Submission No 183

Inquiry into potential reforms of National Security Legislation

Name: Timothy Pilgrim
Privacy Commissioner

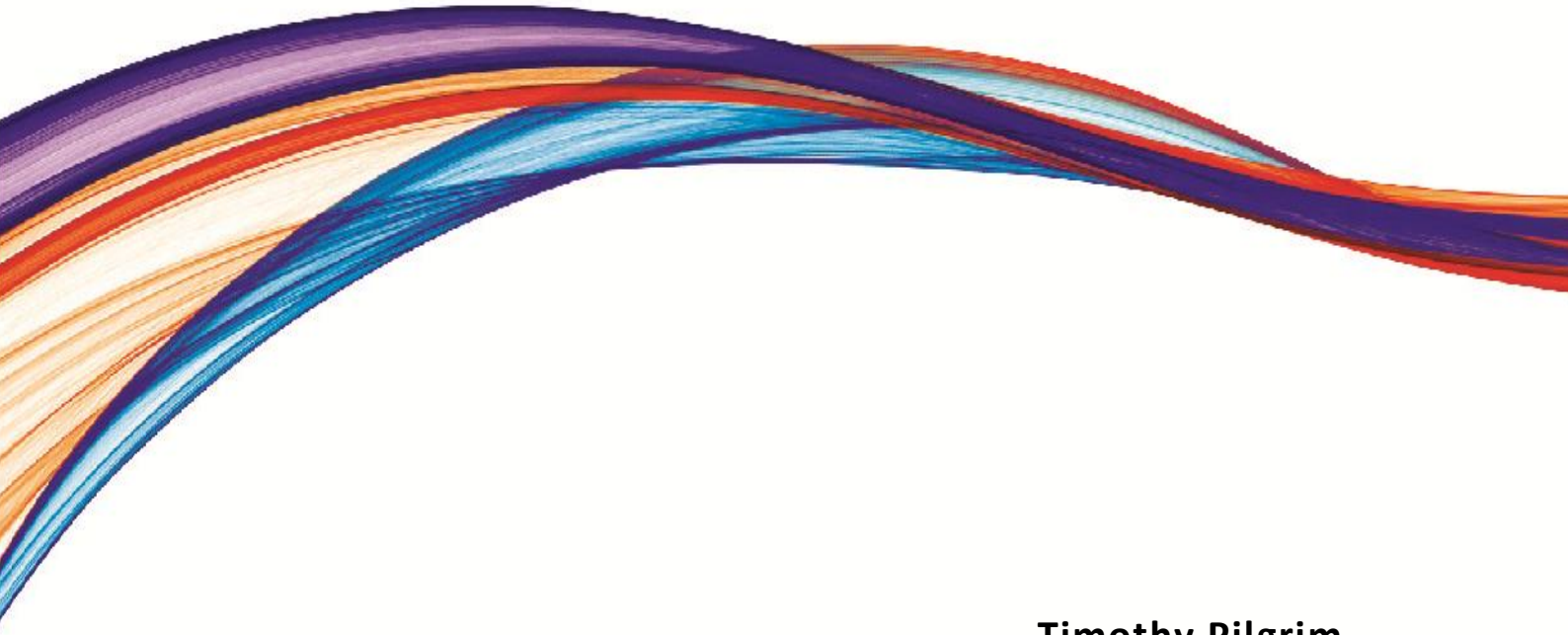
Organisation: Office of Australian Information Commissioner

Australian Government
Office of the Australian Information Commissioner

Inquiry into potential reforms of National Security Legislation

Submission to the Parliamentary Joint Committee on Intelligence and Security

27 August 2012



Timothy Pilgrim

Privacy Commissioner

Contents

Executive summary

i. The Office of the Australian Information Commissioner (OAIC) thanks the Joint Parliamentary Committee on Intelligence and Security (the Committee) for the opportunity to comment on the Inquiry into Potential Reforms of National Security Legislation (the Inquiry).

ii. The OAIC welcomes the focus of the Inquiry on ensuring that the proposals it canvasses contain appropriate safeguards for protecting the human rights and privacy of individuals. The OAIC is also supportive of the Committee giving consideration to ensuring proposals are proportionate responses to any threat to national security, critical infrastructure and law enforcement more generally.[1]

iii. The OAIC believes this Inquiry presents an opportunity to ensure that the privacy interests of Australians receive an appropriate level of protection in the context of the Australian national security framework. The OAIC has considered the proposals in the context of the following key privacy objectives:

- *Reduction of regulatory fragmentation* – The current fragmented approach to regulating the personal information handling practices of law enforcement and intelligence agencies can lead to inconsistencies in the level of privacy protection afforded to personal information and reduced transparency of information handling practices. The OAIC considers that greater consistency across the accountability framework for law enforcement and intelligence agencies could be achieved by ensuring that the different regulatory frameworks are underpinned by a common set of considerations that reflect Australian community expectations about how personal information is handled. In addition, clearly identifying the regulator that is responsible for the oversight of each agency would serve to bolster the public's confidence that effective accountability measures are in place.
- *Proportionality* – Where proposals would expand the existing powers of law enforcement and intelligence agencies in a way that may intrude further upon the privacy interests of Australians, the OAIC considers it is important to ensure the proposed measure is in proportion to the risk it seeks to address and, on balance, is in the public interest.
- *Community expectations* – The OAIC considers it important to ensure that proposals canvassed in the *Discussion Paper – Equipping Australia Against Emerging and Evolving Threats* (Discussion Paper), including those that are intended to strengthen existing safeguards and privacy protections, are in line with contemporary community expectations. The OAIC considers that the *Privacy Act 1988* (C'th)(Privacy Act), as the privacy oversight instrument the public is most familiar with, reflects existing community expectations. Accordingly, incorporating the core principles and values that underpin the

[1] See Attorney-General's Department 2012, *Discussion Paper – Equipping Australia Against Emerging and Evolving Threats* (Discussion Paper), Term of Reference 3(a), p 6.

