OFPC Submission to the Inquiry into the Provisions of the Anti-terrorism Bill (No.2) 2004

In April 2002, the Office of the Federal Privacy Commissioner (the Office) made a submission to the Senate Legal and Constitutional Legislation Committee (the Committee) Inquiry into a number of anti-terrorism bills. The Office remains of the view, expressed in that submission, that there should be an appropriate balance between the need for security and the right to privacy (Attachment 1). As one means of making judgements between competing priorities, the Office recommended to the Inquiry a framework by which new legislative measures could be assessed. Since that submission, the Office has developed and refined this framework (Attachment 2). The Office commends the framework to this Inquiry when it is considering the Anti-terrorism Bill (No.2) 2004 (the Bill).

The proposed amendments

The Office understands that the intention of the Bill is to add new powers to various pieces of existing legislation. Broadly speaking, the goal of these amendments is to enhance the powers of law enforcement and related agencies to meet the threat of terrorist activity.

Obligations under the Privacy Act 1988

Australian Government agencies under the jurisdiction of the *Privacy Act 1988* (the Act), including the Australian Federal Police (AFP), have compliance obligations under the Information Privacy Principles (IPPs) in the Act to ensure respect for the privacy of individuals when they are carrying out their functions. Accordingly, relevant agencies would need to address their obligations under the IPPs if undertaking law enforcement activities in respect of proposals in the Bill.

For example, relevant agencies would need to comply with the IPPs when investigating matters under the amendments to Division 102 of the Criminal Code Act 1995. These amendments would make it an offence to intentionally associate with persons who are, generally speaking, connected with terrorist organisations. To establish whether the conduct of an individual brings them within the terms of the proposed amendment, there will, in many cases, need to be surveillance by law enforcement officers. In the course of this surveillance, it is likely that personal information about 'innocent' individuals will be collected and analysed.

Crimes Act 1914 (forensic procedures)

The Office is represented on the committee undertaking the review of Division 11A of the *Crimes Act 1914*, which was enacted to facilitate disaster victim identification and the criminal investigation of the Bali bomb incident. This committee recommended the domestic mass casualty incidents amendment to the Minister for Justice and Customs in April 2004, ahead of the finalisation of the review, as it had been raised in submissions by several organisations, and the committee considered that the need was important and urgent, particularly in light of the recent bombing incident in Madrid. For these reasons, the Office supports the amendments to the forensic procedures provisions in the *Crimes Act 1914.*

Oversight and Accountability

The Office also notes that some amendments involve the transfer of personal information between jurisdictions. Mechanisms that are consistent with maintaining national security should be considered to ensure that the cross-border activities, both nationally and internationally, of law enforcement and national security agencies are subject to appropriate independent oversight.

Conclusion

As stated in our earlier submission of April 2002, the Office re-affirms the importance of striking the appropriate balance between the right to privacy and the right to be safe and secure. Where proposed legislation, such as the Bill, raises issues regarding competing rights, the Office recommends that its operational impact on individuals' lives be reviewed after a defined period, with the basis for such a review being stated in legislation. The timing of a review would depend on the particular circumstances of each amendment, but a period of two or three years seems reasonable.

ATTACHMENT 1

Inquiry by the Senate Legal and Constitutional Legislation Committee into the following bills:

Security Legislation Amendment (Terrorism) Bill 2002

Suppression of the Financing of Terrorism Bill 2002

Criminal Code Amendment (Suppression of Terrorist Bombing) Bill 2002

Border Security Legislation Amendment Bill 2002

Telecommunications Interception Legislation Amendment Bill 2002

Introduction

1. The community expects that a key role for its parliament is to ensure a safe and secure environment that is reasonably protected from criminal activities such as terrorism. These expectations have been heightened by the terrible events of 11 September 2001. While it is the responsibility of a parliament to deliver on these expectations, it also has the responsibility of ensuring that other rights are not unnecessarily eroded as a consequence. There is little point living in a safe and secure environment if it is not also dignified, free from discrimination and, where desired by the individual, private. At the same time, privacy can not be an absolute right in a modern democratic society.

2. Striking the balance between the right to privacy and the right to feel safe and secure is not always an easy thing to do. Finding the balance, however, is a challenge that befalls the parliaments of all democracies and has done so throughout history. Though they may risk appearing overly simplistic, Benjamin Franklin's words are worth contemplation when he tells us that "(t)hose who are willing to trade civil liberties for temporary security, deserve neither".

3. The anti-terrorism legislation currently being considered by the Senate Legal and Constitutional Legislation Committee (the Committee) is clearly designed to provide our authorities with additional tools for combating terrorism and prosecuting offenders. It does this by giving particular agencies additional powers to monitor the actions of individuals by collecting, using and disclosing personal and other information. It does not appear, however, that the balance between the right to privacy and the right to feel secure has been met in every instance.

4. For this reason the Committee's inquiry into these bills is welcome and the content of this submission is aimed at helping further inform the debate.

