Australian
Privacy
Foundation

http://www.privacy.org.au

Secretary@privacy.org.au

http://www.privacy.org.au/About/Contacts.html

20 August 2012

Hon Anthony Byrne MP
Chair
Joint Parliamentary Committee on Intelligence and Security
Parliament House
Canberra ACT 2600

Dear Mr Byrne

Re: Inquiry into Potential Reforms of National Security Legislation

We attach our Submission to the above Inquiry.

Thank you for your consideration.

Yours sincerely

Roger Clarke
Chair, for the Board of the Australian Privacy Foundation
(02) 6288 1472 Chair@privacy.org.au

Australian Privacy Foundation

SUBMISSION

Inquiry into Potential Reforms of National Security Legislation

20 August 2012

CONTENTS

Contents

EXECUTIVE SUMMARY

The belated exposure for comment of an overall government 'wish-list' for legislative changes in this area is welcome, and stands in stark contrast to the years of secretive consultation with selected stakeholders.

However, the timescale allowed for comment on these very significant proposals is completely inadequate, as is the level of detail provided. The Committee should decline to comment on the substance of the proposals, and invite the government to bring back more detailed proposals, after a more extensive process of consultation with all interested parties.

While some modernisation and streamlining of the interception and access to communications regime are desirable, too many of the proposals outlined in the Discussion Paper would herald a major and unacceptable increase in the powers of law enforcement and national security agencies to intrude into the lives of all Australians.

The case for changes in the powers to access communications needs to be balanced by an equally well informed debate about the appropriate balance, in a free and democratic society, between law enforcement capabilities and privacy and civil liberties. This debate must not take the status quo as a given, as too many of the existing powers and associated processes have been enacted incrementally without the benefit of such a contextual debate. There is for example a strong case for greater consistency in the authorization requirements for access to different forms of communications, but by leveling up to the highest current standards, not leveling down to the lower standards that have crept in, in recent years, in relation to some categories of information.

Some of the more specific proposals are clearly unacceptable, while others may be acceptable with additional safeguards and conditions. Many of the proposals offend against benchmark principles of justification and proportionality – it is not clear that the asserted public benefit outweighs the substantial loss of privacy and freedom that would be involved.

Another main underlying problem with the proposals is that they involve a further extension of the already undesirable level of 'co-option' of the private sector as agents of government, with associated cost shifting. Specifically, the sketchily outlined proposal for a general data retention requirement is not adequately justified, and is in its current form unacceptable even in principle.

The Discussion Paper does not adequately address the international context . There are advanced discussions in many international fora, such as the OECD, about the appropriate balance between various public and private interests in the regulation of telecommunications and the internet economy. These proposals also need to take much greater account of other relevant government policy, and specifically involve the Department of Broadband, Communications and the Digital Economy to represent a different perspective and other public interests.

Australian Privacy Foundation

SUBMISSION

Inquiry into Potential Reforms of National Security Legislation

20 August 2012

1. Introduction

The Australian Privacy Foundation (APF) is the country's leading privacy advocacy organisation. A single page background paper is attached (Annex 1).

1.1 Previous submissions

We note that the Australian Privacy Foundation has made numerous previous submissions on related inquiries and legislation, including on most of the Bills amending the telecommunications interception and access regime over the last decade. These submissions are all online at http://www.privacy.org.au/Papers/indexPolicies.html#TelecommsIA

1.2 Structure of this submission

We firstly address, in Section 2, some general contextual issues. Then in Section 3 we draw attention to some major weaknesses and dangers of the proposals. In section 4 we acknowledge some proposals which might be acceptable, subject to further clarification and safeguards. Finally, in Section 5, we draw attention to some serious procedural failures in the way in which these proposals have been developed and presented, including major inadequacies in the consultation processes.

2. General Comments

Prior to performing an evaluation of a proposal, particularly a proposal of such a wide-ranging and troubling nature, it is essential that a framework for the evaluation process be established.

2.1 Recognition of Technological Change

The APF agrees with the AGD's general contention that substantial changes have occurred in the context of telecommunications since the Telecommunications Interception regime was conceived. We contend, however, that some of the precepts that AGD claims the current interception regime is based on were not appropriate even in the 1960s, and that the changes have accumulated over a long period rather than happening suddenly. In particular, it was never true that there was a "clear, one-to-one relationship between the target of an interception warrant [and] telecommunication services used by the person ..." (p.21).

We also note that the current regime is not entirely historic or outdated –the telecommunications interception and access regime, both under the TIAA and the ASIO Act have been amended many times in the last decade, mostly significantly increasing powers and decreasing safeguards, without adequate debate of the underlying balance of public policy.

The Discussion Paper presents a 'wish-list' of further legislative changes which national security and law enforcement agencies contend are necessary to address contemporary threats. It is at least welcome to see drawn together a number of separate threads that have to date been presented either separately or not at all, having been progressed in largely secret consultations (see section 5 for our concerns about process issues). But this overdue presentation of an overall context for possible reform now requires much lengthier and more substantial public debate than is allowed for in the government's current policy development timetable and processes.