Privacy Act into the other privacy accountability frameworks will help ensure that they remain consistent with community values and expectations.[2]

Key points

A. Proposed amendments to the communications interception regime

General comments

iv. The OAIC supports the proposal to introduce a privacy focused objects clause in the *Telecommunications Act 1997* (Telecommunications Act) and the *Telecommunications (Interception and Access) Act 1979* (TIA Act) (see paragraphs 12 - 14).

v. The OAIC would support a review of the current safeguards and privacy protections with a view to ensuring that the communications interception regime is consistent with contemporary community expectations about the types of communications that can be accessed and the purposes for which they can be accessed (see paragraphs 15 - 16).

vi. The OAIC is of the view that, in contemplating any proposed amendments to provisions providing for access to communications that intrude upon the privacy interests of Australians, consideration should be given to what measures are necessary to enable law enforcement and intelligence agencies to carry out their legitimate functions and whether or not each proposed measure is a proportional response to the problem it is seeking to address (see paragraphs 17 - 18).

Privacy accountability framework

vii. The OAIC emphasises the need to ensure that parallel privacy accountability arrangements exist where the Privacy Act does not apply and that any such arrangements provide substantially similar levels of privacy protection and are consistently applied (see paragraphs 19 - 23).

Communications interception warrants

viii. Noting the rapid pace at which telecommunications technology evolves, the OAIC suggests that the development of a plain English explanation outlining the types of communications information that can be intercepted and accessed under a warrant would assist in providing an appropriate level of transparency (see paragraph 27).

ix. The OAIC supports changes to the warrant regime that would enable law enforcement agencies to better target relevant communications when engaging in interception activities (see paragraph 29).

[2] In considering community expectations regarding the handling of personal information by Australian Intelligence agencies, the OAIC has had regard to the see also Australian Law Reform Commission (ALRC) 2008, *For Your Information, Australian Privacy Law and Practice, Report No. 108* (ALRC Report 108), Chapter 34: Intelligence and Defence Intelligence Agencies, available at www.alrc.gov.au/publications/report-108.

Information sharing arrangements

x. The OAIC considers that each of the regulatory frameworks setting out information sharing arrangements between law enforcement and intelligence agencies should clearly state the nature, scope and limits of the information sharing activities (see paragraphs 30 - 32).

Record-keeping by law enforcement agencies

xi. The OAIC would support a shift to a reporting framework that requires agencies to demonstrate that their communications access powers are being used lawfully and that any intrusions on the privacy of individuals are proportional to the outcomes being sought. The OAIC further suggests that reporting requirements should be developed to ensure that consistent standards are applied to all agencies and organisations involved in the communications interception regime (see paragraphs 33 - 35).

xii. Noting the fragmentation of existing oversight arrangements, the OAIC suggests that a more appropriate level of transparency could be achieved by providing the public with clear information about which oversight bodies are responsible for overseeing the access and interception activities of specific law enforcement agencies (see paragraph 36).

Retention of communications data under the TIA Act

xiii. In view of the potential for any data retention scheme to impact on the privacy interests of large numbers of individuals, the OAIC suggests consideration should be given to what steps can be taken to ensure there is a clear accountability framework in place for protecting the large volumes of personal information that would be required to be stored by carriers and carriage service providers (C/CSPs) (see paragraphs 37 - 38).

xiv. The OAIC believes that further information should be published:

- outlining the case for a two year retention period (see paragraphs 43 - 44)
- clarifying what information C/CSPs will be required to retain (see paragraph 45).

B. Telecommunications security sector reform

General comments

xv. The OAIC supports the policy intention behind the proposal to introduce a regulatory framework that will address security and resilience risks posed to Australia's telecommunications infrastructure (see paragraph 47).

xvi. In particular, the OAIC supports possible amendments to the Telecommunications Act to create an industry wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference (see paragraph 49).

Interaction of the proposed security framework with the obligations under the Privacy Act

xvii. The OAIC would welcome any changes implemented under the proposed security framework that would complement the existing obligations that C/CSPs have under the National Privacy Principles (NPP), particularly under NPP 4, and any other obligations currently imposed on agencies and organisations by the Privacy Act (see paragraph 52).

xviii. Noting that some C/CSPs operating under the proposed security framework may also be small business operators (SBOs) and therefore not covered by the operation of the Privacy Act, the OAIC suggests that consideration be given to ensuring that all C/CSPs are covered by both the proposed framework and the Privacy Act. The OAIC notes that section 6E of the Privacy Act provides the means to regulate the information handling practices of classes of SBOs that would not otherwise be subject to the obligations of the Privacy Act (see paragraph 55).

Implications for the OAIC's role as regulator under the Privacy Act

xix. Noting recommendations made by the Australian Law Reform Commission it its Report 108 *For Your Information, Australian Privacy law and Practice,* the OAIC suggests that a mandatory obligation to notify the Commissioner and affected individuals in the event of a data breach be considered as part of the proposed framework (see paragraphs 62 - 63).

C. Other proposals

xx. The OAIC suggests that the Committee may find it useful, when considering the proposals canvassed in the Discussion Paper relating to specific provisions in the *Australian Security Intelligence Organisation Act 1979* and *Intelligence Services Act 2001,* to have regard to the considerations contained in the OAIC's 4A Framework (see paragraphs 65 - 66).

xxi. The OAIC suggests that where the proposals would expand the existing powers of law enforcement and intelligence agencies in a way that may intrude upon the privacy interests of Australians, specific and transparent consideration of whether the proposed expansion is proportional to the public interest it is intended to address should be undertaken (see paragraph 66).

Office of the Australian Information Commissioner

1. The OAIC was established by the *Australian Information Commissioner Act 2010* (the AIC Act) and commenced operation on 1 November 2010. The OAIC is an independent statutory agency headed by the Australian Information Commissioner. The Information Commissioner is supported by two other statutory officers: the Freedom of Information Commissioner and the Privacy Commissioner. The former Office of the Privacy Commissioner (OPC) was integrated into the OAIC on 1 November 2010.
2. The OAIC brings together the functions of information policy and independent oversight of privacy protection and freedom of information (FOI) in one agency, to advance the development of consistent workable information policy across all Australian government agencies.
3. The Commissioners of the OAIC share two broad functions:
    - the FOI functions, set out in s 8 of the AIC Act – providing access to information held by the Australian Government in accordance with the *Freedom of Information Act 1982*
    - the privacy functions, set out in s 9 of the AIC Act – protecting the privacy of individuals in accordance with the *Privacy Act 1988* (C'th)(Privacy Act) and other legislation.
4. The Information Commissioner also has the information commissioner functions, set out in s 7 of the AIC Act. Those comprise strategic functions relating to information management by the Australian Government.