5. The Committee should be aware of the limitations of this submission. The Office of the Federal Privacy Commissioner (the Office) seeks to promote an Australian culture that respects privacy and has prepared this submission from a privacy and data protection perspective only – it is not a comprehensive analysis of

the legislation from other perspectives. Furthermore, this submission is not intended as a definitive discussion of the privacy implications of the proposed legislation. In particular, the period allocated for comment has not allowed consideration of these bills in a broader legal context. In the time available, many existing legal provisions and administrative practices likely to impact upon these bills, or upon an individual's right to privacy, have not been considered within the analysis.

6. This submission is divided into two main sections. The first outlines a general approach to assessing bills that are likely to have an impact on privacy. This approach incorporates a framework that intends to bring balance and perspective to any deliberations. The framework emphasises the ideas of proportionality and the need to strike an appropriate balance between an individual's right to privacy and the right of the community to safety and security.

7. The second section applies this framework, and its underlying principles, to an analysis of the bills currently before the Committee.

Section One – A Framework

Balance and Perspective: A Path to Effective Solutions

8. It is easy to argue that security necessarily comes at a cost to liberty. That is, we can only enjoy the right to feel safe and secure if we forgo certain other rights, such as the right to privacy. This is not necessarily the case. It is possible for people to have both privacy and security and they expect their parliament to provide them with both. For example, in the biometrics field, some airports are considering introducing body scanning technology that will help security staff identify hidden firearms and other devices. One version of this technology, being used in the USA, is a privacy invasive technique that scans a person and shows an image of each traveller's naked body in some detail on a computer screen. A privacy respecting version of the same technique is available that simply indicates to an officer the vicinity in which there may be a concealed weapon, without displaying the individual's naked body. The first technique is privacy invasive, while the second technique, which achieves the same outcome, is less so.[i]

9. Admittedly, it is not always as simple as this in practice and there will be times when the only solution available to legislators involves a diminishment of our privacy and other rights. Such approaches, however, should always be the measure of last resort, used only after other options have been identified and rejected.

10. The challenge, then, is to find a fair and useful means of considering, weighing and making judgements about the seemingly competing priorities involved in a debate such as this. Identifying the parameters and community values is the key to determining how to address our need for security, while respecting privacy and having regard for other individual freedoms. This section outlines a framework that could prove useful in moving our community's deliberations forward in this area.

11. Arguably, the current challenges before our community and this Parliament are not new. Others before us have struggled with responses to threats of terrorism

against their states and nations, with ranging degrees of success. Justice Kirby, in an address to the 32nd Australian Legal Convention[ii] in Canberra only a month after the events of 11 September 2001, offered an account of history in this regard. He reminded us of the terrorist challenges faced by Uruguay, Italy and Germany to name but a few.[iii] Justice Kirby, however, also offered salient guidance about the more successful approaches to such a challenge, including keeping our perspective, analysing the threat and responding in proportion to what we find.

12. Justice Kirby further cautioned that sometimes "it is wise to pause", for "[the] countries that have done best against terrorism are those that have kept their cool, retained a sense of proportion, questioned and addressed the causes".[iv] It is now more than six months since the events in the USA. Commendably, we in Australia have taken time to begin to think about how we might respond, about what those threats mean to our country and to our choices for how we live. The issues are complex and demand careful, balanced consideration – they are matters, which for all of us, are worth taking the time to get right.

13. Before considering the framework in more detail, there is a little more to say on perspective. Determining what our Australian perspective might be is a multi-faceted task. We need to try to consider the issue in both the shorter and the longer terms. For example, does the degree and type of threat we feel today differ from that which existed in the days and weeks after 11 September 2001; if so, how and why? Will the way we assess the issues today differ in the future? If we are uncertain, what does this say about the purported permanency of any measures put in legislation in the coming months? How do we weigh the risks and benefits of taking steps against a threat we may know today, but that may not be present in the future? If the measures remain, they may remain open to use for other purposes – what do we do to avoid 'function creep'?

14. Often the best way to strike a good balance is to ensure there is ample public debate on the issues and that such debate is conducted in an open and transparent manner. Our search for perspective may be influenced also by our geographic location, our history and our cultural response to threats of the current kind. Is the nature of the threat and the proposed resultant change to things (such as the protection of our personal information) the same for us as for other nations; if not, why not? We should reflect on the proportionality of any proposed response, and in ways congruent with our perspective on world events.

15. The framework outlined here for considering new legislative responses that have a major impact on the community, by giving law enforcement agencies more intrusive powers, was first explored at the Australian Institute of Criminology's conference in June 2001. Broader discussion can be found in the paper 'Preserving Privacy in a Rapidly Changing Environment'[v] (this paper is attached to the submission, also available online at www.privacy.gov.au/news/speeches/sp34note.doc). Critique of this framework has been sought in a number of forums, with a view to either improving it or replacing it with a better framework. So far though, the framework has attracted little criticism.

16. Further consideration and deliberation of security and privacy issues over recent months suggest the framework applies to matters not only about developments

in domestic law enforcement, but also to those about broader safety and security in civilian society.