In the context of technological change, we also take the opportunity to point out that the entire regime for access and interception of communications has been developed without sufficient regard for 'equivalence' across different modes of communication. Some of the existing powers in relation to telecommunications would be rejected by the community if government attempted to apply them to postal traffic. The Committee, like the wider community, should regularly apply a 'what if' equivalence test when considering the appropriateness of any ambit claims for further powers.

2.2 Foundation Principles

The APF supports the need for law enforcement and national security agencies to have appropriate capacity and tools to conduct investigations into crime, and into genuine threats to the security of Australia and Australians.

However, all powers granted to government agencies create threats to the very freedoms that the agencies are supposed to be protecting. The massive increase in powers granted since 2001 have dramatically altered the balance, and created a real prospect of an un-free society dominated by powerful government agencies utilising technology in order to conduct mass surveillance. In relation to this wider context, we draw attention to several recent analyses of regulatory responses to the perceived threat of terrorism (Annex 2)

On the other hand, privacy is a fundamental human right, and is critical to the social, economic and political functioning of a free society. Privacy must therefore be constrained only where it is demonstrated that the constraint is necessary in order to satisfy a more important public interest. Any discretion exercised when implementing the restrictions must not be unfettered. Restrictive measures must also conform to the principle of proportionality: they must be appropriate to achieve their protective function; they must be the least intrusive instruments amongst those, which might achieve the desired result; and they must be proportionate to the interest to be protected.

Arguably the most invasive form of privacy interference is mass surveillance. This is because mass surveillance involves the interference with the privacy right of everyone with the aim of identifying particular acts by a small minority (such as those engaging in terrorism or other serious criminal activities).

Indiscriminate mass surveillance will never be justified – any surveillance should always be targeted. While targetted surveillance of groups may be justified in some circumstances, it should only ever be as a last resort, and should be preceded by widespread consultation and a detailed Privacy Impact Assessment (PIA).

SUBMISSION 1:
The Committee should explicitly recognise that enormous care is needed in establishing appropriate balances between national security and law enforcement powers, on the one hand, and the human rights that underpin a free society, on the other.

All powers granted to law enforcement agencies must be justified, proportionate and controlled, and the organisations and individuals must be accountable, and subject to regulatory regimes that are independent of the law enforcement and national security agencies themselves.

These principles should be applied retrospectively to existing powers as well as to all new bids for additional and extended powers.

SUBMISSION 2:
The Committee should recognise a number of overarching principles that should be applied when evaluating proposals of the kind contained in the Discussion Paper:

- Justification
- Proportionality
- Controls

- Accountability

2.3 The Centrality of Privacy

The APF reminds the Committee of the significance of privacy rights in free and democratic societies – they serve not only individual interests but also a collective public interest in limiting the ability of large powerful organizations in both the public and private sectors to intrude into the personal lives of citizens and consumers. Australia has acknowledged the importance of privacy rights by becoming a party to the International Convention on Civil and Political Rights, under Article 17 of which Australia has undertaken to 'adopt such legislative measures a may be necessary to give effect to the right of persons not to be subjected to arbitrary or unlawful interference with their privacy, family, home or correspondence'.

Privacy comprises multiple dimensions, including privacy of the physical person, privacy of personal behaviour, privacy of personal communications, and privacy of personal data.

Australian law provides only very patchy and weak protections, primarily:

- very patchy protection of privacy of personal behaviour, in surveillance devices legislation
- very patchy protection of privacy of personal communications, primarily in the TIAA
- weak protection of privacy of personal data in the Privacy Act 1988, with amendments currently before the Parliament further weakening the privacy principles (see our submissions to the Senate and House Committees currently reviewing the Privacy Amendment (Enhancing Privacy Protection) Bill 2012.

The APF draws attention to the Australian Privacy Charter, which is comprehensive in its coverage of privacy, rather than being restricted merely to data protection. See the Attachment to this Submission (Annex 3).

SUBMISSION 3:

The Committee should acknowledge the Australian Privacy Charter as a more appropriate basis against which to measure privacy protections than narrow instruments such as the Privacy Act and the weak sets of (Information) Privacy Principles found in that Act. We note that Parliament is currently considering proposed amendments to the Privacy Act in the Privacy Amendment (Enhancing Privacy Protection) Bill 2012 which in our view, and the considered views of other key stakeholders, actually weaken rather than strengthen the statutory privacy protection framework.[1]

SUBMISSION 4:

The Committee should find that there are areas in which revision of the TIAA, and related provisions of the ASIO Act, are justified. However, it should also find that there is a great deal of complexity in the technologies involved, in the policy issues that arise, in the existing regime, and in the regime that AGD wishes to develop on behalf of the at least 17 'interception agencies' and multiple and possibly large numbers of 'other enforcement agencies' (p. 24). These complexities, and the implications for an appropriate balance of public and private interests, deserve a longer and more considered public debate

