Terms of Reference

Review of measures designed to protect classified and security sensitive information in the course of investigations and proceedings

I, DARYL WILLIAMS, Attorney-General of Australia, acting pursuant to section 20 of the *Australian Law Reform Commission Act 1996* refer the following matter to the Australian Law Reform Commission for inquiry and report pursuant to s 20(1) of the *Australian Law Reform Commission Act 1996:*

Measures to protect classified and security sensitive information in the course of investigations and proceedings. 'Security sensitive information' is information that has implications for Australia's security but is not formally classified, for whatever reason.

1. The Commission shall consider, among other matters:

    a. The operation of existing mechanisms designed to prevent the unnecessary disclosure of classified material or security sensitive material in the course of criminal or other official investigations and court or tribunal proceedings of any kind, including:

        - common law public interest immunity;
        - section 23V of the *Crimes Act 1914* in relation to the provision of material to suspects and any other relevant provisions;
        - section 85B of the *Crimes Act 1914* in relation to in camera proceedings;
        - the enforceability of Commonwealth protective security standards as set out in the Commonwealth Protective Security Manual;
        - other mechanisms available to investigators and the courts to limit the disclosure of classified or security sensitive material including redaction and excision of sensitive material from classified documents; and
        - whether existing mechanisms adequately protect security sensitive information.

    b. International practice with regard to the protection of classified or security sensitive information in the course of criminal or other official investigations and court or tribunal proceedings of any kind;

c. Training, functions, duties and role of judges, judicial officers, tribunal members and lawyers in relation to the protection of classified and security sensitive information that is or may be presented to the court;

d. Training, functions, duties and role of investigators in relation to the protection of classified and security sensitive information that is obtained or used in the course of any investigation or court or tribunal proceedings; and

e. Any related matter.

2. The Commission shall consider the need for regulatory measures designed to protect classified information or security sensitive material in the course of criminal investigations and proceedings including:

a. Assessing the practical implications of any recommendations for measures; and

b. Assessing alternatives, including non-regulatory alternatives.

3. The Commission will consult widely with the public and key stakeholders.

4. The Commission is to report not later than 29 February 2004.

Dated:2 April 2003

Daryl Williams
Attorney-General

Participants

Australian Law Reform Commission

The Division of the ALRC constituted under the *Australian Law Reform Commission Act 1996* (Cth) for the purposes of this inquiry comprises the following:

President
Professor David Weisbrot

Members
Mr Ian Davis (Commissioner in charge)
Professor Anne Finlay
Associate Professor Brian Opeskin
Justice Susan Kenny (part-time Commissioner)
Justice Susan Kiefel (part-time Commissioner)
Justice Mark Weinberg (part-time Commissioner)

Senior Legal Officers
Carolyn Adams
Isabella Cosenza

Legal Officer
Kate Connors

Project Assistant
Alayne Harland

Legal Interns
Katherine Jones
Elly Krimotat

1. Introduction

Background to the ALRC's inquiry

1.1 The Attorney-General has asked the Australian Law Reform Commission (ALRC) to inquire into and report on measures to protect classified and security sensitive information in the course of investigations and legal proceedings, and in other contexts.

1.2 The ALRC has been asked to consider whether existing mechanisms adequately protect classified and security sensitive information, and whether there is a need for further regulatory or non-regulatory measures in this area. Existing mechanisms include: common law and statutory public interest immunity; legislative provisions that allow for closed court proceedings and the restriction of publication of all, or any part, of a proceeding; and the standards set out in the Commonwealth Protective Security Manual.

1.3 In assessing these existing mechanisms, the ALRC will have regard to the rights of individuals to a fair hearing and the general public interest in open government and open court proceedings, taking into account how Australian and international laws currently protect these interests. The ALRC also will consider Australia's position and proposals for changes to the law here in the light of overseas laws and experience in this area.

1.4 This inquiry provides all sectors of the Australian community—individuals, civil rights groups, government agencies, the courts, the police and prosecuting authorities, the legal profession, legal aid bodies, and bodies representing migrants and refugees, to name just some—with an opportunity to contribute to developing government and public policy.

1.5 This inquiry arises at a time when Australia's security is seen to be confronted with new and increased threats, especially those associated with international terrorism. There is no real doubt that there is some information which, in the national and public interest, should not be disclosed publicly; nor that there are occasions where the public interests in open justice and open government are in conflict with a proper need for secrecy.

1.6 It is not the ALRC's task in this inquiry to examine broadly Australia's current or proposed anti-terrorism or other crimes and intelligence legislation. However, it is important to consider whether the current circumstances require any substantial departure from the existing principles and procedures that underlie our justice system and balance the conflicting public interests of secrecy and openness—which have been developed over many years in periods of peace and war, threat and stability. The mere fact that security concerns are heightened may not of itself justify new methods of handling classified and security sensitive information, especially if civil liberties were

to be unreasonably curtailed and safeguards against administrative and executive abuse were not also introduced.

1.7 The ALRC is due to report to the federal Attorney-General by 29 February 2004. The Commission anticipates publishing a Discussion Paper later in 2003 to outline its preliminary views and as a basis for further public consultations and submissions. This Paper is intended to act as an outline of the issues that the ALRC is required to consider and as a stimulus for preliminary public submissions and consultations. At this stage the ALRC is entirely open as to the direction that its inquiry will take, within the limits of its Terms of Reference.

1.8 Any public contribution to an inquiry is called a submission and these are actively sought by the ALRC from a broad cross-section of the community, as well as those with a special interest in this inquiry. Submissions are usually written, but there is no set format and they need not be formal documents. It would be helpful if comments address specific questions or paragraphs in this Paper. Where possible, submissions in electronic format are preferred.

What is classified information?

1.9 The Commonwealth Protective Security Manual (PSM) binds all Commonwealth agencies to a series of procedures designed to protect classified and security sensitive information. It contains the definitions and processes by which classifications are made.

