact that NSW has significantly more warrant applications was noted see for example http://www.theregister.co.uk/2011/11/02/interception_report_attorney_general/

- complexity and inconsistency
- the actual utility of the requirements
- the best ways to measure effectiveness for warrants issued, particularly given the view that the current measures – convictions and prosecutions – are considered to possibly under report the effectiveness of warrants, and
- for authorisations for non-content data where there are currently no effectiveness measures.

Changes proposed in part focus on some streamlining of the report requirements in the interests of ease and efficiency of reporting but also propose the reporting of some additional information. In particular, they call for a consistent approach to reporting across warrants and non-content data access authorisations and consistency with the *Surveillance Devices Act 2004*. Other changes of note proposed include:

- removing requirement to report on the cost of interception
- less detailed reporting of type of offences – a more global approach would be adopted
- more reporting on outcomes of access to data and
- more reporting on when issuing bodies are seeking more information (to demonstrate they do not just rubber stamp).

IIS supports the direction of a number of these changes and makes some suggestions about approaches. On the other hand, removing the requirement to report on the cost of interception could mask some insights that have potential value, including to demonstrate that real effort is made by the agencies involved to comply effectively or even indicating where processes are inefficient or in need of streamlining. While it appreciates it is resource intensive to compile the figures, it is another area where there is media interest and it appears a useful, concrete perspective on the extent of interception.

6.5.2 MONITORING AND OVERSIGHT

As has been noted, the monitoring and oversight provisions in the TIA Act are very significant as they counterbalance the lack of individual control. The CO plays an important role in this regard. The drafting instructions identify a range of areas for clarifying and strengthening the CO's role. These are welcome and include:

- clarifying that the CO is able to monitor and report on best practice as well as compliance
- providing for greater consistency in Commonwealth/State inspections and allowing the Attorney-General to ask the CO to undertake inquiries including into State agencies and
- extending the CO powers to inspect prospective data and to monitor agency processes on the issuing of authorisations for non-content data.

IIS considers that the powers of the various oversight bodies, and the need for them to be able to exchange information and to work together if needed, are critical. It can also see an argument for

the one body – the CO – to be able to oversight both Federal and State and Territory agencies use of interception powers. However, it appreciates there are practical or even constitutional issues that would make this a difficult change to achieve. It does suggest a careful examination of the provisions to maximise the ability for cooperation.

IIS notes that the CO has identified an issue with respect to its lack of visibility of carriers' actions.[36] It saw this an issue particularly in regard to stored communications. This appears to be an issue that should be addressed. It also notes that the TA, at section 309, gives the Information Commissioner the function of inspecting carriers' and carriage service providers' records of disclosures made in response to authorisations under the TIA Act. It considers that it would be worth exploring, with the Information Commissioner and the CO, the value in this role being moved to the CO or for there to be specific liaison and reporting on any issues.

IIS does not have specific comments about the IGIS inspection role. As the ALRC notes, its inspection role is wider than that of other inspecting agencies and allows the IGIS 'of his own motion inquiring into any matter, inter alia, that relates to the compliance by ASIO with the laws of the Commonwealth'. IIS notes and supports the ALRC view that the power to obtain access to prospective non-content data has significant privacy implications and should be subject to stringent control and oversight and its recommendation that the IGIS should incorporate into his or her regular inspection program oversight of the use of powers to obtain prospective telecommunications data by ASIO.[37]

6.5.3 Notifications to the Attorney-General and other matters

The drafting instruction propose the removal of a number of current obligations on the AGD, in some cases reallocating the role to a more appropriate body, including:

- requirement to notify warrants, revocations and enabling notices to AGD
- carrier notification of actions taken to enable interception
- effectiveness reporting (but this to be included in Annual Report instead) and
- reporting emergency related interceptions (expand CO role instead) and
- maintaining a warrant register.

The rationale for these changes in broad terms is that they appear not to add anything of substance to the accountability framework or that AGD is not best placed to carry out the role. At this point IIS is inclined to accept this view and so does not have any recommendations in this regard. It does note that the changes could be considered to remove some of the existing accountability framework and so will need to be clearly explained in the exposure draft material.