2.4 Privacy protection for telecommunications

Commonwealth statutory privacy protection has always been found in a range of laws, not limited to the Privacy Act. In the telecommunications area, where both privacy of personal information and

[1] See submissions to the Senate and House Committees at http://www.aph.gov.au/Parliamentary_Business/Committees/House_of_Representatives_Committees?url=spla/bill%20privacy/index.htm and http://www.aph.gov.au/Parliamentary_Business/Committees/Senate_Committees?url=legcon_ctte/privacy_2012/index.htm

privacy of communications are involved, key privacy protection is provided by the Telecommunications Interception and Access Act 1979 (TIAA) [2].

The ALRC, in its major review of Australian privacy law from 2005-2008, looked at privacy protection for telecommunications. In its 2008 Report 108 *For your information*, the ALRC devoted an entire section to telecommunications, and the relationship between the Privacy Act and privacy provisions in telecommunications-specific legislation, and made some welcome proposals for reform and further review. Unfortunately the government has put off a response to this part of the ALRC report into an indefinite future. It would have been far better to have had a fully debated and settled framework in place before having to consider the proposals brought forward in this Discussion Paper.

The Discussion Paper provided by AGD presents initially as if it were proposing enhancements to privacy safeguards ("Strengthening the safeguards and privacy protections", e.g. pp. 8, 13, 14, 22, 23).

The contents of the wish-list, on the other hand, show that the expression in the early parts of the Discussion Paper is misleading, and probably intentionally so. The wish-list contains many elements that, if the Parliament were to ever adopt them, would very substantially shift the balance away from privacy, and in favour of a significantly expanded 'surveillance state' that Australians decried when such things were attempted behind the Iron Curtain, and which we continue to criticize in contemporary authoritarian regimes overseas.

SUBMISSION 5:
The Committee should expressly recognise that the superficially privacy-sensitive aspects of the Discussion Paper's text are misleading, and create a pretence of care for privacy that is not reflected in the body of the document.

The Discussion Paper provides a short background to its purported justification (pp. 14-17), supported by snippets of justification in the sections introducing each category, and further snippets when discussing some of their more specific desires.

SUBMISSION 6:
The Committee should find that justification for highly intrusive elements of the wish-list has not been demonstrated, because the grounds declared in the Discussion Paper are vague, and are supported by very little evidence, even less of which is relevant to the points at issue.

3. Unacceptable elements of the Government's Wish-List

The Discussion Paper is structured in a manner that makes it difficult to extract a single and consistent control-list of all of the desires (wish-list) it contains. The contents pages (pp. 1-2), the Terms of Reference (pp. 6-11), the priority issues (p. 13) each provide different variants.

SUBMISSION 7:
The Committee should express serious concern about the unnecessary challenges that the APF and many other stakeholders have been presented with by the Attorney-General's Department (AGD), including through:

- exclusion from consultations
- unclear structuring of the Discussion Paper
- artificial and very tight time-pressures

The APF draws attention in particular to the following examples of quite clear and serious concern.

[2] Formerly the Telecommunications Interception Act 1979 – the Act was renamed in 2006 when related provisions were transferred from the Telecommunications Act 1997.

3.1 Scope Creep

SUBMISSION 8:
The Committee, in evaluating the desires expressed in the Discussion Paper, should never lose sight of the fact that the TIAA was originally conceived to authorise only 2 agencies (ASIO and AFP – p. 25)), but that both function creep and agency creep have been permitted to occur, such that it is now applicable to over 20 agencies, with enormously greater negative impact on civil liberties than the Parliament originally contemplated.

SUBMISSION 9:
All aspects of the proposals must be treated with extreme caution, and investigated and consulted upon with much more care than has been the case so far.

3.2 The Threshold for Warrants

SUBMISSION 10:
The Committee should recommend that the request to lower the threshold for interception warrants from 'serious offence' / 7 years' imprisonment (p. 24) represents a seriously harmful, unjustified and unjustifiable request.

Access to communications in storage is every bit as intrusive as access to live communications.

SUBMISSION 11:
The Committee should recommend that the threshold for 'stored communication warrants' should be raised from the present 3 years' imprisonment / 180 penalty units' to the same 'serious offence' / 7 years' imprisonment level as currently apply to interception warrants..

3.3 Unjustified Access

SUBMISSION 12:
The Committee should express alarm that the AGD should admit that "[some] agencies able to access communications information [do not] have a demonstrated need to access that type of information" (p. 24, last para.), and should instruct AGD to immediately identify those agencies and uses and take appropriate steps to preclude them from gaining such access.