Background

5. On 9 July 2012 the Attorney-General asked the Parliamentary Joint Committee on Intelligence and Security (the Committee) to consider a package of national security ideas comprising proposals for telecommunications interception reform, telecommunications sector security reform and Australian intelligence community legislation reform.[3]
6. The Terms of Reference state that the National Security Legislation that is the subject of the Inquiry has three different elements and objectives; these relate to:
    - modernising lawful access to communications and associated communications data
    - mitigating the risks posed to Australia's communications networks by certain foreign technology and service suppliers

[3] Parliamentary Joint Committee on Intelligence and Security 2012, *Media Release - Committee to examine potential reforms of national security legislation*, available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/media.htm.

- enhancing the operational capacity of Australian Intelligence Community (AIC) agencies.[4]

7. The Government provided the Committee with the *Discussion Paper – Equipping Australia Against Emerging and Evolving Threats* (Discussion Paper), which describes the reform proposals.

8. The Committee has invited interested persons and organisations to make submissions addressing the Terms of Reference.

Structure of this submission

11. The OAIC's comments on the proposed reforms to national security legislation canvassed in the Discussion Paper are structured as follows:

    A. Proposed amendments to the communications interception regime

    B. Telecommunications security sector reform

    C. Other proposals.

A. Proposed amendments to the communications interception regime

General comments

12. The *Telecommunications Act 1997* (C'th) (Telecommunications Act) and the *Telecommunications (Interception and Access) Act 1979* (C'th) (TIA Act) together regulate the handing of telecommunications information.

13. Part 13 of the Telecommunications Act currently makes it an offence for carriers and carriage service providers (C/CSPs), including internet service providers,[5] to use or disclose information relating to the provision of carriage services; specifically information relating to:

    - the contents of a communication that has been carried by C/CSPs
    - carriage services supplied by C/CSPs
    - the affairs or personal particulars of another person.[6]

[4] See The Australian Government 2012, *Term of Reference - Inquiry into Potential Reforms of National Security Legislation,* available at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=pjcis/nsl2012/tor.htm.

[5] The *Telecommunications Act 1997* (C'th)(Telecommunications Act) does not refer specifically to internet service providers (ISPs). However, ISPs are included within the category of carriage service providers (CSPs). CSPs supply services for carrying communications to the public using a carrier's network (see s 87 Telecommunications Act). Therefore, all obligations that apply to CSPs apply to ISPs. For further information, see Australian Communications and Media Authority, *Internet service providers and law enforcement and national security fact sheet,* http://www.acma.gov.au/WEB/STANDARD/pc=PC_100072.

[6] See s 276 Telecommunications Act.

In addition, the TIA Act prohibits the unauthorised interception of communications passing over a telecommunications network and prohibits unauthorised access to stored communications (including, emails, text messages and voice mail messages stored on a carrier's equipment).[7]

14. To the extent that the TIA Act and the Telecommunications Act prohibit the unauthorised use, disclosure and interception of communications, they are focused on the protection of individuals' privacy interests. The OAIC welcomes this focus on privacy protection and supports the proposal to introduce a privacy focused objects clause in the TIA Act.[8]

15. Both the Telecommunications Act and the TIA Act provide for a limited number of exceptions to the prohibition on the use, disclosure and interception of communications, the most important of which is the ability to intercept or access communications under a warrant.[9] The comments in Part A of this submission are primarily concerned with ensuring that any modifications to the telecommunications interception regime are in keeping with current community expectations and are, on balance, in the public interest.

16. With this in mind, the OAIC would support a review of the current safeguards and privacy protections with a view to ensuring that the communications interception regime is consistent with contemporary community expectations about the types of communications that can be accessed and the purposes for which they can be accessed.[10]

17. The OAIC recognises that there is a public interest in allowing law enforcement and intelligence agencies to access communications where it is necessary for the prevention of serious and organised crime and threats to Australia's national security. In addition, the OAIC is mindful that any such interception regime must be able to take account of the rapid evolution of communications technology in order to ensure its continued effectiveness.

18. The OAIC is of the view that, in contemplating any proposed amendments to provisions providing for access to communications that intrude upon the privacy interests of Australians, consideration should be given to what measures are necessary to enable law enforcement and intelligence agencies to carry out their legitimate functions and whether or not each proposed measure is a proportional response to the problem it is seeking to address. In addition, the OAIC emphasises that any amendments to the interception and access regime should be subject to appropriate and ongoing accountability and review mechanisms.

---

[7] See s 7 *Telecommunications (Interception and Access) Act 1979* (C'th) (TIA Act).
[8] See Discussion Paper, p 23.
[9] See ss 7(2)(b) and 108(2)(a)-(c) TIA Act and s 280 Telecommunications Act; for further information see Australian Government Attorney-General's Department, *Overview of legislation,* available at http://www.ag.gov.au/Telecommunicationsinterceptionandsurveillance/Pages/Overviewoflegislation.aspx.
[10] See Discussion Paper, p 23.

Privacy accountability framework

19. The OAIC is mindful that any exceptions to the general prohibition on the interception of communications have the potential to authorise the collection and disclosure of a wide range of personal information. In these circumstances, an effective and comprehensive privacy accountability framework is essential to safeguard the privacy interests of individuals.

20. The OAIC notes that, in relation to law enforcement and intelligence agencies, the current privacy accountability framework is fragmented and opaque, in the sense that privacy obligations and oversight responsibilities are split across a range of legislation and Commonwealth and State bodies.[11] The OAIC considers that, under the current accountability framework, it is difficult for the Australian public to gain assurance that the existing obligations and oversight mechanisms are adequate to cover the full range of interception activities and agencies. The OAIC is particularly mindful that the Privacy Act does not apply to a number of the law enforcement and intelligence bodies whose activities fall within one or more of the exceptions to the general prohibition against the interception of communications under the TIA Act.[12]

21. In light of these considerations, the OAIC emphasises the importance of ensuring that parallel accountability arrangements are in place where the Privacy Act does not apply and that any such arrangements provide consistent application of substantially similar privacy protections.