1.10 The PSM notes that, in the past, national security information was often referred to as 'classified', while non-national security information was known as 'sensitive'.[i] This caused confusion as both types of information could be subject to a classification process. The Manual now uses the terms 'national security information' and 'non-national security information' to refer to information requiring classification.

1.11 The fact that information is not classified does not mean that it is freely available to all people for all purposes. For example, legislation such as the *Privacy Act 1988* (Cth) restricts the dissemination and use of certain personal information covered by it. All official information (ie, information developed, received or collected by or on behalf of the government):

- must be handled with due care and only in accordance with authorised procedures
- must be made available only to people who have a legitimate need to know to fulfil their official duties or contractual responsibilities
- is only to be released in accordance with the policies, legislative requirements and directives of the Government and the courts.[ii]

1.12 Government officers are generally only entitled to information that they have a need to know to carry out their functions properly.[iii] However, certain legislation—

most notably the *Freedom of Information Act 1982* (Cth)—gives the public certain rights to access government-held or government-controlled information, subject to a number of exceptions and exemptions.[iv] It is also stated government policy that:

> As much official information as possible should be available to the public, as long as the release of that information is not detrimental to:
>
> - public interest
> - government interest
> - the interest of third parties who deal with the Government.[v]

1.13 One element of 'public interest', and possibly 'government interest', is national security.

1.14 The PSM defines **national security information** as any official resource (including equipment) that records information about or associated with Australia's:

- security from espionage, sabotage, politically motivated violence, promotion of communal violence, attacks on Australia's defence system or acts of foreign interference;
- defence plans and operations;
- international relations, that relate to significant political and economic relations with international organisations and foreign governments;
- national interest, that relates to economic, scientific or technological matters vital to Australia's stability and integrity.[vi]

1.15 National security information may be given one of four national protective security markings (listed in order of increasing sensitivity):

- Restricted—if compromise of it could cause 'limited damage' to national security;
- Confidential—if compromise of it could cause 'damage' to national security;
- Secret—if compromise of it could cause 'serious damage' to national security;
- Top Secret—if compromise of it could cause 'exceptionally grave damage' to national security.[vii]

1.16 The PSM notes that most national security information requiring classification would be adequately protected by the first two of these markings. The 'Secret' marking should be used only sparingly and the 'Top Secret' marking should be used with the 'utmost restraint'.[viii]

1.17 The PSM defines **non-national security information** as any official resource (including equipment) that threatens the interests of other important groups or individuals rather than the nation, and requires increased protection. This includes information about:

- government or agency business, whose compromise could affect the government's capacity to make decisions or operate, the public's confidence in government, the stability of the marketplace and so on;
- commercial interests, whose compromise could affect the competitive process and provide the opportunity for unfair advantage;
- law enforcement operations, whose compromise could hamper or render useless crime prevention strategies or particular investigations or adversely affect personal safety;
- personal information that is required to be protected under the provisions of the Privacy Act, the Archives Act, or other legislation.[ix]

1.18 Non-national security information can be given one of three security markings:

- X-in-Confidence—if compromise of it could cause 'limited damage' to the Commonwealth, the government, commercial entities or members of the public. Examples of this marking are Staff-in-Confidence, Security-in-Confidence, Commercial-in-Confidence and Audit-in-Confidence (but not Cabinet-in-Confidence);
- Protected—if compromise of it could cause 'damage' to the Commonwealth, the government, commercial entities or members of the public;
- Highly Protected—if compromise of it could cause 'serious damage' to the Commonwealth, the government, commercial entities or members of the public.[x]

1.19 The PSM notes that most non-national security information requiring classification is adequately protected by the first two of these markings, and that 'Highly Protected' should be used 'sparingly'.[xi]

1.20 The PSM stresses that government policy is to keep classified information to a minimum, so the mere fact that information falls under one of these categories is not sufficient to require classification—that becomes necessary only if the information could cause damage to national security or one of the non-national security groups mentioned above.[xii]

1.21 Information now held in Australia may have been classified by an overseas agency according to its own system. Australian agencies receiving such information may make their own assessment of the appropriate classification unless an agreement exists with the originating agency.[xiii]

1.22 Many of the terms that arise in a discussion of classified and security sensitive information—such as 'sensitive information', 'terrorism', 'in the interests of national security', 'operationally sensitive information' and 'matters of state'—are difficult to define and loaded with political connotations, and hence can be used to advance emotive rather than reasoned points of view. The term 'national security' is used in various contexts. It may be invoked as a source of power for government, such as under the defence power in the *Australian Constitution*; it may be used to describe a state interest or a reason for action by a state; or it may be used in a statute to create an exemption from rules that would otherwise apply.[xiv] National security can be used by government as a reason to withhold information, such as in a claim for public interest immunity in court proceedings (discussed in Chapter 8) or to remove from public scrutiny activities that would otherwise be public.

1.23 In the context of the current inquiry, it is important to remove the political and emotive overlay that accompanies such terminology in order to consider the issues raised by the Terms of Reference in a manner that will lead to better, more principled public policy in this area.

What is security sensitive information?

1.24 For the purposes of this inquiry, the Terms of Reference define 'security sensitive information' as 'information that has implications for Australia's security, but is not formally classified, for whatever reason.' Security sensitive information could be regarded as information associated with Australia's security, defence, international relations or national interest, but which is not of sufficient importance to lead to damage to those interests if it were to be publicly disclosed. Security sensitive information might include, for example, information that ought to have been classified but was not—whether through error, oversight or otherwise. However, it is less clear why security sensitive information merits special treatment if a decision has been made by the relevant agency not to classify it and grant it the protection of a security classification.

Question 1. What examples of *unclassified* security sensitive information can be provided?

Question 2. In what circumstances, if any, would unclassified security sensitive information warrant special treatment? Should the ALRC distinguish between classified information and security sensitive information in its consideration of the issues in this inquiry, and in its final recommendations?