3.4 Reporting Requirements

The APF agrees with the statement that "reporting requirements [should be] attuned to providing the information needed to evaluate whether intrusion to privacy under the regime is proportionate to public outcomes" (p. 26). On the other hand, some of the text reads as though the AGD regards reporting requirements as being for the convenience of law enforcement agencies, which is not the case.

SUBMISSION 13:
The Committee should recommend that reporting requirements be designed to provide public transparency and regulatory control over abuses of the scheme, and that convenience to the reporting agencies is a constraint not an objective.

3.5 Telcos and Internet Intermediaries as agents of the State

Telecommunications legislation already goes much further than regulation in most other sectors in mandating a role for private sector businesses as agents of the state in surveillance and law enforcement (banking and finance is the other main area where this has happened). These proposals would see a further significant extension of this role. Online intermediaries in particular host our communications with our friends, relatives, co-workers etc. They host a vast amount of information, the volume and scope of which is growing exponentially as we move to the cloud, use social networks, etc. Using online intermediaries as an agent of the State dramatically impacts on

the state's surveillance capabilities. Even minor changes in what they are required to do on behalf of government agencies can have very broad implications for people's privacy.

There is a vigorous international debate about the role of intemet intermediaries, and guidance is being developed in international fora on how to achieve an appropriate balance[3]. The Discussion Paper makes no reference to this international context. Australian policy in this area should not be out of step with developing international norms and standards, at least without good reason, publicly debated and justified. The Discussion Paper's failure to acknowledge this context betrays a lack of coordination, at least on some key issues, between the Attorney-General's Department and the Department of Broadband, Communications and the Digital Economy.

SUBMISSION 14:
The Committee should express serious concern about any further significant extension of the trend to co-opt private sector businesses into the national security and law enforcement apparatus. This should be critically assessed both from a rights perspective and in terms of its effect on the internet economy.

3.6 Cost-Sharing (Item 4a)

The bland expression 'Modernising the cost sharing framework' (pp. 8, 14, 23, 27-28) is a misleading use of language. Not content with mandating private sector cooperation, the government is increasingly seeking to externalise the costs of law enforcement and national security onto the private sector.

This trend is highly undesirable in two respects. Firstly such cost impositions warp the commercial decisions of companies, by causing them to build surveillance capabilities into their infrastructure and to seek a return on the investments they have had to make. Secondly, government agencies which benefit from the surveillance capabilities are relieved of the normal discipline of having to justify the cost to taxpayers. This trend to privatise law enforcement and national security is seriously detrimental to both economic efficiency and the accountability of government in a free society.

Any cost-shifting of surveillance to the private sector is also a particular burden on smaller enterprises, such as are increasingly found in the telecommunications sector. It is one thing to ask the major carriers to invest in surveillance capability, and quite another to expect small ISPs to bear the cost of similar capability. We assume that a regulatory impact statement would be required to accompany any implementing legislation, and suggest that such an assessment would almost certainly find the imposition of these burdens on small telecommunications businesses to be both impracticable and unjustified on any rational cost-benefit calculation.

SUBMISSION 15:
The Committee should reject further cost-impositions on companies, and should recommend compensation by the Commonwealth for costs incurred in order to comply with both existing and the proposed new requirements.

3.7 Protection from Criminal and Civil Liability (Item 10)

The Discussion Paper makes the extraordinary bids (pp. 46-47) for:

- a 'get out of jail free' card for breaches
- the capacity of the national security community to issue such cards themselves

[3] See in particular the work of the OECD on Information Security and Privacy http://www.oecd.org/sti/interneteconomy/informationsecurityandprivacy.htm in which the Department of Broadband, Communications and the Digital Economy is involved.

SUBMISSION 16:
The Committee should reject the proposition outright that breaches could be absolved by any party at all, and certainly not by part of the national security community, because that would represent authority for that community to operate beyond the reach of the law.

SUBMISSION 17:
The Committee should assert unequivocally that all such decisions are properly made by, and only by, the courts, on the basis of the law.

3.8 Interference with Data and Devices (Item 11c)

Some parts of Discussion Paper are so unclear as to make it hard to assess whether to be concerned or not (which of course is concerning in itself).

For example, on page 48 there is a discussion of the restriction placed on ASIO "from doing anything under a computer access warrant that adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons". The discussion paper suggests removing this restriction in the context of activities "proportionate to what is necessary to execute the warrant". This may be harmless or disastrous depending on exactly what is intended.

SUBMISSION 18:
The Committee should reject outright the concept of agencies ever being permitted to perform an act that "adds, deletes or alters data or interferes with, interrupts, or obstructs the lawful use of the target computer by other persons", on the grounds that such acts pollute evidence, and enable the 'framing' of suspects.

3.9 Data Retention

There is no heading in the Discussion Paper relating to data retention, despite this clearly being one of the most radical and controversial proposals.