22. The OAIC considers that the Inquiry into Potential Reforms of National Security Legislation (the Inquiry) may present a good opportunity to resolve any inconsistencies in the current privacy accountability framework, and welcomes any proposals that result in reduced fragmentation in relation to accessing communications data.

[11] For example, the Inspector-General of Intelligence and Security (IGIS) has oversight of the six Australian Intelligence Community (AIC) agencies (the Australian Security Intelligence organisation (ASIO), the Australian Secret Intelligence Service (ASIS), Office of National Assessments (ONA), Defence Signals Directorate (DSD), Defence Intelligence Organisation (DIO) and Defence Imagery and Geospatial Organisation (DIGO)). The OAIC understands that the ASIS, DSD and DIGO are required by the *Intelligence Services Act 2001* (ISA) to make written rules regulating the communication and retention of intelligence information concerning Australian persons (see s15 ISA). In contrast, the communication of intelligence information by DIO and ONA is governed by privacy guidelines, issued by the Minister for Defence in the case of DIO, and the Director-General of ONA in the case of ONA. ASIO operates under the *Australian Security Intelligence Organisation Act 1979* under which the Attorney-General may give the Director-General of Security written guidelines to be observed by ASIO in the performance of its functions. For further information see http://www.igis.gov.au.

[12] The obligations imposed by the *Privacy Act 1988* (C'th) (Privacy Act) only extend to Commonwealth agencies, including the Australian Federal Police (see s 6 Privacy Act), and will therefore not apply to state law enforcement agencies; see also ss 7(1) and 7(1A) of the Privacy Act which exempt the acts and practices of intelligence agencies, and the acts or practices of Commonwealth agencies in disclosing personal information to intelligence agencies.

23. The OAIC notes that the Inspector-General of Intelligence Security (IGIS), who has responsibility for the oversight of the AIC,[13] commented in her 2010-2011 Annual Report that the privacy guidelines and rules that apply to a number of the AIC agencies are based on rules which are now 10 years old.[14] The OAIC reiterates its earlier comments regarding the importance of privacy oversight, the need for parallel arrangements where the Privacy Act does not apply and the public interest in ensuring that privacy protections are consistently applied (see paragraphs 19 - 21 above). The extent to which any revisions to the privacy rules and guidelines derogate from or add to the existing privacy obligations on AIC agencies, and if so whether any derogation is necessary and proportional to the needs the amendments are intended to address, may be a matter for the IGIS to consider.

Communications interception warrants

24. The OAIC recognises the need to ensure that the communications interception regime is well adapted to the current technological environment and that certain provisions of the TIA Act, where they are based on considerations that are no longer relevant, may need to be updated. However, the OAIC notes that warrants allowing law enforcement and intelligence agencies to intercept and access communications data have the potential to intrude upon the privacy interests of individuals. In some cases, the information accessed may relate to people who are not themselves the subject of the warrant, and are not of interest to the agency that has sought authority for the interception.[15]

25. Given the extent of the privacy impacts associated with the grant of interception and stored communications warrants, the OIAC reiterates that any amendments to the provisions regulating the availability of such warrants should be proportional to the gravity and probability of the threat those amendments are intended to address. The OAIC considers that this is particularly important when the Committee is considering changes to the threshold test that determines when a warrant can be issued.[16]

26. The OAIC notes the proposal in the Discussion Paper that consideration be given to extending the interception regime to a broader range of telecommunications industry participants, such as social network providers and cloud computing providers.[17] The OAIC is mindful that developments in communications technology mean that a large portion of current communications take place outside of traditional services and/or employ traditional communications services in new and innovative ways. In certain circumstances, there may be a legitimate need for law

[13] See ss 8, 9 and 9A of the *Inspector-General of Intelligence and Security Act 1986*.
[14] IGIS 2011*, IGIS Annual Report 2010–2011 (IGIS Annual Report)* p 9, available at http://www.igis.gov.au/annual_report/index.cfm.
[15] See s 46(1)(d) TIA Act that requires only that the information that would be likely to be obtained by intercepting a communication would '*be likely to assist in connection with the investigation by the agency of a serious offence*' in which *'the particular person is involved'* or *'another person is involved with whom the particular person is likely to communicate using the service'*.
[16] See Discussion Paper, p 24.
[17] See Discussion Paper, p 27.

enforcement and intelligence agencies to have authorised access to information about these new types of communications. However, the OAIC is also mindful that the volume of personal information that is stored on or that passes over these new networks may be very large, and of a different type, when compared with the more traditional telecommunications services. Accordingly, the OAIC believes that careful consideration should be given to the types of information that would be able to be accessed or intercepted by law enforcement and intelligence agencies if the interception regime were extended to include a broader range of telecommunications industry participants.

27. In addition, the OAIC is mindful that communications technology evolves at a rapid pace and that, as a result, the Australian community may not have a clear understanding of what information is able to be the subject of a warrant. Accordingly, the OAIC suggests that the publication of a plain English explanation outlining the types of communications information that can be intercepted and accessed under a warrant would assist in providing an appropriate level of transparency.

28. In keeping with the comments above, the OAIC supports the proposal to limit access to communications information to agencies that have a demonstrated need to access that type of information.[18] Also, the OAIC suggests clarifying the basis on which an agency will be considered to have a need to access communications information. The OAIC considers that this is consistent with the privacy principles that underpin the Privacy Act; in particular, the principle that agencies should only collect information where it is necessary for one of their legitimate functions or activities.

29. The OAIC is supportive of any proposal that has the effect of minimising the intrusion on the privacy interests of individuals that are not under investigation or suspected of being involved in a serious offence. Accordingly, the OAIC would support changes to the warrant regime that would enable law enforcement agencies to better target relevant communications and to isolate these from other communications that are not of interest.[19]

Information sharing arrangements

30. The OAIC recognises that information sharing will often be necessary to facilitate effective cooperation between law enforcement and intelligence agencies, and that ensuring consistency in the protections afforded to personal information is challenging as a result of fragmentation in the existing accountability framework. However, the OAIC considers that this fragmentation makes it particularly important that each of the applicable regulatory frameworks setting out information sharing arrangements between law enforcement and intelligence agencies clearly and consistently specifies the nature, scope and limits of the information sharing

[18] See Discussion Paper, p 24.
[19] See Discussion Paper, p 25.

activities. This includes specifying what protections are afforded to any personal information collected, used or disclosed under the information sharing arrangement.