[36] Commonwealth Ombudsman Submission to the Senate Inquiry into the Cybercrime Bill
[37] ALRC Report 108 For Your Information: Australian Privacy Law and Practice, paragraph 73.127

Preliminary Recommendation 5 – Reporting, Accountability and Oversight

IIS recommends that in developing the proposals further, the AGD should:

- ensure that reports on the operation of the TIA Act include sufficient information to allow the Parliament, interest groups and the community to understand and assess the impact of the TIA Act, in particular the reports should:
    - include information about the 'shape' of the industry, including:
        - estimates of industry parameters as a whole such as number of fixed line calls, mobile calls, VOIP calls, SMS messages, emails and instant messages that are exchanged in Australia annually
        - the number of participants in social networking activities and
        - indicators of the average levels of activity and the types and numbers of service providers that have been requested to provide assistance to agencies,

      so that the number interceptions can be considered as proportion of all call as well as in absolute terms, giving a clearer indication of the growth or otherwise in interceptions and authorised disclosures
    - retain information about the cost of interception
    - ensure that any changes to the reporting of outcomes on interception allows understanding of the attributes used to target warrants and does not otherwise reduce the transparency and accountability of reports, particularly in relation to the extent to which interceptions capture information about innocent third parties (B parties)
    - provide more detail on access to non-content data on matters such as the purpose for access, the nature of the data accessed, how many people are affected by a request and the outcomes
    - use measures, in addition to numbers of accesses, to give an indication of the extent to which accesses may be increasing or decreasing as a percentage of overall communications
    - provide information about the use of encryption notices
    - provide details about interception without third party involvement
    - report on the role of issuing authorities, including for example the number of warrants where attributes are withdrawn and the extent to which external advice on privacy implication of attributes, or how to assess proportionality was sought and was available and any difficulties identified

  - provide for the Attorney-General to report on resourcing for monitoring functions and the extent to which concerns are expressed by the CO or other stakeholders or commentators and
  - to the extent that the changes aim for consistency with reporting under Surveillance Devices Act 2004 changes do not reduce current level of TIA Act transparency

- ensure that, as is proposed in the drafting instructions, the CO's monitoring role is defined broadly covering compliance with the law, how the system is operating overall, and any emerging issues with an impact on privacy
- provide for the IGIS to have a specific responsibility to incorporate into his or her regular inspection program oversight of the use of powers to obtain prospective telecommunications data by ASIO
- require that the CO's reports are made public to the extent possible, allowing for the excision of sensitive material
- ensure that permitted data exchanges between State Ombudsman and the CO are sufficient to allow cooperation for joint investigation or multi- jurisdiction investigations
- provide for regular surveys or research on issuing authorities and how competent they feel to make decisions on impact on privacy, proportionality and a requirement for the Attorney-General to respond to any issues identified and
- consider the resources required to ensure that the TIA Act oversight, accountability and complaint handling functions are effective and make this known to decision-makers.

6.6 INDUSTRY OBLIGATIONS

The drafting instructions make a number of proposals that respond to changes in the telecommunications industry and to telecommunications technology and that aim to ensure the industry will continue to have appropriate obligations to support interception activities. The proposals include:

- broadening beyond carriers and carriage service providers the types of organisations that will have obligations to assist agencies, possibly extending to cloud providers and social networking sites – there will be a new term 'service providers' to cover the whole group of providers, with organisation other than carriers and carriage service providers to be called 'ancillary service providers'
- the intention to capture international providers and communications as far as possible, possible modelling the SPAM Act and Privacy Act approaches
- a three tiered approach to industry obligations so that:
  - lower tier organisations will be required to provide reasonably necessary assistance

  - middle tier organisations will also be required to provide interception capability if nominated in a determination by the CAC and
  - top tier organisations will be required to have a comprehensive interception capability if the CAC determines and the Minister can also regulate for technical requirements

- various changes to definitions and specifications for the concept of a telecommunications service and what is meant by interception
- new obligations for service providers to deal with sensitive law enforcement and national security material in a secure way and for the Minister to have the power to make regulations specifying security standards and
- new obligations to provide an intelligible version of a protected communication or the decryption key where the service provider has legal possession or the means to do so.

IIS considers that these proposals will have possible privacy impacts in three key areas. Given that there will be more types of service providers there may be an impact in terms of collection limitation (IPP 1) (addressed earlier in this report and so the issues are not canvassed again here). There might also be direct impacts on transparency (IPPs 2 and 5) and security (IPP 4).