Item 15, under the misleadingly re-assuring heading of 'Modernising the Industry assistance framework' includes:

> c. tailored data retention periods for up to 2 years for parts of a data set, with specific timeframes taking into account agency priorities, and privacy and cost impacts "(p. 10)

The Committee is expressly invited to give its views on this proposal.

The Discussion Paper provides no further detail of this proposal is, makes no attempt to compare the proposal with the status quo, and provides no justification whatsoever.

This is an excellent example of the kind of vague, unsubstantiated and unjustified proposal that should never be placed before the Parliament.

There is an extensive body of overseas experience of data retention requirements, and it is a very topical and hotly contested area of public policy. The APF would be pleased to make a detailed and substantive submission on the significant privacy issues involved, given more detailed proposals on which to comment. We note that the Electronic Frontiers Australia have given a more detailed critique of the data retention proposals in their submission, and we share many of their concerns. In our view it would be entirely premature for the Committee to give any opinion on the need for and extent of any data retention regime on the basis of the sketchy case presented in this Discussion Paper.

One of the major problems with any data retention requirement is that it is directly contrary to security objectives. Mandating the creation and storage of records of communications that would

not otherwise be kept increases risk and vulnerability, creating additional 'honeypots' of valuable personal information that would be a target for hackers and risk multiple abuses.

SUBMISSION 19:

The Committee should reject any proposal for new data retention requirements on the basis of mere asserted benefits, and should insist that the government present more detailed proposals, with proper justification, before they are given serious consideration.

3.10 Other aspects of cooperation by the Private Sector (Item 9, 12, and 14-16)

There are many references in the Discussion Paper to cooperation. We have already expressed our serious concern about the trend to co-opt the private sector into both implementing and paying for surveillance which should properly remain the domain of clearly accountable government agencies.

A related area of concern is the intentional flexibility (vagueness) which government seeks to build in to any cooperation requirements.

SUBMISSION 20:

The Committee should express serious concern about the continued trend to enlist corporations as part of the national security apparatus. All responsibilities of corporations and individuals must be explicit and clear at law, and not subject to discretionary interpretation by law enforcement and national security agencies of rubbery clauses that permit or require 'cooperation'.

3.11 Use of Third Party Computers and Communications in Transit (Item 17a)

A similar need for further discussion can be noted in the context of "Use of third party computers and communications in transit" on page 50 of the DP.

SUBMISSION 21:

The Committee should require far greater articulation of the proposal, and a prior consultation process (in accordance with Submissions above), prior to considering such a possibility.

3.12 Ministerial Authorisations (Items 18a, 18b)

On pp. 51-54, the AGD seeks to extend the scope of Ministerial Authorisations.

The APF submits that such powers should not be vested in a Minister, but in a suitably senior judicial officer, in a manner akin to the process for judicial warrants.

SUBMISSION 22:

The Committee should reject any extension of the scope of Ministerial Authorisations.

4. Conditionally acceptable elements of the Government's Wish-List

The APF draws attention in particular to the following examples of elements of the proposals that could well attract strong support from public interest advocates generally, if they were further articulated in a manner consistent with the outline descriptions provided in the Discussion Paper.

An example is "a simplified warrant regime that focuses on better targeting the characteristics of a communication that enable it to be isolated from communications that are not of interest" (p. 25).

Possibilities include the following items in the wish list at pages 7-10 of the Discussion Paper:

A1d the strengthening of oversight provisions

A2a reduction in the number of agencies eligible to access communications information

A3b removing legislative duplications

A5a updating the definition of 'computer'

A6 modernising ASIO Act employment provisions

B8a creating a single warrant with multiple TI powers

B11a providing ASIO with a named person warrant option

SUBMISSION 23:
The Committee should recommend that the government engage better with stakeholders, including civil society non-government organisations, to seek support for the less contentious proposed improvements to the regime.

5. Procedural Failures

During the last two decades, the APF has observed a significant worsening of the manner in which government agencies bring draft legislation forward to the Parliament. During this period, there should have been considerable improvements to processes, partly because of the considerably greater data-handling and communications facilities at agencies' disposal, but particularly in view of the enormous increases in the privacy-invasiveness of technologies, and of proposals being placed before the Parliament.

This section briefly outlines what the APF considers to be some important basic principles in relation to the preparation of draft legislation, followed by consideration of the performance of the AGD in this particular matter. In the APF's opinion, the process in relation to these proposals represents a low-water mark in governmental processes.

SUBMISSION 24:
The Committee should recommend that proposals of the gravity of those contained in this Discussion Paper demand the highest standards of preparatory work, which have not been met in this case.

5.1 General Principles for policy development and consultation

When any agency intends bringing forward legislative proposals that have potentially negative impacts on privacy, it is important that a coherent process be devised, to ensure that:

- the agency is informed about all areas of concern
- the many different perspectives of parties affected by the legislation are heard and reflected
- the Parliament receives a mature proposal for consideration
- advocacy organisations (typically under-resourced) are able to merely highlight to Parliamentary Committees the points of difference between the positions of the interest groups, rather than having to build their case from scratch.