31. The OAIC is mindful that the risk of the fragmentation in existing accountability arrangements leading to inconsistencies in the level of privacy protection afforded to personal information is increased in the context of information sharing between law enforcement and intelligence agencies. The OAIC considers that this increase in risk occurs because the information handling practices of each agency involved in the exchange of the communications information may not impose the same, or substantially similar, obligations. More specifically, the OAIC considers that the obligations on the agency providing the information should be substantially equivalent to the obligations imposed on the recipient; this would ensure that the personal information is provided with the same level of protection at all points in the information handling process.

32. In view of these considerations, the OAIC reiterates the importance of ensuring that the accountability arrangements that apply to the various law enforcement and intelligence agencies are underpinned by a common set of considerations that accord with current community expectations regarding the protection of individuals' privacy interests.

Record-keeping by law enforcement agencies

33. Both the Telecommunications Act and the TIA Act impose obligations on law enforcement agencies to maintain records of their activities relating to access and interception of telecommunications information.[20] The Discussion Paper highlights the fragmentation of existing oversight arrangements in relation to record-keeping by law enforcement agencies.[21] The OAIC understands that the existing oversight arrangements are broken up as follows:

    - The Commonwealth Ombudsman has oversight of Commonwealth law enforcement bodies, such as the Australian Federal Police, that intercept communications under the TIA Act.[22]

    - The equivalent state bodies (for example, State Ombudsman) have oversight for the interception of communications by state law enforcement agencies under the TIA Act.[23]

[20] See ss 306 and 306A Telecommunications Act and ss 80 (communications interception warrants) and 151 (stored communication warrants) TIA Act.
[21] See Discussion Paper, p 26.
[22] See s 83 TIA Act; ALRC Report 108, para 73.129. For more information see: the Commonwealth Ombudsman's website at http://www.ombudsman.gov.au/pages/about-us/our-office/our-inspections-role.php#2.
[23] Under s 35(1)(h) TIA Act, before a State law enforcement agency is eligible to intercept communications there must be an equivalent State law requiring regular inspections of the agency's records relating to the interception of communications by an independent State authority.

- The Commonwealth Ombudsman has oversight of all agencies in relation to access to stored communications (including, emails, text messages and voice mail messages stored on a carrier's equipment).[24]

- In relation to the authorised use and disclosure of telecommunications information held by C/CSPs under the Telecommunications Act, the Commissioner is responsible for monitoring compliance with the record-keeping requirements imposed under ss306 and 306A of that Act.[25]

34. The Discussion Paper proposes new reporting requirements that provide the flexibility for each law enforcement agency to determine the best way to record and report on information that demonstrates that they are using their powers lawfully. This is in response to concerns that the current oversight system, which is focused on ensuring that law enforcement agencies meet their administrative reporting obligations, is not achieving its objectives.[26] The OAIC supports the proposed shift to a reporting framework that requires agencies to demonstrate that their powers relating to access to communications are being used lawfully and that any intrusions on the privacy of individuals are proportional to the outcomes being sought.

35. The OAIC suggests that such reporting requirements should be developed to ensure that consistent standards are applied to all agencies and organisations that are involved in the communications interception regime.

36. Additionally, the OAIC notes that the fragmentation of existing oversight arrangements can make it difficult for the public to discern which oversight body is responsible for overseeing the access and interception activities of a particular law enforcement agency. The OAIC is mindful that the nature of the activities undertaken by law enforcement agencies may mean that, in certain circumstances, it is not appropriate for these activities to be made public. In these circumstances, it is particularly important that effective oversight arrangements exist to ensure that these agencies are not exceeding their lawful authority and to give the public confidence that their personal information is being handled in accordance with contemporary community expectations. The OAIC suggests that providing the public with clear information about which oversight bodies are responsible for overseeing the access and interception activities of specific law enforcement agencies would provide a more appropriate level of transparency.[27]

[24] See s 152 TIA Act.
[25] See s 309 Telecommunications Act.
[26] See Discussion Paper, p 26.
[27] For example, the website of the IGIS provides a clear outline of the privacy protections that apply to the Australian Intelligence Community (AIC) agencies, as well as identifying the roles played by different oversight bodies in ensuring that the AIC agencies meet their obligations; see IGIS, *AIC Privacy Protections*, available at http://www.igis.gov.au/aic/privacy_protection.cfm.

Retention of communications data under the TIA Act

37. The OAIC notes that the proposals relating to data retention[28] would involve vast amounts of personal information relating to large numbers of people. Accordingly, any regime providing access to this data has the potential to intrude upon the privacy interests of large numbers of individuals. The OAIC notes that the majority of these people will not themselves be under investigation or suspicion at any time in their lives. In light of these considerations, the OAIC emphasises the importance of ensuring that any data retention scheme is a proportional response to address legitimate needs of law enforcement and intelligence agencies; moreover, that the scope of such a scheme is limited to what is necessary to ensure that those needs are met.

38. The OAIC is concerned to ensure that any data retention regime is accompanied by a regulatory framework that provides the necessary level of transparency and accountability and is consistent with contemporary community expectations. In view of the potential for such a scheme to impact on the privacy interests of large numbers of individuals, consideration should be given to what steps can be taken to ensure there is a clear accountability framework in place for protecting the large volumes of personal information that would be required to be stored. The OAIC suggests that such steps might include:

    - Government setting the standards, through legislation and guidance, for ensuring there is an appropriate security regime in place to protect individuals' personal information.

    - Legislation imposing an industry wide obligation on all C/CSPs to protect their infrastructure and the information held on it, or passing across it, from unauthorised interference.

    - Provision of guidance material and support to help C/CSP implement strategies to mitigate potential security risks.

    - Introducing a mandatory data breach notification scheme to ensure that C/CSPs are also accountable for the information they hold under the proposed communications data retention scheme.