Information covered by this inquiry

1.25 It is important to distinguish the information which is at the heart of this inquiry from other sensitive information which emerges in the course of law enforcement

operations. Police forces, prosecuting authorities, courts and defence lawyers often handle sensitive information in the investigation and prosecution of criminal offences, before and during trial. This information includes the identity and location of police informers, the identity and location of witnesses, and the details of undercover investigations. Disclosure of this information could endanger the viability of undercover operations and the lives of those involved in them, and there is a strong public interest in the successful detection and prosecution of criminal activity.

1.26 In some respects, the classified and security sensitive information that is central to this inquiry includes material of this sort. However, it is significantly different in that it includes information of the following sorts:

- information concerned with Australia's security, defence, international relations and other national interests;

- information, the existence of which is sensitive as it would reveal the existence of covert operations that could embarrass Australian or allied interests; and

- information which is generated by Australia's allies and which must be afforded protection in accordance with the interests and security procedures of those countries—revelation of which would also endanger the further exchange of security information.

1.27 The ramifications of the disclosure of classified and security sensitive information may also be significantly different from sensitive information surrounding law enforcement operations, and may include:

- identifying to foreign powers and others the capabilities (or limitations) of Australia's intelligence services;

- undermining international or diplomatic relations; and

- confirming the existence of matters which are otherwise only the subject of public speculation.

Who is responsible for classifying information?

1.28 The Commonwealth Protective Security Manual (PSM) states that the person responsible for classifying information is the person responsible for generating it ('the originator') or 'actioning' it if it is generated outside Australia.[xv] Only the originating agency (ie, the agency that assigned the original classification) can reclassify or declassify the information.[xvi]

1.29 The PSM does not suggest that there is any mechanism in place to review security classifications once made. The Manual simply notes that 'to keep the volume of security classified information to a minimum, agencies should limit the duration of

the classification and establish review procedures'.[xvii] Neither is there any system contemplated in the PSM for the routine re-consideration of a security classification, whether through the effluxion of time or by a challenge of some sort to its classification status.[xviii] Such a challenge might arise through a request under freedom of information legislation, or when a party—whether a government agency or a private entity or individual—seeks to use the information in court or some other public forum. The ALRC is interested in learning whether any such review procedures, whether formal or informal, are in place and, if so, how they operate.[xix]

Question 3. Within an agency generating or handling classified and security sensitive information, who is generally the 'originator' of that information? What level of seniority or security clearance is this person required to have?

Question 4. Is there, or should there be, any process for reviewing security classifications, whether as a matter of course or in response to a particular event:

(a) at the time that it is first classified;

(b) after the effluxion of time;

(c) in response to a challenge to its classification status; or

(d) when there is a need or threat to use that information in court or other public forum?

Some threshold questions

1.30 The ALRC is interested in learning how frequently investigations and proceedings arise which involve classified and security sensitive information. It appears that they are fairly rare—but they attract significant publicity when they do occur. What may be harder to determine is the number of potential prosecutions, civil court cases or other public proceedings that do *not* go ahead or are in some way frustrated because of the difficulties associated with protecting classified and security sensitive information in open proceedings.

1.31 At present, some cases involving classified or security sensitive information never get to trial in Australia and overseas. In large part this is because governments do not pursue some or all possible charges, or seek to secure a guilty plea (usually involving a lesser sentence) to avoid making classified or sensitive information public and to avoid the exposure and cross-examination of agents, even in restricted circumstances.[xx]

1.32 If such cases are in fact rare, is it necessary or desirable to establish new, restrictive or invasive procedures—especially where there is a fear or perception

(accurate or otherwise) that this would unduly impinge on civil liberties? Or would it be better to consider existing principles and procedures, recommend modifications where appropriate, but leave it to the courts and tribunals to determine the procedures to be followed on a case-by-case basis in line with these principles and in the light of the particular requirements of justice in each case?

Question 5. How often do cases involving classified or security sensitive information arise? How often are potential cases or other public proceedings involving classified or security sensitive information abandoned or otherwise frustrated in some way because of the difficulties associated with the public disclosure of classified and security sensitive information?

Question 6. If cases involving classified or security sensitive information are rare, is it necessary or desirable to establish special procedures to deal with them—especially if there are fears or perceptions that civil liberties will be unduly infringed? Would it be better to consider (and modify where necessary) some basic principles but leave it to the courts and tribunals to determine the procedures to balance the demands of justice and public interest in each case?

1.33 Section 24(1) of the *Australian Law Reform Commission Act 1996* (Cth) requires the ALRC, in performing its functions, to ensure that the laws, proposals and recommendations it reviews or considers

> (1) do not trespass unduly on personal rights and liberties or make the rights and liberties of citizens unduly dependent on administrative, rather than judicial, decisions; and
>
> (2) are, as far as practicable, consistent with the International Covenant on Civil and Political Rights.

1.34 The ALRC is also required to have regard to all of Australia's international obligations that are relevant to the matter which is the subject of an inquiry.[xxi]

Security and intelligence agencies

Australia's security agencies

1.35 The Australian Security Intelligence Organisation (ASIO) is Australia's best known security service. It is responsible for gathering information and intelligence to make assessments about risks to national security. The *Australian Security Intelligence Organisation Act 1979* (Cth) (ASIO Act) defines 'security' as the 'protection of Australia and its people from espionage, sabotage, politically motivated violence, the promotion of communal violence, attacks on Australia's defence system, and acts of foreign interference'.[xxii] ASIO provides security assessments for government agencies, including assessments of individuals seeking security clearances.[xxiii]

1.36 The Australian Secret Intelligence Service (ASIS) focusses on the collection of overseas intelligence about the capabilities, intentions and activities of individuals or organisations outside Australia which may impact on Australian interests and the well-being of its citizens. ASIS is not a police or law enforcement agency.[xxiv] There are a number of limits on the activities that ASIS can undertake; for example, the responsible Minister must make written rules in relation to the communication and retention of intelligence information about Australians, having regard to the need to ensure their privacy.[xxv]