A fundamental need is for the agency to develop a comprehensive understanding of the stakeholder groups, not merely government agencies, and not merely 'the industry', but also including representatives of all categories of organisations and individuals affected by the proposal.

It is also critical that the agency enter into effective engagement with all such stakeholders.

As appropriate to the circumstances, the process may form part of a broader Risk Assessment from the perspective of the affected individuals or population segments, or a broad Social Impact Assessment.

In particular, well-developed guidance in relation to the conduct of Privacy Impact Assessment is provided by the Victorian Privacy Commissioner, the UK Information Commissioner, and the Australian Privacy Commissioner (in order of their value, in our view) [4].

5.2 Application of these policy development and consultation principles in this case

The AGD declares that is has undertaken consultation, but only with "the telecommunications industry", comprising "telecommunication carriers and carriage service providers (C/CSPs)" (p. 29. See also pp. 4, 33-39). APF is aware that discussions with industry have been underway for many years – for instance serious consideration was being given to data retention requirements as long ago as 2006 – and yet there has been no significant consultation with other interested parties.

Telecommunications involves a very substantial ecology, far beyond the CSPs that AGD works through in operating the regime. Players that the AGD has sought to ignore include:

- professional associations, such as ACS, IEEE and AusNOG
- user representative organisations, such as ISOC-AU, EFA and PPA
- human rights and privacy advocacy organisations, such as APF and the four major councils for civil liberties (CCLs)

The AGD appears to have conducted no direct consultations that involved public interest organisations such as those identified above. It is completely inappropriate for the Parliament to be used by government agencies as a clearing-house for their wish-lists.

SUBMISSION 25:
The Committee should recommend that AGD adapt and extend its consultation processes to encompass all organisations that represent interests in telecommunications services, and in particular relevant advocacy organisations for the interests of the public, including professional, user and human rights and privacy organisations.

Further, the APF finds it extraordinary that the AGD should presume to instruct the Parliament on what it should do: "it is imperative that the PJCIS take into account a wide range of views on the proposals from public stakeholders and government agencies" (p. 55).

The inappropriateness of the executive giving instructions to the parliament is compounded by the fact that the AGD has abjectly failed to follow its own advice.

SUBMISSION 26:
The Committee should recommend that AGD to build into its processes:

- stakeholder analysis, in order to identify all relevant organisations that represent the interests of all affected population segments, and not merely government agencies and CSPs
- publication to those organisations of sufficient information to enable effective consultations to take place
- consultation with all relevant organisations, at a sufficiently early stage that the design reflects the outcomes of the consultations
- reflection of the views of those organisations in resulting documents

SUBMISSION 27:
The Committee should communicate to the AGD that it will not consider draft legislation or other documents that are not the result of a process as described in the immediately preceding Submission.

A mature proposal comprises a legislative package including:

[4] See Clarke R. (2011) 'An Evaluation of Privacy Impact Assessment Guidance Documents' International Data Privacy Law 1, 2 (March 2011), PrePrint at http://www.rogerclarke.com/DV/PIAG-Eval.html

- a submission reconciled against the key points arising during consultations
- the Bill(s), Explanatory Memoranda, any other required Statements and Second Reading Speech
- all significantly impacted statutes in the form they would take following enactment, to assist understanding of the effect of amendments

The AGD is seeking to suppress public reporting by the Parliamentary Committee, in that the Terms of Reference refer only to a report to the Attorney-General, with the clear implication that the public will be denied access to important information contained in the Committee's Report. It is acknowledged that justification may exist for specific details to be contained in closed Appendices. It is essential, however, that all substantive arguments and conclusions, and sufficient evidence supporting them, be included in a published Report.

SUBMISSION 28:
The Committee should reject this grossly inappropriate Term of Reference, and should publish a comprehensive Report.

For further information please contact:

Nigel Waters 0407 230 342 board5@privacy.org.au

Board Member
Australian Privacy Foundation

APF Web site: http://www.privacy.org.au

Please note that APF's preferred mode of communication is by email, which should be answered without undue delay. APF does not have an organisational postal address. If postal communication is necessary, please contact the person named above to arrange for a postal address.

ANNEX 1: Australian Privacy Foundation

Background Information

The Australian Privacy Foundation (APF) is the primary national association dedicated to protecting the privacy rights of Australians. The Foundation aims to focus public attention on emerging issues that pose a threat to the freedom and privacy of Australians. The Foundation has led the fight to defend the right of individuals to control their personal information and to be free of excessive intrusions.

The APF's primary activity is analysis of the privacy impact of systems and proposals for new systems. It makes frequent submissions to parliamentary committees and government agencies. It publishes information on privacy laws and privacy issues. It provides continual background briefings to the media on privacy-related matters.