39. The OAIC is mindful of the risk of creating a 'honey pot' of personal information that would be an attractive target for individuals with criminal or malicious intent. The OAIC notes that the imposition of a requirement on C/CSPs to retain data for an extended period increases the risk of a data breach. The OAIC considers that this increase in risk is attributable to two factors:

    1. The creation of large repositories of personal information is an attractive target for people with malicious and/or criminal intent

[28] See Discussion Paper, p 13.

2. The challenges faced by C/CSPs in discharging their obligation to maintain adequate security arrangements to protect the data they hold from unauthorised interference become more difficult as technology evolves.

The OAIC emphasises that the regulation and security framework put in place by the government to oversee C/CSPs' management of this large volume of personal information should take account of this increase in risk and the extent of the damage that could occur to the privacy interests of a large number of individuals in the event of a data breach.

40. The OAIC notes that any data retention regime would place a heavy reliance on the participation of industry (particularly C/CSPs) to appropriately store and provide access to communications data. The need for government involvement in establishing an appropriate security regime, including through regulation, is evidenced by the number of large scale data and security breaches that have occurred in recent times.

41. The OAIC notes that the Australian Privacy Commissioner's own motion investigations (OMIs) into these breaches have noted the failure of a number of organisations to adequately protect the personal information they hold in compliance with their obligations, including under National Privacy Principle (NPP) 4, contained in Schedule 3 to the Privacy Act. More specifically, since early 2011 the Commissioner has undertaken a series of OMIs in which he concluded that the relevant organisations did not have reasonable steps in place to protect personal information, in contravention of NPP 4.[29]

42. Importantly however, following other OMIs the Commissioner found that the data breach in question occurred despite the organisations having taken reasonable steps to protect the personal information. Data breaches may occur, for example, due to a malicious attack, even though all reasonable steps have been taken to secure the data. In these cases, while personal information may have been compromised, the Commissioner found the organisations were not in breach of their obligations under NPP 4.[30]

43. The OAIC is mindful that the retention of communications data is a live issue in a number of jurisdictions around the world, most notably in Europe. In particular, the

[29] For further information see Office of the Australian Information Commissioner (OAIC) 2012, *Medvet Science Pty Ltd - Own motion investigation report*, available at http://www.oaic.gov.au/publications/reports/medvet_own_motion_July2012.html; OAIC 2012, *Telstra Corporation Limited - Own motion investigation report*, available at http://www.oaic.gov.au/publications/reports/own_motion_telstra_bundles_June_2012.html; OAIC 2011, *Vodafone Hutchison Australia - Own motion investigation report*, available at http://www.oaic.gov.au/publications/reports/Report-Investigation-Vodafone_Hutchison_Australia_OMI.html; OAIC 2012, *First State Super Trustee Corporation - Own motion investigation report*, available at http://www.oaic.gov.au/publications/reports/own_motion_first_state_super_review_June_2012.html.

[30] For example see OAIC 2012, *Sony PlayStation Network / Qriocity - Own motion investigation report*, available at http://www.oaic.gov.au/publications/reports/own_motion_sony_sep_2011.html.

OAIC notes that the proposed retention period of up to two years is at the upper end of retention periods permitted by the EU Data Retention Directive (DRD).[31] Since the enactment of the DRD, all member states except one have transposed the DRD into national legislation[32] and only one EU member state has imposed a retention period of two years for all types of communications data, with the majority of member states imposing a retention period of one year or less.[33] This includes the equivalent provisions in the United Kingdom *Draft Communications Data Bill 2012* (UK Draft Communications Data Bill) that is currently the subject of a Joint Committee inquiry.[34]

44. The OAIC notes that the Discussion Paper does not include a detailed discussion of proposals relating to data retention. In particular, it is not clear what the basis for the proposed two year data retention period is and whether alternative retention periods were considered. The OAIC believes that further information should be published about the consideration that has been given to the case for a two year retention period being proportional to address the legitimate needs of law enforcement and intelligence agencies.

45. In addition, the OAIC believes that clarification should be provided about what information will be retained under any data retention scheme. Given the potential for the proposed data retention scheme to impact upon the privacy interests of individuals, the OAIC considers that it is important that the Australian public is fully informed about the type of information that would be stored by C/CSPs. [35]

46. The OAIC suggests that further analysis be undertaken to explore the range of options that are available to address the legitimate needs of law enforcement and

[31] Directive 2006/24/EC of the European Parliament and of the Council of 15 March 2006 on the on the retention of data generated or processed in connection with the provision of publicly available electronic communications services or of public communications networks and amending Directive 2002/58/EC (EU Data Retention Directive).

[32] Although the OAIC notes that this national legislation has been the subject of a constitutional challenge in a number of member states, for example Germany. For further information see European Commission 2011, *Report from the Commission to the Council and the European Parliament: Evaluation report on the Data Retention Directive (Directive 2006/24/EC)*, pp 20-21, available at http://ec.europa.eu/commission_2010-2014/malmstrom/archive/20110418_data_retention_evaluation_en.pdf (EC Report on the DRD) (EC Report on the DRD).

[33] Poland is the only EU member state that has imposed a data retention period of 2 years; for further information see EC Report on the DRD, pp 13-14.

[34] Under the *Draft Communications Data Bill 2012* the United Kingdom Government is proposing a data retention period of 1 year; for further information on the Joint Committee Inquiry see http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/.

[35] The OAIC notes that there has been some discussion about what information is characterised as 'subscriber information' in relation to the data retention provisions in the UK *Draft Communications Data Bill 2012*; specifically, whether this category of personal information could extend to all the information contained in an individual's social networking account (e.g. Facebook account). See for example comments made by Jim Killock, Executive Director of Open Rights Group, in the House of Lords House of Commons Oral Evidence before the Joint Committee on the Draft Communications Data Bill 2012, available at http://www.parliament.uk/business/committees/committees-a-z/joint-select/draft-communications-bill/ pp 12-13.

intelligence agencies in relation to obtaining access to communications. This would include consideration of the duration of the proposed retention period and the type of information that would be retained and help to clarify the matters that were considered when settling on a period of up to two years. In undertaking such analysis, it may be useful to draw on elements of the OAIC's privacy impact assessment (PIA) framework.[36] The OAIC would be willing to engage with the government in undertaking such an assessment process. In the event that such analysis has already been undertaken, the OAIC suggests that it should be made public.