17. Essentially, the framework intends to bring about balance and perspective to considerations of legislative proposals with significant effects on privacy. It does so by leading us through seven key steps, including: defining the nature of the problem and the scope of possible responses to it; thinking about how new powers might be enacted; considering what the transparency, accountability and reporting requirements should be; and ensuring review of the mechanisms after a suitable period.

The Framework

Key step	Things to consider, including:
Identify the problem	✓ Size & scope of the problem ✓ Likely longevity ✓ Implications in the Australian context
Identify the range of possible solutions	✓ The range of responses open to us ✓ Resource implications of these options ✓ Efficacy issues – which option/s will work best and not unduly affect people's lives?
Think carefully and clearly about the proposed solution	✓ What is the impact on privacy, and on whose privacy? ✓ Will the solution work and will it meet its target? ✓ What are the community's values here? ✓ Proportionality – is the measure proportional to the known risk?
What does the community think?	✓ What consultation or debate has occurred? ✓ What does it tell us?
Implementing the new powers	✓ Confer intrusive powers expressly in law (via an Act, not subordinate legislation) ✓ Legislation to state, expressly and objectively, the grounds on which the powers may be used ✓ Authority to exercise powers to rest at an appropriate level – to be expressly stated in legislation
Need to ensure transparency, accountability and reporting	✓ Make sure the community is kept informed about use of the powers ✓ Ensure a transparent and independent complaints-handling system, monitoring system and the powers of independent audit ✓ Include an independent and public assessment and reporting process for the operation of the measures ✓ Ensure reporting and oversight powers are commensurate with the intrusiveness of the measures ✓ Preferably spell out these arrangements in legislation, especially where the new powers are particularly intrusive
Review processes	✓ Parliamentary review of the measures after a fixed period – identify operational successes, as well as unintended or undesirable consequences ✓ Modify or remove powers as needed ✓ Include a 'sunset clause' – it is wise to pause and think again.

18. The latter two steps (outlined in the table above), reflect a vital process in ensuring that what we aim for in constructing anti-terrorism measures is just what we deliver. Not only this, but individuals have a reasonable right of complaint and should have available the option of redress by an independent body. The community expects to be told about how the use of these measures is progressing with regard to their effects upon the use of personal information.[vi] These steps, supplemented by the assurance that necessary monitoring and auditing maintains an effective and proportional overview of the measures, go far in maintaining community confidence that potentially intrusive actions are minimised, justified, exercised accountably and that they are reviewed.

19. Finally, building in a review of the measures helps guard against 'function creep' at a later date or the otherwise unnecessary retention of powers that risk losing their necessity as circumstances change. Two practical ways of achieving this outcome are to build into the legislation a trigger for parliamentary review, perhaps involving an assessment and report to that review by an independent body, or alternatively (and arguably more effectively) to insert a 'sunset clause' into the legislation. The latter step means that the law will lapse, so the parliament must look again at the circumstances and consider anew whether that which influenced the measures in the past, remains a consideration in the present. If so, further legislation would need to be passed.

20. It is in the context of seeking a truly proportional and appropriate response that this approach to considering the current anti-terrorism bills is presented. If "every erosion of liberty must be thoroughly justified"[vii], calm reflection will help to ensure the steps we are about to take are wise, effective, commensurate with the problems before us, open to appropriate scrutiny and likely to last for as long, or as short, a period as they are needed.

Section Two – Analysis of the Bills

Definition of *Terrorism*

21. One of the most difficult issues in considering anti-terrorism legislation is the problem of defining *terrorism* and subsequently deciding what categories of offences constitute a terrorist act. No comprehensive definition has emerged in the international arena that is not also sweeping in scope.

22. In most cases it appears that *terrorism* is an event driven term. That is, it is defined in immediate response to a specific action or threat of action. The dangers of so doing have been highlighted internationally where terrorism has been defined in such ways as to allow governments to advance political agendas or justify improper action to varying degrees. Concern followed the introduction in the early-1970s, within the UK and Northern Ireland, of internment without trial measures for suspected Irish republican terrorist activity. These powers were followed by the UK *Prevention of Terrorism (Temporary Provisions) Act* in 1974. In retrospect, questions have arisen about the effectiveness of these kinds of measures.[viii] For instance, in the

first 8 years of operation (to the end of 1982) of the 5500 people detained under these provisions, less than 2% were charged with any offence. [ix]

23. *Terrorism* is a term that evokes an emotive response from most people (particularly given recent world events). In people's minds it is an offence of the highest order and one where the penalties need to be most severe.

24. These bills would establish the broad offence of *terrorism* under the Criminal Code and in doing so authorise law enforcement and other agencies to collect, use and disclose personal information in ways not otherwise permitted under existing legislation. For example, the *Telecommunications Interception Legislation Amendment Bill 2002* places terrorism-related offences in the same category as serious arson offences (which are serious but well defined offences), thus ensuring the availability of telecommunications interception as an investigative tool with regard to these offences.

25. In this case, the term *terrorism*, which may encompass a wide range of offences, will need to include offences of such significant magnitude to justify interception while at the same time excluding offences of lesser harm or significance. If the definition of *terrorism* in these bills includes offences that might otherwise be regarded as minor (or less severe in nature than serious arson for example), then it is possible the privacy rights of individuals will be unduly infringed during an investigation.