6.6.1 RANGE OF SERVICE PROVIDERS WITH OBLIGATIONS TO ASSIST AND TRANSPARENCY

The drafting instructions identify a significant range of service providers that might be considered 'ancillary service providers' – including providers of services such as:

- SMS
- VOIP
- Social Networking
- encryption
- tele-hosting content service providers who provide data centre accommodation, equipment rack space, server and storage infrastructure, interconnect facilities etc to other industry participants
- plus others if so 'determined' by the Attorney-General.

The questions from a privacy perspective include:

- whether, given the small business operator provisions in the Privacy Act, all these service providers would be subject to the Privacy Act
- will people be sufficiently aware of industry obligations, for example, that a warrant might be served on non-traditional telecommunications service or that non-content data held in the cloud could be provided to law enforcement, or other, agencies or ASIO
- the likelihood of access being provided to non-communications information stored by third party

- whether the monitoring bodies have sufficient resources available to monitor record-keeping and reporting obligations and
- if Australian accountability mechanisms could apply effectively to overseas based services.

6.6.2 SECURITY OF INFORMATION AND DATA BREACH RISKS

IIS considers that the inclusion of a wider range of organisations, with less regular contact with the interception and access regime, increases the risk that some organisations will not understand or manage the interception/authorisation process properly or may not protect information properly, exposing it to loss, unauthorised access or disclosure and leading to risks to individual's information or reputation.

In part in response to this concern, the drafting instructions do provide for more specific obligations on organisations to protect interception processes and data. However, IIS understands this is from the perspective of risks to law enforcement or national security.

IIS considers that specific consideration is also needed of the risks to individuals and the provisions and processes that could be put in place to manage those risks. These processes might include specific legislative obligations to protect individuals' information, some monitoring of security measures by an appropriate regulator and specific actions in the context of any data security breaches, for example, where information held by a service provider is lost, hacked or otherwise inappropriately disclosed. The OAIC guide on handling data security breaches canvasses the possible approaches to security breach notification.[38] While there is currently no specific obligation to this effect in the Privacy Act, the ALRC report 108 recommended data breach notification in certain circumstances.[39] IIS appreciates that data breach notifications in the context of interception or authorised access would be sensitive; an option could be proxy notification to an appropriate regulator who could then determine if actions were needed to protect individuals.

6.6.3 AGENCY/INDUSTRY COST SHARING

The current regime divides the costs of telecommunications interception between industry (fixed cost of capability) and agencies (variable cost of delivery of intercepted material to agencies). While approaches to costs and cost sharing do not raise direct privacy issues IIS considers that is important that the approach is consistent with and supports the privacy protective aspects of the regime; for example, aligning costs attribution with extent of use would reinforce the exceptional nature of the regime.

[38] Guide to handling personal information security breaches (August 2008) available at http://www.privacy.gov.au/materials/types/guidelines/view/6478

[39] ALRC Report 108, Chapter 51 available at http://www.alrc.gov.au/publications/For%20Your%20Information%3A%20Australian%20Privacy%20Law%20and%20Practice%20(ALRC%20Report%20108)%20/51-data-br

Preliminary Recommendation 6 – Industry Obligations

IIS recommends that in developing the proposals further, the AGD should ensure that:

- all organisations that will have obligations under the TIA Act should be subject to the Privacy Act, whether or not the organisation might otherwise by exempt from the Privacy Act because of the small business operator provisions
- there will be transparency about the role of the industry in assisting with interceptions and in providing access to non-content data – measures might include:
    - providing regular public information about industry obligations and
    - requiring industry service providers to advise their customers, in general terms, about their obligations under the TIA Act, and in particular obligations to provide decrypted documents or encryption keys
- in addition to TIA Act provisions relating to the security of the interception process that the legislation address the security of information about individuals who have been subject to interception or data access and provide for data breach obligations on service providers, whether directly to individuals or to a regulator on their behalf
- the approach to cost sharing between agencies and the industry operates as a signal that interception is an exceptional rather than routine investigative tool.