B. Telecommunications security sector reform

General comments

47. The OAIC supports the policy intention behind the proposal to introduce a regulatory framework that will address security and resilience risks posed to Australia's telecommunications infrastructure.

48. The OAIC welcomes the fact that one of the desired outcomes of the framework is that the security of individuals' personal information contained on or transmitted across telecommunication networks is better assured. The OAIC notes that this is particularly important in the context of the ongoing evolution of telecommunications technology, the shift towards the provision of telecommunications services on a global scale, increased standardisation and mass-production of network equipment and increased market participation and competition.

49. The OAIC notes that ensuring that Australian telecommunications networks are protected by an effective security framework is particularly important given the proposals relating to data retention (see discussion at paragraphs 37 - 46 above). In particular, the OAIC supports possible amendments to the Telecommunications Act to create an industry wide obligation on all C/CSPs to protect their infrastructure and the information held on it or passing across it from unauthorised interference.[37]

50. The OAIC notes that industry expressed a preference for an approach that avoids the need for government approval of network architecture at a technical or engineering level and instead focuses on the security outcome, leaving industry to choose the most effective way to achieve it.[38] The OAIC considers that such an outcomes-based regulatory framework would ensure that C/CSPs have sufficient flexibility to respond to changes in telecommunications technology, whilst also ensuring that the Government remains responsible for ensuring that the overall protection of personal information is achieved.

[36] OAIC 2010, Privacy Impact Assessment Guide (PIA Guide), available at http://www.privacy.gov.au/materials/types/guidelines/view/6590.
[37] See Discussion Paper, p 33.
[38] See Discussion Paper, p 35.

51. The OAIC considers that the regulatory framework should be underpinned by a security framework set and administered by government. The OAIC considers that will be particularly important in the event that a data retention proposal is progressed. Consideration will need to be given to what measures can be taken to provide appropriate levels of assurance that the telecommunications industry has taken sufficient steps to protect the data it holds from unauthorised interference.

Interaction of the proposed security framework with obligations under the Privacy Act

52. If implemented, the proposed security framework would operate in conjunction with the Privacy Act. The OAIC notes that, in addition to any obligations imposed under the proposed security framework, C/CSPs may also have National Privacy Principle (NPP) or Information Privacy Principle (IPP) obligations with which they will also need to comply. In particular, NPP 4 requires an organisation to take reasonable steps to protect the personal information it holds from misuse, loss, unauthorised access, modification or disclosure.[39] The OAIC would welcome any changes implemented under the proposed framework that would complement the obligations in NPP 4 and any other obligations currently imposed on agencies and organisations by the Privacy Act.[40]

53. Generally, small business operators (SBOs) with an annual turnover of $3 million or less are not covered by the Privacy Act.[41] The OAIC is mindful that it is possible that some C/CSPs may be SBOs and therefore may not be covered by the operation of the Privacy Act. In developing this framework further, the OAIC suggests that consideration be given to how the privacy of individuals' personal information will be better assured given that there may be C/CSPs operating under the security framework that are not covered by the Privacy Act.

54. In particular, the OAIC suggests that any further analysis of proposals relating to data retention (see discussion at paragraph 46 above) consider whether any C/CSPs are likely to be exempt from the application of the Privacy Act.

55. The OAIC considers that steps should be identified that would ensure that all C/CSPs are covered by both the proposed framework and the Privacy Act. Ensuring that all

[39] See National Privacy Principle (NPP) 4 and also Information Privacy Principle (IPP) 4 in the Privacy Act.
[40] In addition, the OAIC notes that the *Privacy Amendment (Enhancing Privacy Protections) Bill 2012* (Privacy Amendment Bill), currently being considered by the Senate Committee on Legal and Constitutional Affairs and the House of Representatives Committee on Social Policy and Legal Affairs, proposes to consolidate the NPPs and the IPPs into a single streamlined set of principles – the Australian Privacy Principles (APPs) – that apply to both agencies and organisations alike. The OAIC notes that APP 11 imposes similar obligations in relation to the protection and destruction of personal information as those imposed under NPP 4 and IPP 4. For a discussion of the differences between the obligations imposed by APP 11 and existing obligations see Explanatory Memorandum, Privacy Amendment (Enhancing Privacy Protection) Bill 2012, p 86, available at www.aph.gov.au/Parliamentary_Business/Bills_Legislation/Bills_Search_Results/Result?bId=r4813 (Explanatory Memorandum).
[41] See ss 6C and 6D Privacy Act.

C/CSPs are covered by both the proposed security framework and the Privacy Act will help ensure that the necessary level of accountability is achieved and thereby lead to increased consumer confidence and trust in the operations of the C/CSPs. The OAIC notes that section 6E of the Privacy Act enables the Governor-General to prescribe that certain SBOs are to be treated as organisations for the purposes of the Privacy Act. This mechanism provides the means to ensure that the information handling practices of C/CSPs that are SBOs are subject to the obligations of the Privacy Act in relation to the provision of carriage services.

56. The Discussion Paper notes that in order to assist industry in meeting its obligation to protect infrastructure and customer information from unauthorised interference, the government will disseminate threat information on security risks to the sector, which may include general security advice or specific mitigation information and targeted briefings.[42] The OAIC supports this proposal as it may assist C/CSPs to take reasonable steps to mitigate privacy risks and comply with their obligations under the Privacy Act and as a means of further strengthening privacy practices within the telecommunications industry.

57. In addition, the OAIC reiterates its comments at paragraph 51 above; namely that, in the event that proposals relating to data retention are progressed, it is important to consider what measures could be taken to provide appropriate levels of assurance that there is an effective security framework in place to protect individuals' personal information. The OAIC considers that the provision of guidance material and support will help C/CSP implement strategies to mitigate potential security risks and, thereby, bolster public confidence in C/CSP's information handling practices.