26. It is vital that we get this step right in building a balanced and proportional legislative response to the threat of *terrorism*. The struggle to achieve a workable and yet proportional definition in this area is not new[x], but it is essential that necessary care be taken to ensure the definition is carefully cast. The importance is such that the definition is one of the core elements that future Parliaments will need to consider when reviewing this legislation, both because experience may show where the definition has not worked as intended (especially if it has been cast too widely) and because the threat of *terrorism* as envisaged may have declined.

27. It is **recommended** that the Committee further consider the proposed definition of *terrorism*, giving further thought to this country's limited history with the types of offence usually considered as constituting a *terrorist* act.

Security Legislation Amendment (Terrorism) Bill 2002

28. This Bill seeks to amend the Criminal Code by defining *terrorism* and *terrorist act* and describing offences in relation to such acts, for example, being a member of a *terrorist* organisation.

29. A quick analysis of this Bill does not appear to raise any significant privacy matters on which it would be necessary to comment at this stage. It is **recommended**, however, that the Committee consider this Bill and its interaction with the Criminal Code and other legislation in light of the above framework and good privacy practice.

30. It is **recommended** that the Committee give close consideration to the definitions of *terrorism* and *terrorist act* as defined in this Bill, in light of the issues discussed above.

Suppression of the Financing of Terrorism Bill 2002

31. This Bill seeks to create a number of offences relating to the financing of *terrorist* organisations and activities. It enables Commonwealth officers to collect, use and disclose an individual's financial transaction reports and other forms of personal information.

Reasonable grounds

32. The Privacy Act sets strict rules with regard to the disclosure of personal information to third parties. One reason for this is that limiting disclosure helps to ensure that individuals retain some control over their personal information by being aware of how it is handled and who has access to it.

33. The Privacy Act sets out 11 Information Privacy Principles (IPPs) that govern the way Commonwealth Government agencies (and their outsourced providers) collect, use, disclose and handle personal information. The principles also give individuals the right to gain access to information held about them and they oblige agencies to correct information if it is inaccurate. In a similar way, many private sector organisations are governed by the National Privacy Principles (NPPs) as set out in Schedule 3 of the Privacy Act.

34. There are exceptions under both the IPPs and the NPPs that allow disclosure to occur when it is 'required or authorised by law'. The decision to set down a law that would require or authorise such a disclosure, however, should not be taken lightly. Such actions, *prima facie*, detract from the spirit of the Privacy Act. While it is acknowledged that there is a need for governments to combat terrorism, they must also be concerned to ensure that their citizens' personal information is only disclosed when this is absolutely necessary.

35. The concept of 'reasonable grounds', as cited in this Bill, has the potential to be interpreted broadly. It is quite possible that, in the future, broad interpretation will lead agencies and organisations to disclose personal information that was never intended to be disclosed in this way. For example, section 16(1A) of the proposed amendments would require cash dealers, with *reasonable grounds* to suspect that

(i). a transaction is preparatory to the commission of a financing of terrorism offence; or

(ii). information the cash dealer has concerning the transaction may be relevant to the investigation of, or prosecution of a person for a financing of terrorism offence,

to prepare a report of the transaction and communicate the information contained in that report to the Director of AUSTRAC.

36. In this situation, a cash dealer may suspect a transaction purely on the grounds that the subject fits a generic profile of a potential suspect. This type of behaviour

could lead to disclosures of personal information that unduly interfere with the privacy rights of individuals.

37. It is preferable that the legislation makes explicit exactly what sort of personal information may be disclosed and under exactly what circumstances this can be done. It is **recommended**, however, that if disclosures are to be based on the concept of 'reasonable grounds', there should be tight accountability measures in place to ensure that personal information is disclosed only when necessary, that reports are made in de-identified form wherever possible, and that these provisions are reviewed in the future to determine whether they are being misused or misunderstood. This recommendation is consistent with the framework outlined in Section One of this submission.

Disclosure of personal information overseas

38. Technological advances make it ever easier for governments and the private sector to collect, store, and manipulate personal information. It has also become more profitable to use and disclose such information for purposes other than those for which it was collected. This is where data protection rules (such as the IPPs and NPPs under the Privacy Act) play an increasingly important role in protecting the privacy rights of individuals.

39. Some countries now have laws that prohibit organisations from transferring information to other countries that do not have equivalent privacy protection for personal information. A number of other countries are responding in turn, by developing or enhancing their own privacy regimes. For example, in Australia the recently introduced NPPs have begun to regulate private sector disclosures overseas.

40. When data is transferred out of Australia, there is the potential for its misuse by foreign recipients, while individuals and the Commonwealth Government are limited in their ability to take action in response to such misuse. It is in this context that the Committee is **recommended** to seek the limitation of the disclosure of personal information overseas to: a) countries with similar privacy protections as Australia, or b) situations where the disclosing agency has entered into an enforceable agreement with the foreign government, to ensure that the information is used only for the purposes for which it was released from Australia. An agreement in the latter case should also ensure that the overseas entity takes all reasonable steps to protect the information from unauthorised access, modification and disclosure.