1.37 The Defence Intelligence Organisation (DIO) is located within the Department of Defence. The DIO provides intelligence assessments from all sources at the national level to support the Department of Defence and wider government decision making, and the planning and conduct of defence force operations.[xxvi]

1.38 The Defence Signals Directorate (DSD) is also located within the Department of Defence. The Directorate has two main functions: to collect and disseminate foreign signals intelligence and to provide information about security products and services to the government and the defence forces.[xxvii]

1.39 The Office of National Assessments (ONA) was established under the *Office of National Assessments Act 1977* (Cth) as an agency providing information and advice directly to the Prime Minister. It produces reports and assessments on international political, strategic and economic matters for the Prime Minister, ministers and departments. ONA assessments are based on information available from all sources, both inside or outside government. Information is gathered from intelligence, diplomatic reporting and also public material such as news media and other publications. The ONA also consults people outside government who have expertise on the subject under study.[xxviii]

1.40 The Australian Federal Police (AFP) is the primary Commonwealth law enforcement agency, with responsibility for Commonwealth protective security, and the prevention, detection and investigation of criminal offences against the Commonwealth. The AFP was established by the *Australian Federal Police Act 1979* (Cth).

1.41 The Australian Crime Commission (ACC) was established under the *Australian Crime Commission Act 2002* (Cth) and commenced operations on 1 January 2003. It took over the functions of the National Crime Authority, the Australian Bureau of Criminal Intelligence and the Office of Strategic Crime Assessment. The ACC is designed to co-ordinate criminal intelligence with a view to setting enforcement priorities, conducting investigations of significant criminal activity (including taskforce co-ordination) and exercising coercive powers to assist in intelligence operations and investigations. The ACC is currently establishing priority investigation teams, the first of which will focus on illegal firearms.[xxix]

Who monitors their activities?

1.42 The Inspector-General of Intelligence and Security (IGIS) is an independent statutory officer within the Prime Minister's portfolio established by the *Inspector-General of Intelligence and Security Act 1986* (Cth). The IGIS monitors the activities of intelligence and security organisations in Australia, conducts inquiries, investigates complaints and provides annual reports to the federal Parliament.[xxx] The IGIS has powers to obtain information including requiring persons to answer questions and produce documents, to take sworn evidence and to enter agency premises.

1.43 The Parliamentary Joint Committee on ASIO, ASIS and the DSD is an amalgam of two previous separate Parliamentary committees overseeing those three agencies. The functions of the Committee are defined under s 29 of the *Intelligence Services Act 2001* (Cth) as:

- to review the administration and expenditure of ASIO, ASIS and DSD, including their annual financial statements;

- to review any matter in relation to ASIO, ASIS or DSD referred to the Committee by the responsible Minister or a resolution of either House of the Parliament; and

- to report the Committee's comments and recommendations to each House of the Parliament and to the responsible Minister.

1.44 The Joint Committee is not authorised to initiate its own references but may request the responsible Minister to refer a particular matter to it for review.[xxxi] The Joint Committee is specifically excluded from reviewing, amongst other things, the intelligence-gathering priorities of the agencies, their sources of information or other operational matters, and from conducting inquiries into individual complaints made against those agencies.

1.45 The Security Appeals Division of the federal Administrative Appeals Tribunal can hear two types of matters:

- applications for review of a qualified or negative security assessment made by ASIO under s 54 of the ASIO Act; and

- applications under the *Archives Act 1983* (Cth) for access, or partial access, to an ASIO record held by the Australian Archives.[xxxii]

Overseas security legislation and agencies

Canada

1.46 The Canadian Security and Intelligence Service (CSIS) is a civilian intelligence service established to collect, analyse and retain information concerning threats to the security of Canada.[xxxiii] The *Canadian Security and Intelligence Service Act 1985* defines 'threat to the security of Canada' as 'espionage, foreign influenced activities

within Canada detrimental to national interests, and activities supporting violence for a political objective or any unlawful acts'.[xxxiv] The CSIS has liaison offices in some other countries, and it is involved in the exchange of security intelligence information which concerns threats to the security of Canada.[xxxv] The Communications Security Establishment within the Canadian Department of National Defence is responsible for providing the Canadian government with foreign intelligence, and seems to be similar to the DSD in Australia.[xxxvi]

United Kingdom

1.47 In the UK, the *Intelligence Services Act 1989* governs secret service arrangements. The British Security Service (also known as MI5) is responsible for security intelligence work against threats to national security, including terrorism, espionage and serious crime. In addition, MI5 also provides security advice to a range of other organisations.[xxxvii] The Secret Intelligence Organisation (formerly known as MI6) is the British equivalent of ASIS, with a focus on overseas information. It was not officially recognised under any statute until 1994, when it was brought under the *Intelligence Services Act*.[xxxviii] Both organisations report to the parliamentary Intelligence and Security Committee—although this does not have the status of a normal parliamentary committee, since the members report to the Prime Minister rather than to Parliament.[xxxix]

United States of America

1.48 The United States has two well known intelligence bodies: the Central Intelligence Agency (CIA) and the Federal Bureau of Investigation (FBI). A number of other organisations also deal with security, including the National Security Agency, the Defence Intelligence Agency and the Customs Service.[xl] The CIA was created in 1947 by the *National Security Act*. Its operations are overseen by the security committees of Congress.[xli] The CIA provides intelligence on national security topics and conducts counter-intelligence activities, 'special activities', and other functions related to foreign intelligence and national security, as directed by the US President.[xlii] This interventionist charter is said to differentiate the CIA from similar agencies in other countries.[xliii]

1.49 The FBI is the investigative arm of the US Department of Justice. Among other things, it has a role in investigating terrorism and foreign intelligence activities from a domestic perspective. It differs from an organisation like ASIO in that its operatives are law enforcement agents (all of whom are qualified in law or accountancy) with police powers, including the use of force.[xliv] House of Representative and Senate Committees oversee the operations of the CIA and FBI, and may hold in camera hearings.[xlv]

1.50 In late 2001, the US Government established a new Department of Homeland Security. This Department is intended to draw together a number of existing responsibilities, such as border control and transport, to provide greater coordination of

efforts to prevent terrorist attacks within the USA and minimise damage should those attacks occur.[xlvi]

2. Open Government

Accountability of the Executive

2.1 It is a central tenet of a representative democracy that the government be open to account for its actions, policies and administrative decisions. The interests of the government of the day are not necessarily those of the state or the public generally. A key part of this accountability is public access to the information on which action and policies are based.[xlvii] Balanced against this is the interest of the state in keeping some information secret.