6.7 Non-content Data Retention

The drafting instructions include proposals to require telecommunications service providers to retain some non-content data for specified periods. IIS understands this section of the drafting instructions is not the final position and will not be revised. Currently the instructions suggest that much of the detail of the non-content data retention regime will be set by a determination by the Attorney-General. The instructions provide that:

- there will be a data retention requirement with a minimum data retention of 2 years (but IIS queries if the intention here was for an outer limit of 2 years)
- the Attorney-General will have a power to make a determination on data retention that must take into account privacy as well as interests of national security and law enforcement and will specify the types of data affected and data retention periods and
- service providers will bear costs but can recover marginal cost when providing data to agencies.

Data retention is likely to be considered sensitive from a privacy perspective for the following reasons:

- it involves holding information about much of the population, that was collected for the purpose of providing telecommunication services, for a new unrelated purpose (IPPs 1 and 10)

- while data is retained there is risk of further new uses, either by law enforcement agencies or others, that people may not expect or of security breaches (IPPs 4 and 10) and
- it affects the whole population, not just those who are breaking the law, and so interested parties will be looking for evidence that the requirement is justified and proportionate (the analysis arm of the 4As framework).

IIS appreciates that data held by the telecommunications sector has historically been available for law enforcement purposes and is considered a vital and useful source of information and that this data is becoming less available as telecommunications industry practices change. IIS also appreciates that the EU has operated a data retention regime since 2006. As noted earlier in this report, the EC recently conducted a review of the data retention directive and decided it would continue with the policy, although with some finetuning, on the grounds of its important contribution to law enforcement. There clearly will be legitimate law enforcement interests to consider as the proposals develop.

However, IIS also considers that there are some factors that are likely to add to the sensitivity of the proposals. Firstly, as discussed elsewhere in this report, and in the drafting instructions (in the context of proposals to limit authorised access to non-content, non-subscriber data), access to non-content data is becoming more sensitive as the extent and nature of the data held expands and the power to analyse and draw inferences from personal information increases. Requiring service providers to hold non-content data for long periods will add to the pool of data available (to the service provider as well as other agencies) and hence the sensitivity. Secondly, elsewhere the drafting instructions also propose to permit law enforcement agencies to use accessed non-content data more freely including for intelligence and with less restrictions on data retention. While this use will happen within a rigorous framework, there is nevertheless the potential, real or perceived, for data retention requirements to provide a pool of population information for surveillance type activities.

In developing the proposals further, and explaining them in the exposure draft material, IIS suggests that consideration or evidence will be important in the following areas:

- whether to include the data retention proposals in primary legislation or to provide for regulations – given the likely sensitivity of the proposals, IIS suggests the former
- options for storing retained data, particularly if there is any proposal, as canvassed in background material provided to IIS, for it to be held centrally
- whether telecommunications providers should be subject to additional security requirements, or limits on re-use where data is only retained for law enforcement purposes to reflect the increasing value of the personal information, and its richness over time

- the ways in which the value of retained data for law enforcement purposes can be demonstrated – while anecdotal evidence will be useful, statistical information is likely to be more telling (and noting that there will be some counter evidence in this regard) [40]

- whether, taking account of factors already canvassed on the sensitivity of collections of personal information, access to retained data, or data retained for more than a short period, should be subject to prior approval by an independent third party

- the period for retention and if the retention period of two years goes beyond what is necessary (noting that the EU Data Protection Supervisor commenting of the EC review of the data retention directive noted that statistical information from a number of Member States shows that over 80% of access requests relate to data up to six months)[41]

- the nature of the data items to be retained – the EC review has this issue under consideration, it felt that not all data items so far required may be needed in the future and submissions to its review (for example from the EU's Article 29 Working Party) suggest the need to define data items carefully to avoid confusion or which the retention of information which has content such as URLs of websites or headers of emails.