41. In short, the legislation should provide for agencies to ensure that foreign governments and their law enforcement agencies are bound by equivalent standards for handling personal information as would be the case under Australian law.

Review of effectiveness of amendments

42. Including a review of these provisions will allow the Parliament to assess whether they are working effectively and as intended. It is encouraging to see that there are some provisions for review in the current Bill. The provisions that allow for the Privacy Commissioner to be involved in this process are also welcome.

43. If the findings of the respective reviews, however, identify unintended or undesirable consequences resulting from inadequacies in the legislation, then it is **recommended** the Parliament be required under the legislation to take steps to rectify the problems. As it stands, there does not appear to be any obligation on the Parliament to adopt the recommendations of the review panel or even to consider them.

44. The proposed amendments provide a necessary and urgent response to current world events. While the threat of terrorism may decline in coming years, its monument may be a 'surveillance society'. Therefore, in addition to the above recommendation, it is also **recommended** that the Committee seek the inclusion in the legislation of a sunset clause of four years. That is, after four years, the legislation would lapse and Parliament would have to reassess the need for these measures, passing further legislation if necessary.

Criminal Code Amendment (Suppression of Terrorist Bombing) Bill 2002

45. This Bill seeks to create offences relating to international *terrorist* activities with respect to *terrorist* attacks using bombs and other lethal devices and gives effect to the *International Convention for the Suppression of Terrorist Bombings.*

46. A quick analysis of this Bill does not appear to raise any significant privacy matters on which it would be desirable to comment at this stage. It is **recommended**, however, that the Committee consider this Bill and its interaction with the Criminal Code and other legislation in light of the above framework and good privacy practice.

Border Security Legislation Amendment Bill 2002

47. This Bill seeks to introduce provisions that would affect the handling of personal information by private sector companies (including, employers at air and sea ports and the operators of air and shipping lines); and government agencies, in particular the Australian Customs Service (Customs) and the Department of Immigration and Multicultural and Indigenous Affairs (DIMIA). The provisions would affect the handling of personal information for individuals entering Australian borders and those being employed at entry points to Australia. The acts and practices that this Bill seeks to make lawful might otherwise be inconsistent with the provisions of the Privacy Act if not for the 'required or authorised by law' exceptions made available under the IPPs and NPPs.

48. At a broad level, it is necessary to consider whether this proposed legislation is appropriate to the social context in which it will function, both in the present and in the future. Accordingly, future review of the legislation would seem an imperative. A review should include an examination of the impact of any unintended or undesirable consequences, such as 'function creep', as well as re-evaluating whether

the measures implemented are necessary, suitable and proportionate to any risks or challenges that may exist at the time. It is **recommended** that the legislation include a sunset clause for these provisions, such that they lapse after a set period, unless Parliament considers it necessary to pass further such legislation.

49. In addition to these broad comments, this Office provides the following, specific comments in relation to this Bill.

An Individual's 'Right to Know'

50. Giving individuals a right to privacy includes ensuring that they are aware of what personal information is being collected about them, who holds this information, and for what purposes it will be used. These are the themes advocated by the Privacy Act as well as the various international directives and guidelines that have influenced the contemporary understanding of privacy as a fundamental human right.

51. There are various provisions in this Bill that would provide agencies, such as Customs, with a lawful purpose for collecting personal information. These provisions, however, should not be interpreted as a means of undermining the general principle that individuals have a right to know what is happening with their personal information, unless there are specific, limited and reviewable reasons why such actions should remain covert.

52. One example in the proposed legislation, where there appears to be an undermining of an individual's right to know, involves agencies collecting personal information about people working in restricted areas.

53. The Privacy Act exempts certain organisations and activities from its coverage. One of the exemptions involves information handling activities directly related to a private sector employment relationship. Therefore, there appears to be no obligation on the employer or the agency to inform the individual that their personal information is being collected and disclosed, since this is not required under the Privacy Act or the proposed legislation.

54. In order to address this concern, it is **recommended** that the Committee seek that the proposed legislation be amended to ensure individuals (in this case employees working in restricted areas) are made aware by agencies that their information is being collected, how it is likely to be used and to whom it is likely to be disclosed.

Ensuring Accountability of Decision Making

55. When legislation allows an individual's privacy rights to be eroded, adequate accountability measures must be implemented in order to ensure that privacy rights are not further and unnecessarily diminished. Currently, there are provisions in the Bill that do not appear to be supported by adequate accountability mechanisms or procedures.

56. The provision in s*ubdivision HA, section 213A(3*), allowing an authorised person to require disclosure of an individual's personal information on the basis that

they suspect, on *reasonable grounds*, that the individual has committed, or is likely to commit, a breach of Commonwealth law, introduces a degree of subjective interpretation that is inconsistent with the above framework and good privacy practice. The notion of *reasonable grounds*, here, may be abused if interpreted too loosely and with inadequate justification, scrutiny or backing.