Where possible, the APF cooperates with and supports privacy oversight agencies, but it is entirely independent of the agencies that administer privacy legislation, and regrettably often finds it necessary to be critical of their performance.

When necessary, the APF conducts campaigns for or against specific proposals. It works with civil liberties councils, consumer organisations, professional associations and other community groups as appropriate to the circumstances. The Privacy Foundation is also an active participant in Privacy International, the world-wide privacy protection network.

The APF is open to membership by individuals and organisations who support the APF's Objects. Funding that is provided by members and donors is used to run the Foundation and to support its activities including research, campaigns and awards events.

The APF does not claim any right to formally represent the public as a whole, nor to formally represent any particular population segment, and it accordingly makes no public declarations about its membership-base. The APF's contributions to policy are based on the expertise of the members of its Board, SubCommittees and Reference Groups, and its impact reflects the quality of the evidence, analysis and arguments that its contributions contain.

The APF's Board, SubCommittees and Reference Groups comprise professionals who bring to their work deep experience in privacy, information technology and the law.

The Board is supported by Patrons The Hon Michael Kirby and Elizabeth Evatt, and an Advisory Panel of eminent citizens, including former judges, former Ministers of the Crown, and a former Prime Minister.

The following pages provide access to information about the APF:

- Policies http://www.privacy.org.au/Papers/
- Resources http://www.privacy.org.au/Resources/
- Media http://www.privacy.org.au/Media/
- Current Board Members http://www.privacy.org.au/About/Contacts.html
- Patron and Advisory Panel http://www.privacy.org.au/About/AdvisoryPanel.html

The following pages provide outlines of several campaigns the APF has conducted:

- The Australia Card (1985-87) http://www.privacy.org.au/About/Formation.html
- Credit Reporting (1988-90) http://www.privacy.org.au/Campaigns/CreditRpting/
- The Access Card (2006-07) http://www.privacy.org.au/Campaigns/ID_cards/HSAC.html
- Privacy and the Media (2007-) http://www.privacy.org.au/Campaigns/Media/

ANNEX 2: Recent analyses of regulatory responses to the perceived threat of terrorism

We draw attention to two valuable recent analyses of anti-terrorism laws:

A Decade of Australian Anti-Terror Laws, Professor George Williams, Melbourne University Law Review, 2012 (forthcoming)
http://www.mulr.com.au/issues/35_3/35_3_13.pdf

Report of the Special Rapporteur on the promotion and protection of human rights and fundamental freedoms while countering terrorism; United Nations General Assembly Human Rights Council A/HRC/13/37 December 2009
http://daccess-dds-ny.un.org/doc/UNDOC/GEN/G09/178/04/PDF/G0917804.pdf

We also acknowledge the value of the Parliamentary Library's collation of Terrorism Laws 2001-10, (although not updated for 2011 and 2012), at:
http://www.aph.gov.au/About_Parliament/Parliamentary_Departments/Parliamentary_Library/Browse_by_Topic/TerrorismLaw/legislativedev

ANNEX 3: THE AUSTRALIAN PRIVACY CHARTER

The Australian Privacy Charter was launched in December 1994. It was developed by a specially-formed group which styled itself the Australian Privacy Charter Council (APCC). This was established in 1992, under the Chairmanship of Justice Michael Kirby, to develop a Privacy Charter comprising principles which would encompass and apply:

- to all forms of privacy and surveillance (i.e. not just information privacy); and
- to both private and public sector organisations and their clients.

APCC comprised 25 invited members with backgrounds in law, business, auditing, information technology, security, privacy, media and politics. The final draft was sent to representatives of other relevant organisations and community groups throughout Australia and privacy advocates in Australia and overseas.

[The Council was wound up in 2002 and the Charter transferred to the Australian Privacy Foundation. The Council's web site was archived in June 2003 and transferred to http://www.privacy.org.au/apcc/.]

Preamble

THE MEANING OF 'PRIVACY'

Australians value privacy. They expect that their rights to privacy be recognised and protected.

People have a right to the privacy of their own body, private space, privacy of communications, information privacy (rights concerning information about a person), and freedom from surveillance.

'Privacy' is widely used to refer to a group of related rights which are accepted nationally and internationally. This Charter calls these rights 'privacy principles'.

Privacy Principles comprise both the rights that each person is entitled to expect and protect, and the obligations of organisations and others to respect those rights.

Personal information is information about an identified person, no matter how it is stored (eg sound, image, data, fingerprints).

PRIVACY IS IMPORTANT

A free and democratic society requires respect for the autonomy of individuals, and limits on the power of both state and private organisations to intrude on that autonomy.

Privacy is a value which underpins human dignity and other key values such as freedom of association and freedom of speech.

Even those privacy protections and limitations on surveillance that do exist are being progressively undermined by technological and administrative changes. New forms of protection are therefore required.