Preliminary Recommendation 7 – Non-Content Data Retention

IIS recommends that in developing the proposals further, the AGD should:

- to the extent possible, include provisions relating to non-content data retention in the primary legislation rather than in regulation

- support the exposure draft of the legislation with detailed and concrete evidence on the issues and problems the proposals address

- apply the provisions only to non-content data that service providers would otherwise collect for their particular business model – in other words there should be no requirement to collect/generate data if it is not required for business needs

- limit the non-content data retention requirement to a short period (6 months) unless there is strong evidence relevant to Australia of the utility of a longer period

- require the prior approval of an independent body for access requests for older non-content data or for particularly sensitive data such as geo-location data

- provide that the obligation to retain non-content data is subject to prior notice to individuals that this will occur

[40] For example, a report from Germany's Bundestag Working Group on data retention said that the [data retention] law is disproportionate in fighting crime as data retention increases the crime clearance rate only slightly http://www.pcworld.com/businesscenter/article/240649/civil_liberties_groups_slam_eu_data_retention_as_unnecessary.html#tk.mod_rel

[41] Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) May 2011 available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf

- include measures to protect retained information from misuse, loss or other unauthorised (or new) uses such as security requirements and data breach notification (as proposed in preliminary recommendation 6
- subject to consultation on the exposure draft, prohibit the central storage of retained non-content data on the grounds that the 'honey pot' effect is likely to outweigh other concerns
- clearly define the nature of the non-content data that can or cannot be retained, for example does this include location data or the content of web pages.

7 APPENDIX 1 –TELECOMMUNICATIONS INTERCEPTION LAW REVIEWS

The Barrett Review

In 1994 Mr Pat Barrett (then a Deputy Secretary in the Department of Finance and Administration and later Commonwealth Auditor-General) conducted a review into the long term cost effectiveness of telecommunications interception. The Barrett Review formed the basis of new telecommunications funding arrangements, which were introduced in 1995 and replaced by new arrangements in 1997. Mr Barrett also recommended a further review of telecommunications interception after deregulation of the telecommunications market in 1997.

The Boucher Review

In 1999, Mr Dale Boucher, an Associate Member of the Australian Communications Authority (ACA), as it then was, and a former Australian Government Solicitor, conducted the further review foreshadowed in the Barrett Review. The review was carried out by the ACA pursuant to section 332R of the Telecommunications Act 1997.

The Boucher Review made a number of recommendations relating to the longer-term cost-effectiveness of telecommunications interception arrangements. The Review stressed the importance of ensuring that interception must be available for all telecommunications services on the basis that the telecommunications carriers and the carriage service providers provide and fund the capability and that intercepting agencies must reimburse those costs on a 'user pays' basis.

The Ford Review

In 1999, Mr Peter Ford, a First Assistant Secretary of the Attorney General's Department, made a number of recommendations that formed the basis of the 2000 amendments to the *Telecommunications (Interception) Act 1979*. The most significant of these amendments was the creation of a named person warrant regime, which permitted the issuing of a warrant that authorised the interception of multiple services used by the person of interest.

The Sherman Review

In 2003, Mr Tom Sherman AO, President of the ACT Legal Aid Commission, conducted a review following a recommendation of the Senate Legal and Constitutional Legislation Committee in its report on the provisions of the *Telecommunications (Interception) Legislation Amendment Bill 2000*. This Bill had implemented many of Mr Ford's recommendations, particularly those including the creation of a named person regime. The Senate Committee recommended that a review be conducted on the operation of the named person regime within three years. It was the general conclusion of the review that the named person warrant regime should continue and that the regulatory regime generally contains adequate safeguards and reporting mechanisms. In particular, the review found that the interception regime has a strong compliance culture, which is well audited by the inspecting authorities.

The Blunn Review

In 2005, Mr Anthony Blunn AO, a former Secretary of the Attorney-General's Department, conducted a review on issue of access stored communications, following an amendment that had been passed in late 2004.

The review found that the interception regime had proved remarkably robust in an era of revolutionary technological change. However, it recommended a series of amendments to ensure the ongoing effectiveness of the regime. In particular, these recommendations included:

1. the development of overarching legislation concerning enforcement and national security access to telecommunications data,
2. the maintenance of the distinction between interception and accessing communications that are stored,
3. permitting interception based on the person with whom the target is likely to communicate, permitting interception based on equipment used to intercept, and
4. the development of binding Australian standards for interception in the absence of applicable international standards.

8 APPENDIX 2 – LIST OF MATERIAL REVIEWED

The material IIS reviewed are listed below. It also drew on additional confidential briefing material from the Attorney-General's Department and stakeholder agencies.