57. Further, determining on *reasonable grounds* whether an individual is *likely to commit* an offence against Commonwealth law would seem greatly problematic, as it seeks to make presumptions about an individual's motives or intentions. An approach based on such a test of *reasonable grounds* would have to be subject to strong accountability and transparency arrangements.

58. There are also various provisions contained in the Bill that would appear to grant considerable discretion to *authorised officers* of government agencies to make decisions that may progressively expand the acts and practices related to the Bill. For example, *Schedule 6, section 64ACA(2)* provides for the CEO to approve various methods for the transmission of personal information. Similarly, *Schedule 6, sections 64ACA(9)* and *64ACB(7)* grant the CEO with unilateral authority to change the forms with which personal information is provided to Customs, and accordingly the type of personal information that will be collected for inclusion in these forms.[xi] Accordingly, this provision could facilitate the broadening of the types of personal information collected – it leaves an agency with the discretion that might accompany a blank cheque.

59. A further example of the provision of unilateral authority is contained in *Schedule 7, section 64AF(1)(a),* whereby the CEO can request that an operator provide Customs with access to that operator's customer information on an on-going basis. This section effectively seems to provide an instrument for on-going surveillance of an operator's database in a form that may not be compatible with the above framework or good privacy practice. Such extreme measures should only be enacted where appropriate safeguards and accountability procedures are in place.

60. The above examples highlight provisions in the proposed legislation that include loosely defined terms and unilateral decision making powers. Such unilateral authority seems difficult to reconcile with the principles of accountability and transparency. There appear to be few, if any, safeguards to prevent the erosion of privacy standards to a point not currently envisaged in the proposed Bill. Further, the Bill offers no guidance about how decisions may be made or what criteria should be used.

61. In this regard, it is **recommended** that the legislation include instruments which better promote accountability and transparency consistent with the framework outlined above, especially in covering gaps where provisions that are not currently subject to scrutiny under the Privacy Act. These instruments can be separated into those that come into play before the event occurs, such as provisions about the authorisation to act (eg. an officer requiring authorisation from a senior officer, CEO or Minister before proceeding) or those that operate *ex-post* such as auditing provisions or an independent complaints-handling mechanism.

62. Such instruments might also include listing in the legislation the specific categories of personal information that may be collected by *authorised officers* or via forms, listing matters that *authorised officers* must have regard to (including the privacy rights of individuals) when making decisions and handling personal information, and the provision for appropriate Ministerial and Parliamentary oversight through the review of these measures.

63. Against this background, if Parliament wishes to proceed with this Bill largely in its present form, then it is **recommended** the legislation contain a sunset clause with regard to the most privacy invasive provisions. At this point, the legislation would lapse, unless Parliament sees fit to pass further legislation at that time.

Recurrent Obligations of the Privacy Act 1988

64. As already established, the effect of many of these proposed amendments will be to satisfy exceptions to the IPPs and NPPs, such that personal information can be collected, used and disclosed on the basis that such practices are 'required or authorised by law'.

65. It is important to recognise, however, that the proposed legislation does not have the effect of limiting the application of any other obligations contained in the Privacy Act, neither does it function to provide agencies with immunity from meeting such obligations. Agencies retain ultimate responsibility for ensuring that information collected is relevant to the purpose of collection and that it is up-to-date and complete. Such responsibilities are required by the IPPs, and expected by standards of good privacy practice.

66. Further, the obligations imposed on record keepers by IPPs 5, 6 and 7, which provide the individual with access to their personal information and ensure the accuracy of such information, may still apply. These obligations remain unless limited by Commonwealth laws which specifically release agencies from them – although there does not seem to be anything in the current Bill that serves such a restrictive purpose.

67. The concern here is that there appears to be significant potential for agencies to act beyond the policy intent of the provisions (in their handling of personal information) and for officers to test the barriers of their legal powers. This is always a potential when legislation is broad in its application. Moreover, there are unlikely to be many complaints associated with the handling of personal information under the proposed legislation, given the largely covert nature of its operation.

68. An example of particular concern involves the various references to the exchange of personal information between third parties and government agencies. In particular, the transmission of personal information as discussed in: *Schedule 6 section 64ACA(1)* through *(9); Schedule 6 section 64ACB(1)* through *(7); Schedule 6 64ACE(1)* and *(2); Schedule section 245J(1)* through *(4).*

69. Security and proper storage of personal information by agencies is essential in maintaining the integrity of data and in ensuring an individual's privacy is not

breached once they have disclosed their personal information. Similar expectations are held for organisations, such as private sector airlines and shipping companies.

70. The proposed legislation does not seem to set out any levels of protection for data, beyond an agency's current obligations under the Privacy Act. Indeed, the Bill even advocates granting to Customs the right to approve various electronic systems to transmit data. The unilateral and internal setting of data security standards does not appear to lead to a very transparent or accountable system.

71. In circumstances such as these, where such significant powers are created and used covertly, this Office will carry particularly clear obligations in ensuring the transparent and accountable discharge of these powers. This raises problems for the Office as these steps are likely to require a large commitment of resources (which currently are unavailable), for channelling into the auditing and monitoring of the proposed new powers and their subsequent systems.