Implications for the OAIC's role as regulator under the Privacy Act

58. The OAIC is mindful that under the Privacy Act, individuals can make a complaint to the OAIC about the handling of their personal information by Australian government, Australian Capital Territory and Norfolk Island agencies and private sector organisations covered by the Privacy Act.[43] If a complaint were made involving a C/CSP and its security arrangements relating to the protection of personal or sensitive information, the information the C/CSP had received from the government on specific threats may be an important factor in the OAIC's assessment of the complaint and the reasonableness of the steps taken by the C/CSP.

59. The OAIC notes that under the proposed framework some C/CSPs would be required to provide government with information on significant business and procurement decisions and network designs.[44] The OAIC suggests that the framework clearly state that as part of the notification obligation, C/CSPs be required to notify government if the proposed significant changes will involve any new handling (i.e. collection, use, storage or disclosure) of personal information; for example, new outsourcing arrangements that may result in other entities having access to personal information.

[42] See Discussion Paper, p 36.
[43] See s 36 Privacy Act.
[44] See Discussion Paper, p 10.

In addition, the OAIC notes that under the proposed changes to privacy law currently being considered by the Senate Committee on Legal and Constitutional Affairs and the House of Representatives Committee on Social Policy and Legal Affairs,[45] the Privacy Commissioner would have a new power to conduct an assessment to determine whether personal information held by an entity is being maintained in accordance with the proposed Australian Privacy Principles.[46]

60. When contemplating any significant changes to their infrastructure, procurement or other business arrangements, the OAIC would encourage C/CSPs to conduct a PIA as a way of identifying any privacy risks or benefits of particular information handling practices that may improve project implementation and outcomes.[47]

61. Under the proposed framework, a graduated suite of enforcement measures (including powers of direction and the imposition of financial penalties) are envisaged for C/CSPs who fail to take action to reasonably protect their infrastructure.[48] It should be noted that the proposed reforms to privacy law include provisions that will strengthen the Commissioner's enforcement powers.[49] These proposed changes include the power to accept written undertakings by entities that they will take, or refrain from taking, specific action to ensure compliance with the Privacy Act.[50] In the event that a C/CSP does not comply with such undertakings, or in event of a serious or repeated interference with the privacy of an individual, the proposed provisions empower the Commissioner to seek a civil penalty in the Federal Court or Federal Magistrates Court.[51]

62. The ALRC, in its Report 108 *For Your Information, Australian Privacy law and Practice* (ALRC Report 108), also recommended that the Privacy Act be amended to impose a mandatory obligation to notify the Commissioner and affected individuals in the event of a data breach that could give rise to a real risk of serious harm to affected individuals.[52] The OAIC notes that the Government has stated that it will be considering mandatory data breach notification as part of its second stage response to the ALRC Report 108.[53] The OAIC also notes that data breach notification is an issue that was considered by the Australian Government's Cyber White Paper and

[45] For more information see the Parliament of Australia website at http://www.aph.gov.au/Parliamentary_Business/Bills_Legislation.
[46] See clause 33C(1) Privacy Amendment Bill.
[47] For more information on Privacy Impact Assessments see the OAIC PIA Guide available at http://www.privacy.gov.au/materials/types/guidelines/view/6590.
[48] See Discussion Paper, p 37.
[49] See Schedule 4 Privacy Amendment Bill and Explanatory Memorandum, pp 1, 4-5, 216-263.
[50] See cl 33E Schedule 4 Privacy Amendment Bill.
[51] See cll 13G and 33F(1) Schedule 4 Privacy Amendment Bill.
[52] ALRC, Report 108, recommendation 51-1.
[53] The Australian Government 2009, *Enhancing National Privacy Protection, Australian Government First Stage Response to the Australian Law Reform Commission Report 108* (Government first stage response), p 62, available at www.ag.gov.au/Privacy/Pages/Privacy-Reforms.aspx.

that responses from stakeholders indicated a broad level of support for a mandatory data breach notification regime.[54]

63. Data breaches are not limited to malicious actions, such as theft or 'hacking', but may arise from internal errors or failures to follow information handling policies that cause accidental loss or disclosure. While notification of a data breach is currently not required by the Privacy Act[55], the OAIC suggests that it be considered as part of the proposed framework as an important mitigation strategy against privacy risks. It may also assist in promoting transparency and trust for C/CSPs.

64. The OAIC suggests that the implementation of an effective mechanism for ensuring that industry has taken reasonable steps to mitigate security risks is essential and will assist in achieving the necessary levels of transparency and accountability. In the event that there is a complaint to the OAIC, access to any compliance assessments and audits of the Government under the proposed regime would assist the OAIC in its investigation of the matter.

C. Other proposals

65. The OAIC notes the focus of the inquiry on ensuring that the proposals contain appropriate safeguards for protecting the human rights and privacy of individuals and are proportionate to any threat to national security and the security of the Australian private sector. In light of this focus, the Committee may find it useful when considering the proposals canvassed in the Discussion Paper relating to specific provisions in the *Australian Security Intelligence Organisation Act 1979* and *Intelligence Services Act 2001* to have regard to the considerations contained in the OAIC's 4A Framework.[56]

66. The OAIC is mindful that many of these proposals are directed towards streamlining and simplifying existing administrative arrangements and procedures, particularly those relating to warrants. However, the OAIC suggests that where the proposals (especially those relating to warrants) would expand the existing powers of law enforcement and intelligence agencies in a way that may intrude upon the privacy of Australians, specific and transparent consideration of whether the proposed expansion is proportional to the public interest it is intended to address should be undertaken.

[54] For further information see Australian Government, *Connecting with Confidence: Optimising Australia's Digital Future*, available at http://cyberwhitepaper.dpmc.gov.au/.
[55] For further information please see the OAIC's 2012 edition of its *Data breach notification: A guide to handling personal information security breaches*, available at http://www.oaic.gov.au/publications/guidelines/privacy_guidance/data_breach_notification_guide_april2012.html
[56] For further information see OAIC 2001, *4A framework – A tool for assessing and implementing new law enforcement and national security powers*, available at http://www.oaic.gov.au/publications/privacy_fact_sheets/Privacy-fact-sheet3_4Aframework.pdf.

67. In making this observation, the OAIC is mindful that the IGIS has responsibility for the oversight of AIC agencies to which these provisions relate and may be better placed to assist the Committee in relation to these issues.