> Categorising national security issues is particularly troubling, since they fall at once into both camps: secrecy is essential to the conduct of foreign relations and defence strategy; at the same time, however, it stifles domestic democratic processes and citizens' first amendment rights to debate controversial issues of national policy.[xlviii]

2.2 One barrier to public access to information is a claim of public interest immunity (discussed in Chapter 9) frequently used in the court and tribunal proceedings being considered by the ALRC in this inquiry. However, access to government information is regulated in a number of other ways—those considered here are freedom of information laws, privacy law and legislation protecting public interest disclosures made by 'whistleblowers'.[xlix]

Freedom of information

2.3 A general review of the operation of freedom of information laws—which allow access to many types of information held by the government—is outside the scope of this inquiry. Nevertheless, it is important to understand the general principles underlying the way in which the government handles classified and security sensitive information in this context.

2.4 The *Freedom of Information Act 1982* (Cth) (FOI Act) gives individuals certain rights of access to information held by the government. These rights are not unqualified: in some circumstances they are balanced against the need for secrecy or confidentiality in certain areas of government decision making. Section 7 of the FOI Act provides a blanket exemption to those agencies conducting intelligence work or whose central purpose is national security activities.[l] Various documents produced by other security agencies are also exempted.

2.5 Other Commonwealth agencies which handle a significant amount of material related to national security, such as the Department of Foreign Affairs and Trade, the Department of Immigration, Multicultural and Indigenous Affairs and the Australian Federal Police (AFP), are open to the FOI process. However, access to sensitive documents may be denied on the basis of one of the specific grounds of exemption under s 33 of the FOI Act.[li]

2.6 Section 33(1) of the Act provides:

> A document is an exempt document if disclosure of the document under this Act:
>
> (a) would, or could reasonably be expected to, cause damage to:
> (i) the security of the Commonwealth;
> (ii) the defence of the Commonwealth; or
> (iii) the international relations of the Commonwealth; or
>
> (b) would divulge any information or matter communicated in confidence by or on behalf of a foreign government, an authority of a foreign government or an international organization to the Government of the Commonwealth, to an authority of the Commonwealth or to a person receiving the communication on behalf of the Commonwealth or of an authority of the Commonwealth.

2.7 Section 4(5) defines, in part, what is meant by 'security of the Commonwealth':

> Without limiting the generality of the expression *security of the Commonwealth*, that expression shall be taken to extend to:
>
> (a) matters relating to the detection, prevention or suppression of activities, whether within Australia or outside Australia, subversive of, or hostile to, the interests of the Commonwealth or of any country allied or associated with the Commonwealth; and
>
> (b) the security of any communications system or cryptographic system of the Commonwealth or of another country used for:
> (i) the defence of the Commonwealth or of any country allied or associated with the Commonwealth; or
> (ii) the conduct of the international relations of the Commonwealth.

2.8 Section 33(2) authorises a Minister to certify that 'a document is an exempt document for a reason referred to in subsection (1)'. A decision to exempt in this fashion can be reviewed by the Administrative Appeals Tribunal (AAT).[lii] In *Re Anderson and the Australian Federal Police*, the claims for exemption by the AFP were not based on national security but, amongst other things, protection of witnesses, sources and investigation techniques.[liii] In that case, the AAT upheld the claim for exemption (after it had inspected the documents) on the ground that disclosure would reveal confidential sources of information. The AAT made a similar evaluation of a document classified as 'Secret'.[liv]

2.9 Hanks, Lee and Morabito conclude that the many exemptions to access rights under freedom of information legislation result in very restricted access to information that might have national security implications. They further note that the US *Freedom of Information Act* contains no blanket exemption of security intelligence agencies and that its exemption for security sensitive information is subject to judicial review.[lv] However, this approach may now have changed in the US, where Attorney General John Ashcroft recently directed that, in response to the numerous FOI requests for information on names of detainees being secretly held by the US government, information be withheld by agencies as a matter of policy, regardless of whether disclosure would be harmful.[lvi]

Question 7. In practice, do the exemptions in the *Freedom of Information Act 1982* (Cth) result in the inadequate protection, or over-protection, of classified or security sensitive information?

Question 8. Are ministerial certificates under s 33(2) of the *Freedom of Information Act 1982* (Cth) often issued or challenged in the Administrative Appeals Tribunal? What procedures does the Tribunal use to consider the status of material covered by a ministerial certificate?

Privacy

2.10 Under federal law, privacy of personal information is governed by the *Privacy Act 1988* (Cth). The *Privacy Act* aims to protect personal information about individuals and allow them some control over how that information is collected, used, stored, controlled and disclosed. It also gives individuals rights to access and correct their own personal information.[lvii]

2.11 The *Privacy Act* contains privacy safeguards set out in a number of Information Privacy Principles (IPPs) and National Privacy Principles (NPPs), which have the force of law.[lviii] The IPPs cover the collection, storage and security, use and disclosure of, and access to, 'personal information', which is in a 'record' held by an 'agency', as those terms are defined in the Act. With limited exceptions, these agencies include only Commonwealth and ACT public sector entities.