INTERFERENCES WITH PRIVACY MUST BE JUSTIFIED

Privacy is a basic human right and the reasonable expectation of every person. It should not be assumed that a desire for privacy means that a person has 'something to hide'. People who wish to protect their privacy should not be required to justify their desire to do so.

The maintenance of other social interests (public and private) justifies some interferences with privacy and exceptions to these Principles. The onus is on those who wish to interfere with privacy to justify doing so. The Charter does not attempt to specify where this may occur.

AIM OF THE PRINCIPLES

The following Privacy Principles are a general statement of the privacy protection that Australians should expect to see observed by both the public and private sectors. They are intended to act as a benchmark against which the practices of business and government, and the adequacy of legislation and codes, may be measured. They inform Australians of the privacy rights that they are entitled to expect, and should observe.

The Privacy Charter does not attempt to specify the appropriate means of ensuring implementation and observance of the Privacy Principles. It does require that their observance be supported by appropriate means, and that appropriate redress be provided for breaches.

Privacy Principles

1 . JUSTIFICATION & EXCEPTIONS

Technologies, administrative systems, commercial services or individual activities with potential to interfere with privacy should not be used or introduced unless the public interest in so doing outweighs any consequent dangers to privacy.

Exceptions to the Principles should be clearly stated, made in accordance with law, proportional to the necessities giving rise to the exception, and compatible with the requirements of a democratic society.

2. CONSENT

Individual consent justifies exceptions to some Privacy Principles. However, 'consent' is meaningless if people are not given full information or have no option but to consent in order to obtain a benefit or service. People have the right to withdraw their consent.

In exceptional situations the use or establishment of a technology or personal data system may be against the public interest even if it is with the consent of the individuals concerned.

3. ACCOUNTABILITY

An organisation is accountable for its compliance with these Principles. An identifiable person should be responsible for ensuring that the organisation complies with each Principle.

4. OBSERVANCE

Each Principle should be supported by necessary and sufficient measures (legal, administrative or commercial) to ensure its full observance, and to provide adequate redress for any interferences with privacy resulting from its breach.

5. OPENNESS

There should be a policy of openness about the existence and operation of technologies, administrative systems, services or activities with potential to interfere with privacy.

Openness is needed to facilitate public participation in assessing justifications for technologies, systems or services; to identify purposes of collection; to facilitate access and correction by the individual concerned; and to assist in ensuring the Principles are observed.

6. FREEDOM FROM SURVEILLANCE

People have a right to conduct their affairs free from surveillance or fear of surveillance. 'Surveillance' means the systematic observation or recording of one or more people's behaviour, communications, or personal information.

7. PRIVACY OF COMMUNICATIONS

People who wish to communicate privately, by whatever means, are entitled to respect for privacy, even when communicating in otherwise public places.

8. PRIVATE SPACE

People have a right to private space in which to conduct their personal affairs. This right applies not only in a person's home, but also, to varying degrees, in the workplace, the use of recreational facilities and public places.

9. PHYSICAL PRIVACY

Interferences with a person's privacy such as searches of a person, monitoring of a person's characteristics or behaviour through bodily samples, physical or psychological measurement, are repugnant and require a very high degree of justification.

10. ANONYMOUS TRANSACTIONS

People should have the option of not identifying themselves when entering transactions.

11. COLLECTION LIMITATION

The minimum amount of personal information should be collected, by lawful and fair means, and for a lawful and precise purpose specified at the time of collection. Collection should not be surreptitious. Collection should be from the person concerned, if practicable.

At the time of collection, personal information should be relevant to the purpose of collection, accurate, complete and up-to-date.

12. INFORMATION QUALITY

Personal information should be relevant to each purpose for which it is used or disclosed, and should be accurate, complete and up-to-date at that time.

13. ACCESS & CORRECTION

People should have a right to access personal information about themselves, and to obtain corrections to ensure its information quality.

Organisations should take reasonable measures to make people aware of the existence of personal information held about them, the purposes for which it is held, any legal authority under which it is held, and how it can be accessed and corrected.

14. SECURITY

Personal information should be protected by security safeguards commensurate with its sensitivity, and adequate to ensure compliance with these Principles.

15. USE & DISCLOSURE LIMITATIONS

Personal information should only be used, or disclosed, for the purposes specified at the time of collection, except if used or disclosed for other purposes authorised by law or with the meaningful consent of the person concerned.

16. RETENTION LIMITATION

Personal information should be kept no longer than is necessary for its lawful uses, and should then be destroyed or made anonymous.

17. PUBLIC REGISTERS

Where personal information is collected under legislation and public access is allowed, these Principles still apply except to the extent required for the purpose for which public access is allowed.

18. NO DISADVANTAGE

People should not have to pay in order to exercise their rights of privacy described in this Charter (subject to any justifiable exceptions), nor be denied goods or services or offered them on a less preferential basis. The provision of reasonable facilities for the exercise of privacy rights should be a normal operating cost.