Materials Reviewed for the Preliminary PIA
A Blunn, Report of the Review of the Regulation of Access to Communications (2005) Australian Government Attorney-General's Department
Attorney-General's Guidelines in relation to the performance by the Australian Security Intelligence Organisation of its function of obtaining, correlating, evaluating, and communicating intelligence relevant to security (including politically motivated violence) http://www.asio.gov.au/img/files/AttorneyGeneralsGuidelines.pdf
Attorney-General's Department - Public consultation document - Australia's proposed accession to the Council of Europe Convention on Cybercrime (March 2011)
Attorney-General's Department - Public consultation document Outline of the articles of the Council of Europe Convention on Cybercrime and Australia's compliance This outline accompanies the public consultation document titled: "Australia's proposed accession to the Council of Europe Convention on Cybercrime" (March 2011)
Australian Law Reform Commission Report 108 For Your Information: Australian Privacy Law and Practice ALRC 2006
Commission Of The European Communities - Brussels, 21.9.2005 COM (2005) 438 final 2005/0182 (COD) Proposal for a Directive of the European Parliament and of the Council on the retention of data processed in connection with the provision of public electronic communication services and amending Directive 2002/58/EC (presented by the Commission) {SEC (2005) 1131}
EU Press MEMO/05/328 Release Data Retention - Brussels, 21 September 2005
EU Press Release P/11/484 - Brussels, 18 April 2011 Commission evaluates the Directive on retention of telecommunications data
European Commission - Brussels, 18.4.2011 Com (2011) 225 Final Report From The Commission To The Council And The European Parliament Evaluation - Report On The Data Retention Directive (Directive 2006/24/EC)
House of Commons Home Affairs Committee Unauthorised tapping into or hacking of mobile communications Thirteenth Report of Session 2010–12 http://www.parliament.uk/documents/commons-committees/home-affairs/unauthorised_tapping_or_hacking_mobile_communications_report.pdf
House of Commons Research Paper 00/25 - 3 March 2000 - The Regulation of Investigatory Powers Bill 64 of 1999-2000
Nigel Waters Government Surveillance in Australia 2006 http://www.pacificprivacy.com.au/Government%20Surveillance%20in%20Australia%20v6.pdf
Opinion of the European Data Protection Supervisor on the Evaluation report from the Commission

Materials Reviewed for the Preliminary PIA
to the Council and the European Parliament on the Data Retention Directive (Directive 2006/24/EC) May 2011 available at http://www.edps.europa.eu/EDPSWEB/webdav/site/mySite/shared/Documents/Consultation/Opinions/2011/11-05-30_Evaluation_Report_DRD_EN.pdf
Privacy fact sheet 3 - 4A framework – A tool for assessing and implementing new law enforcement and national security powers July 2011 http://www.oaic.gov.au/publications/privacy_fact_sheets/Privacy-fact-sheet3_4Aframework.pdf
Telecommunications (Interception and Access) Act 1979 - Annual Report for the year ending 30 June 2011
The Economics of Personal Data and Privacy: 30 Years after the OECD Privacy Guidelines http://www.oecd.org/document/22/0,3746,en_2649_34255_46565782_1_1_1_1,00.html#Agenda__Biographies_and_Presentations
The Parliament of The Commonwealth of Australia, House Of Representatives, Cybercrime Legislation Amendment Bill 2011, Explanatory Memorandum, (Circulated by authority of the Attorney-General, the Honourable Robert McClelland MP)
The Senate Environment and Communications References Committee The adequacy of protections for the privacy of Australians online April 2011 Senate Printing Unit, Parliament House, Canberra (download 26 July from http://www.aph.gov.au/senate/committee/ec_ctte/online_privacy/report/report.pdf)
Thirteenth Annual Report Of The Public Interest Monitor, Delivered Pursuant to the Police Powers And Responsibilities Act 2000, and the Crime And Misconduct Act 2001, Reporting Period 1 July 2009 - 30 June 2010 http://www.parliament.qld.gov.au/Documents/TableOffice/TabledPapers/2010/5310T3566.pdf
Tom Sherman AO Report of review of named person warrants and other matters - June 2003 Telecommunications (Interception) Act 1979
Victorian Ombudsman Investigation into the Office of Police Integrity's handling of a complaint October 2011 http://www.ombudsman.vic.gov.au/www/html/285-parliamentary-reports-2011.asp