2.12 The Federal Privacy Commissioner has a number of statutory functions in relation to complaint handling, investigations of breaches of the Act and enforcement. Under Part V of the Act, the Commissioner has the power to investigate complaints,[lix] obtain information and documents[lx] and examine witnesses.[lxi] The Commissioner's determinations may be enforced by proceedings in the Federal Court of Australia or the Federal Magistrates Service.[lxii]

2.13 The *Privacy Act* regime is not specifically connected to issues of national security. However, under NPP 6.1 there are exemptions to the principles on grounds related to national security: if an organisation holds personal information about an individual, it must provide the individual with access to the information on request by the individual, except to the extent that:

> (j) providing access would be likely to prejudice:
>
> (i) the prevention, detection, investigation, prosecution or punishment of criminal offences, breaches of a law imposing a penalty or sanction or breaches of a prescribed law; or
>
> (ii) the enforcement of laws relating to the confiscation of the proceeds of crime; or

(iii) the protection of the public revenue; or

(iv) the prevention, detection, investigation or remedying of seriously improper conduct or prescribed conduct; or

(v) the preparation for, or conduct of, proceedings before any court or tribunal, or implementation of its orders;

by or on behalf of an enforcement body; or

(k) an enforcement body performing a lawful security function asks the organisation not to provide access to the information on the basis that providing access would be likely to cause damage to the security of Australia.

2.14 One of the IPPs may also be of interest in relation to the collection of information regarding a person that is then proposed to be used for another purpose. Principle 11, *Limits on the Use of Personal Information*, states:

1. A record-keeper who has possession or control of a record that contains personal information that was obtained for a particular purpose shall not use the information for any other purpose unless:

(a) the individual concerned has consented to use of the information for that other purpose;

(b) the record-keeper believes on reasonable grounds that use of the information for that other purpose is necessary to prevent or lessen a serious and imminent threat to the life or health of the individual concerned or another person;

(c) use of the information for that other purpose is required or authorised by or under law;

(d) use of the information for that other purpose is reasonably necessary for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue; or

(e) the purpose for which the information is used is directly related to the purpose for which the information was obtained.

2. Where personal information is used for enforcement of the criminal law or of a law imposing a pecuniary penalty, or for the protection of the public revenue, the record-keeper shall include in the record containing that information a note of that use.[lxiii]

2.15 Information that could prejudice the security, defence or international relations of Australia need not be disclosed under the *Privacy Act* regime. Section 70 of the FOI Act allows the Attorney-General to give the Federal Privacy Commissioner a certificate denying the Commissioner the power that he or she would otherwise have had to require the production of specified material or documents if to do so would be contrary to the public interest. The Federal Privacy Commissioner has informed the ALRC that this provision has not yet been invoked.[lxiv]

Question 9. Does the *Privacy Act 1988* (Cth) draw an appropriate balance between the collection, storage, use, control and disclosure of, and access to personal information, and the protection of classified and security sensitive information?

Protection of whistleblowers

2.16 Some legislation seeks to protect 'whistleblowers'—people who make certain public interest disclosures—from some of the consequences that might normally follow such disclosures, such as prosecution, and from other reprisals. The underlying principle in this legislation is that the public interest in learning about fraud or other incompetent or improper conduct by government officials outweighs the normal public or other interests in keeping certain information secret. The protection of 'whistleblowers' is an area in which there can be a direct tension between the public interest in protecting classified and security sensitive information and the public interest in facilitating the disclosure of such information, without reprisal, where it will assist in the elimination of fraud or impropriety.[lxv]

Whistleblower legislation in Australia

2.17 Most States and Territories have some form of whistleblower protection legislation.[lxvi] These Acts limit the liability of people who make public interest disclosures and limit the legal action that can be taken against them on the basis of having made such disclosures.[lxvii] The Acts also make provision for prosecution in the case of unlawful reprisals,[lxviii] and for whistleblowers to seek damages if they suffer reprisals.[lxix]

2.18 The Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Cth), which is to a great extent modelled on the *Public Interest Disclosure Act 1994* (ACT), was introduced into the Senate by Senator Andrew Murray as a private member's bill on 11 December 2002. The proposed legislation aims to provide a comprehensive Commonwealth public sector whistleblowing scheme and 'to enable a person to report improper conduct in the knowledge that the allegation will be duly investigated and that he or she will not suffer from reprisals on account of disclosing such information'.[lxx] However, the Finance and Public Administration Legislation Committee, a Senate Standing Committee, has recommended that the Bill not proceed in its current form, although it 'recognises the need for separate legislation addressing the matter of whistleblowing and supports the general intent of the Bill'.[lxxi] Accordingly, the *Public Service Act 1999* (Cth) continues to be the only relevant federal legislation in force, but it offers only limited protection to, and coverage of, Commonwealth public sector whistleblowers.

2.19 Section 16 of the *Public Service Act 1999* (Cth), headed *Protection for Whistleblowers*, provides that:

> A person performing functions in or for an Agency must not victimise, or discriminate against, an APS employee because the APS employee has reported breaches (or alleged breaches) of the Code of Conduct[lxxii] to:
>
> (a) the Commissioner[lxxiii] or a person authorised for the purposes of this section by the Commissioner; or
>
> (b) the Merit Protection Commissioner[lxxiv] or a person authorised for the purposes of this section by the Merit Protection Commissioner;
>
> (c) an Agency Head or a person authorised for the purposes of this section by an Agency Head.

2.20 The Senate Finance and Public Administration Legislation Committee considers that the scope of s 16 is limited as it only applies to that part of the public sector covered by the Act, and the Act only applies to about half of the Commonwealth public sector.[lxxv] Of relevance to this inquiry is the fact that officers and employees of the Australian Security Intelligence Organisation (ASIO) are not subject to the *Public Service Act 1999*[lxxvi] and hence are not covered by s 16 of that Act.