72. The Office has not been provided with any additional resources, however, and these additional obligations come at a time when the Office is already diverting resources to meet the unexpectedly high workload arising from the *Privacy Amendment (Private Sector) Act 2000*. If these resources are not provided to the Office, it is **recommended** that the Committee further consider how necessary accountability measures might be incorporated into the legislation.

73. Furthermore, it is **recommended** that the Committee seek the inclusion in the legislation of a sunset clause of four years, such that the legislation would lapse after that time. Parliament would then have to reassess the need for such measures, passing further legislation if necessary.

Telecommunications Interception Legislation Amendment Bill 2002

74. The primary objective of the *Telecommunications (Interception) Act 1979* (the Interception Act) is to protect the privacy of individuals who use the Australian telecommunications system. The Interception Act does this by making it an offence to intercept communications passing over the system, while also balancing this with the Parliament's and the broader community's law enforcement and national security interests. The Interception Act specifies the circumstances in which it is lawful for law enforcement agencies and the Australian Security Intelligence Organisation (ASIO) to intercept communications under the authority of a warrant, subject to reporting and accountability mechanisms.

75. For most of the 20th century it has been a fundamental tenet of Western democracy that direct, personal conversations and phone conversations should not be intercepted, except under tightly controlled and extremely limited circumstances. The privacy provisions that this Bill defends, in a general sense, are welcome. It is not clear, however, whether the proposed amendments will provide the clarity that is necessary to ensure that adequate privacy protection is extended to all levels of telecommunications interception.

76. The Attorney-General, in his second reading speech, stated that "[t]he amendments make clear that a communication will fall outside the definition of interception where it is stored on equipment and can be accessed using that equipment but without reference to the telecommunications network. In these circumstances agencies will be able to access the communications pursuant to other appropriate means of lawful access, such as a search warrant authorising the operation of the equipment. These amendments reflect a much needed clarification, and will assist agencies in the performance of their functions".

77. The proposed additions to section 6 of the Interception Act will define *delayed access message service* and a *stored communication* and state that stored communications will no longer pass over a telecommunications system when they have been accessed. Thus, it appears that these amendments will essentially remove stored communications, such as emails and Short Message Service (SMS) messages, from the protections afforded to other types of telecommunication. These amendments, however, remain ambiguous, particularly in relation to whether emails that are in transit and stored on an ISP's server can be accessed only after having obtained a warrant issued under the Interception Act.

78. Beyond this ambiguity, all forms of telecommunication should, where practicable, be afforded an equivalent level of privacy protection.

79. Evolving technologies have lead to a substantial increase in the use of stored communications, such as SMS messaging and email, in Australia. Reading someone's stored communications is just as intrusive as intercepting a voice communication and should be subject to an equivalent level of privacy protection, and certainly a greater level of protection than would be afforded under the *Telecommunications Act 1997*. There seems to be little justification for reducing the privacy protection of a communication as intimate as a voice mail message or SMS, in comparison with a 'live communication' simply because the transmission of the former is temporarily delayed.

80. It is **recommended** that the Committee take up the discrepancy in privacy protection for stored communications and consider whether equivalent privacy protections would be appropriate for these types of communications. If a difference is to be retained, then the transparency and accountability of the use of such powers need improvement. The intrusive nature of these provisions again suggests they should be subject to a sunset clause such as that set out in para. 43.

Conclusion

81. The following is a summary of the recommendations and issues raised in the body of this submission.

82. It is recognised that privacy is not an absolute right, and that privacy interests must be balanced with other valid, and sometimes competing, public interests. The challenge facing Parliament in this current raft of anti-terrorism bills is how to achieve a balance between privacy and security, particularly in situations where the two are opposed.

83. The framework outlined in Section One of this submission may provide guidance towards establishing a balance between privacy and security. This framework suggests that the introduction of potentially privacy invasive measures requires society to be reasoned in its forethought, and vigilant in its oversight, so as to ensure that an appropriate balance is met between interests. Applying such a framework leads to the following, privacy-related, **recommendations**:

i. At a number of points, the proposed legislation contains provisions, which invest significant degrees of unilateral authority in individuals with no corresponding guidance about how this authority should be executed, or what criteria ought to be used for decision making. Such unilateral authority seems difficult to reconcile with the principles of accountability and transparency. The legislation should expressly and objectively state the grounds on which the powers may be used, including the facility for the review of decision making.

ii. The use, in various bills, of a test of 'reasonable grounds' to govern the handling of personal information is one matter of concern. Such a subjective criterion may increase the likelihood of 'function creep', resulting in an outcome not intended by the proposed legislation. This can be avoided by specifically listing the grounds on which information can be collected, used and disclosed.

iii. While the threat of terrorism may decline in coming years, its monument may be a 'surveillance society'. To guard against such an outcome, a transparent monitoring, review and audit process should be introduced to accompany these bills. The inclusion of 'sunset clauses' in the proposed legislation warrants close consideration where privacy is likely to be greatly affected. Such a clause would result in the relevant provision lapsing after a given period. Thereafter, Parliament would need to pass further legislation if the circumstances were to warrant it.