2.21 Further, there are no provisions in the *Australian Security Intelligence Organisation Act 1979* (Cth) dealing with whistleblowing procedures or whistleblowing protections for ASIO officers and employees. Similarly, the Australian Federal Police (AFP) is not an Australian Public Service agency and hence its employees are not covered by s 16. There are no provisions in the *Australian Federal Police Act 1979* (Cth) dealing with whistleblowing procedures or whistleblowing protections for AFP officers and employees. By contrast, the Department of Defence and the Office of Inspector-General of Intelligence and Security are Australian Public Service agencies and hence employees of those organisations appear to be covered by s 16 of the *Public Service Act 1999*.[lxxvii]

2.22 It is unclear whether s 16 of the *Public Service Act 1999* applies to the Australian Secret Intelligence Service (ASIS). Section 35 of the *Intelligence Services Act 2001* (Cth) provides that:

> Although employees of ASIS are not employed under the *Public Service Act 1999*, the Director-General must adopt the principles of that Act in relation to employees of ASIS to the extent to which the Director-General considers they are consistent with the effective performance of the functions of ASIS.

When is disclosure in the public interest?

2.23 The Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Cth) and the *Public Interest Disclosure Act 1994* (ACT) have similar definitions of a 'public interest disclosure'. In the Bill it is defined as a disclosure of information that the person making the disclosure believes on reasonable grounds tends to show:

> (a) that another person has engaged, is engaging, or proposes to engage, in disclosable conduct; or

(b) public wastage; or

(c) conduct involving substantial risk to the environment; or

(d) that a person has engaged, is engaging, or proposes to engage, in an unlawful reprisal; or

(e) that a public official has engaged, is engaging, or proposes to engage, in conduct that amounts to a substantial and specific danger to the health or safety of the public;

and includes an anonymous disclosure.[lxxviii]

2.24 'Disclosable conduct' would, if proven, constitute either a criminal or disciplinary offence, or reasonable grounds for dismissing or terminating the services of a public official.[lxxix] Types of disclosable conduct covered by the Bill include:

(a) Conduct of a person (whether or not a public official) that adversely affects, or could adversely affect ... the honest or impartial performance of official functions by a public official or agency;

(b) Conduct of a public official which amounts to the performance of any of his or her official functions dishonestly or with partiality;

(c) Conduct of a public official, a former public official or an agency that amounts to a breach of public trust;

(d) Conduct of a public official, a former public official or an agency that amounts to the misuse of information or material acquired in the course of the performance of official functions (whether for the benefit of that person or agency or otherwise);

(e) Conduct of a public official of a kind that amounts to maladministration which is action or inaction of a serious nature that is:

(i) contrary to law; or

(ii) unreasonable, unjust, oppressive or improperly discriminatory; or

(iii) based wholly or partially on improper motives;

(f) a conspiracy or attempt to engage in conduct referred to in paragraphs (a) to (e) (inclusive).[lxxx]

2.25 The definition of 'public interest disclosure' makes no specific reference to a disclosure that reveals classified or security sensitive information. The issue arises whether whistleblowers are improperly discouraged from coming forward where classified or security sensitive information is involved. If so, should whistleblower legislation explicitly provide that its protections extend to persons who reveal classified or security sensitive information? What safeguards might need to be imposed to protect against abuse of such protection?

Who can make a public interest disclosure?

2.26 Australian legislation makes a distinction between public interest disclosures that can be made by 'any person' and those that must be made by a public official. For example, any person can make a public interest disclosure under the legislation in Victoria and the ACT, and under the Commonwealth Bill.[lxxxi] In contrast, the legislation in NSW and Tasmania provides that disclosures must be made by a public official or public officer.[lxxxii]

2.27 In considering the Public Interest Disclosure Bill 2002, the Senate Finance and Public Administration Legislation Committee supported the enabling of all members of the public to make public interest disclosures.[lxxxiii]

2.28 There are provisions of varying effect in the legislation relating to anonymous disclosures. For example, under the ACT legislation an anonymous disclosure need not be investigated.[lxxxiv] The Victorian legislation specifically allows anonymous disclosures in relation to improper conduct.[lxxxv] Clause 15 of the Commonwealth Bill provides for a person to make an anonymous disclosure in accordance with the section, and for that disclosure to be protected.[lxxxvi]

Penalties

2.29 State and territory whistleblower laws set penalties of varying magnitude for offences including breach of confidentiality by a public official,[lxxxvii] provision of false or misleading information[lxxxviii] and unlawful reprisal.[lxxxix] The wording of each offence differs in detail across the legislation.

Whistleblower legislation overseas

United States

2.30 In the United States, employees of the National Security Agency, the FBI and the CIA are excluded from the *Whistleblower Protection Act 1989* (USA). The US Department of Justice established a separate system for the protection of FBI whistleblowers in 1999, but it affords less protection than the legislation.

> For example, under the rules of the system, FBI whistleblowers are protected only if they report misdeeds to a short list of FBI and Justice Department officials—not to Congress, in court, or to supervisors. FBI personnel also have no right to federal court review.[xc]

2.31 Recently, FBI agent Coleen Rowley 'blew the whistle' on the FBI for allegedly mishandling the investigation of Zacarias Moussaoui, an alleged conspirator in the terrorist attacks on the World Trade Centre and the Pentagon on 11 September 2001.[xci] As FBI agents are not covered by the whistleblower legislation, members of the Senate requested the US Attorney General to promise that Agent Rowley would not face reprisals for her actions.[xcii]

2.32 Employees of the newly created US Department of Homeland Security will have whistleblower protections.[xciii] Early versions of the homeland security legislation did not include such protections.[xciv] Senator Chuck Grassley (Republican–Iowa) insisted

that the whistleblower protections be added to the final Bill.[xcv] Senator Grassley is a co-author of the *Whistleblower Protection Act 1989* (USA). He has stated:

> Government agencies too often want to cover up their mistakes, and the temptation is even greater when bureaucracies can use a potential security issue as an excuse. At the same time, the information whistleblowers provide is all the more important when public safety and security is at stake … Any bill to create a new agency without whistleblower protection is doomed to foster a culture that protects its own reputation before the security of the homeland.[xcvi]