iv. The discrepancy in the *Telecommunications Interception Legislation Amendment Bill 2002*, regarding the differing privacy protection afforded to 'stored communications' when compared with more immediate 'live communications', must be addressed. Equivalent privacy protection, as afforded to other telecommunications, should be extended to stored communications.

v. The disclosure of personal information overseas should be limited to: a) countries with similar privacy protections to Australia; or b) where the disclosing agency has entered into an enforceable agreement with the foreign government,

to ensure that the information is protected as it would be in Australia and used only for the purposes for which it was released from Australia.

vi. These bills should not be interpreted as a providing a means for undermining the general principle that individuals have a right to know what will, or may, happen to their personal information, including for what purposes it will be used and to whom it may be disclosed. Agencies should be compelled to ensure that individuals are aware that their personal information may be disclosed to those agencies, as well as ensuring they are made aware of the purposes for which this personal information may be used, unless there are clear (and adequately accountable) grounds for justifying covert operations.

---

[i] Example used by Ann Cavoukian, Ph.D. Information and Privacy Commissioner of Ontario. Further reference available at: www.ipc.on.ca/english/pubpres/ext-pub/steps.htm

[ii] Kirby, J., 'Australian Law – after September 11, 2001', paper presented to the 32nd Australian Legal Convention in Canberra on 11 October 2001, which can be found at: www.highcourt.gov.au/speeches/kirbyj/kirbyj_after11sep01.htm

[iii] Op cit., pp. 4-5

[iv] Op. cit., pp. 6-7

[v] Office of the Federal Privacy Commissioner, 'Preserving Privacy in a Rapidly Changing Environment', paper presented at the Australian Institute of Criminology Conference called 'Future Directions, Crime Prevention, Legal Responses and Policy' on 22 June 2001 (COPY ATTACHED and available online at www.privacy.gov.au/news/speeches/sp34note.doc).

[vi] OFPC Research 'Privacy and the Community' (Approx. 90% of those surveyed wanted to know what information about them was being collected and for what purposes it was being used.) The research is available at: www.privacy.gov.au/publications/rcommunity.html

[vii] Kirby, J., op. cit., p. 7

[viii] Northern Ireland Human Rights Commission's 'Response to The White Paper Legislation Against Terrorism', April 1999

[ix] Hocking, J., Beyond Terrorism: the development of the Australian security state, (Allen & Unwin, Sydney, 1993), p. 24

[x] Northern Ireland Human Rights Commission, and Hocking, J., op. cit.

[xi] Schedule 6 Sections 64ACA(7)(c) and 64ACB(5)(c) require that the report given to Customs "contain such information as is required by the form".

Attachment 2

Office of the Federal Privacy Commissioner

Framework for assessing and implementing new law enforcement and national security powers

The Office of the Federal Privacy Commissioner has developed a proposed framework for assessing and implementing new law enforcement and national security powers. The framework was first outlined in a paper for the Australian Institute of Criminology's conference in June 2001[xi] and again in a submission to the Senate Legal and Constitutional Committee in April 2002 on proposed anti-terrorism legislation[xi].

The framework sets out a life cycle approach to such proposals from development to implementation and review. The aim of the framework is to bring balance and perspective to the assessment of proposals for law enforcement or national security measures with significant effects on privacy.

First, careful analysis is needed in the development phase to ensure that the proposed measure is necessary, effective, proportional, the least privacy invasive option and consistent with community expectations. This analysis should involve consideration of the size, scope and likely longevity of the problem, as well as the range of possible solutions, including less privacy invasive alternatives. The impact on privacy of the proposed solution should be analysed and critical consideration given to whether the measure is proportional to the risk.

Second, the authority by which the measure is implemented should be appropriate to its privacy implications. Where there is likely to be a significant impact on privacy, the power should be conferred expressly by statute subject to objective criteria. Generally, the authority to exercise intrusive powers should be dependent on special judicial authorisation. Intrusive activities should be authorised by an appropriately senior officer.

Third, implementation of the measure should be transparent and ensure accountability. Accountability processes should include independent complaint handling, monitoring, independent audit, and reporting and oversight powers commensurate with the intrusiveness of the measures.

Finally, there should be periodic appraisal of the measure to assess costs and benefits. Measures that are no longer necessary should be removed and unintended or undesirable consequences rectified. Mechanisms to ensure such periodic review should be built into the development of the measure. This could involve a sunset clause or parliamentary review after a fixed period.

In summary:

Analysis – is there a problem? Is the solution proportional to the problem? Is it the least privacy invasive solution to the problem? Is it in line with community expectations?

Authority – Under what circumstances will the organisation be able to exercise its powers and who will authorise their use?

Accountability – What are the safeguards? Who is auditing the system? How are complaints handled? Are the reporting mechanisms adequate? And how is the system working?

Appraisal – Are there built in review mechanisms? Has the measure delivered what it promised and at what cost and benefit?