Other overseas legislation

2.33 Other international legislation dealing with whistleblower protection includes New Zealand's *Protected Disclosures Act 2000*, South Africa's *Protected Disclosures Act 2000* and the UK's *Public Interest Disclosure Act 1998*. None of the protections available to whistleblowers under the UK Act extends to those employed by the security and intelligence services, even where they disclose illegalities and incompetence. ARTICLE 19 and Liberty[xcvii] have recommended that the 'protections of the [UK Act] should apply to security and intelligence personnel'.[xcviii]

2.34 New Zealand's *Protected Disclosures Act 2000* provides for the protection of disclosures of information relating to intelligence and security and international relations.[xcix] Section 12 of the Act states that the internal procedures of an intelligence and security agency must:

> (a) provide that the persons to whom a disclosure may be made must be persons holding an appropriate security clearance and be authorised to have access to the information; and
>
> (b) state that the only appropriate authority to whom information may be disclosed is the Inspector-General of Intelligence and Security; and
>
> (c) invite any employee who has disclosed, or is considering the disclosure of, information under this Act to seek information and guidance from the Inspector-General of Intelligence and Security, and not from the Ombudsman; and
>
> (d) state that no disclosure may be made to an Ombudsman, or to a Minister of the Crown other than–
>
> (i) the Minister responsible for the relevant intelligence and security agency; or
>
> (ii) the Prime Minister.

Johannesburg Principles

2.35 The *Johannesburg Principles on National Security, Freedom of Expression and Access to Information* were adopted by 'a group of experts in international law, national security, and human rights convened by ARTICLE 19, the International Centre Against Censorship, in collaboration with the Centre for Applied Legal Studies of the University of Witwatersrand' in Johannesburg, South Africa.[c] The aim of the

Johannesburg Principles is to 'clarify the meaning of—and the scope of justifiable limitations upon—the right to free expression as contained in various international conventions and covenants', including the European Convention on Human Rights.[ci]

2.36 The Johannesburg Principles have no legal force but reinforce the principle underlying whistleblower legislation that, in some circumstances, individuals should be allowed to determine what is in the public interest without suffering reprisal.

2.37 Principle 15 of the Johannesburg Principles provides:

> No person may be punished on national security grounds for disclosure of information if (1) the disclosure does not actually harm and is not likely to harm a legitimate national security interest, or (2) the public interest in knowing the information outweighs the harm from disclosure.

2.38 Principle 16 provides:

> No person may be subjected to any detriment on national security grounds for disclosing information that he or she learned by virtue of government service if the public interest in knowing the information outweighs the harm from disclosure.

Question 10. Are the current arrangements under s 16 of the *Public Service Act 1999* (Cth) adequate to deal with disclosures by whistleblowers that reveal classified or security sensitive information?

Question 11. Should Commonwealth legislation provide a specific scheme for the protection of whistleblowers for the disclosure of classified or security sensitive information which they believe on reasonable grounds is in the public interest? Who should be covered by such legislation? Should whistleblower protection be extended to officers of Australia's intelligence and investigative agencies and defence forces? What safeguards against might be necessary?

3. Commonwealth Protective Security Manual

3.1 The Terms of Reference ask the ALRC to consider the enforceability of protective security standards set out in the Commonwealth Protective Security Manual (PSM). Specific criminal offences for the unauthorised disclosure of classified and security sensitive, and other government-held, information are considered in Chapter 4.

What is the PSM?

3.2 The PSM is issued by the Attorney-General.

> It is the principal means for disseminating Commonwealth protective security policies, principles, standards and procedures to be followed by all Commonwealth agencies for the protection of official resources.[cii]

3.3 The PSM sets out minimum standards in protective security for all Commonwealth agencies, and for contractors and their employees who perform services for or on behalf of the Commonwealth. It is of particular relevance to agencies concerned with national security matters and law enforcement. The PSM sets minimum standards in each of the following eight areas:

A. Protective Security Policy
B. Guidelines on Managing Security Risk
C. Information Security
D. Personnel Security
E. Physical Security
F. Security Framework for Competitive Tendering and Contracting
G. Guidelines on Security Incidents and Investigations
H. Security Guidelines on Home-based Work.

3.4 Part C of the PSM, which deals with information security, is of particular relevance to this inquiry. It describes the government's classification system in relation to national security and non-national security material[ciii] and sets out 29 minimum standards in relation to information security, including the following key matters:

- Where the compromise of official information could cause harm to the nation, the public interest, the government or other entities or individuals, agencies must consider giving the information a security classification.[civ]

- Once information has been security classified, agencies must observe the minimum procedural requirements for the use, storage, transmission and disposal of security classified information.[cv]

- Agencies must take all reasonable and appropriate precautions to ensure that only people with a demonstrated need to know and the appropriate security clearance gain access to security classified information.[cvi]

- Once information has been identified as requiring security classification, a protective marking must be assigned to the information,[cvii] from which flow certain consequences about the way in which it must be handled, used and disseminated.

Enforceability of the standards

3.5 There are a number of statements within the PSM itself that the standards prescribed by the PSM are not legally enforceable. For example:

> Although the minimum standards and general guidelines provided in the PSM are not legally prescribed, they reflect the aims and objectives of the Commonwealth government and legislation relating to protective security. Therefore, agencies and their employees must adhere to at least the minimum standards in order to fulfil their portfolio responsibilities.[cviii] …
>
> The security classification system and the protective markings carry no direct implications in law; they are instead administrative labels that indicate the mandatory requirements for a minimum level of protection. They will, however, help agencies to meet legislative requirements for protecting official information.[cix]

3.6 The PSM allows for waiver of certain minimum standards.

> If an agency is unable to adhere to a particular minimum standard, policy or procedure in the PSM, the agency head may waive that requirement only in limited circumstances. The waiver would be sought only:
>
> - for a defined purpose
> - for a nominated period of time.[cx]

3.7 While the standards are not enforceable in the sense that a breach of the standards *per se* would not appear to give the government a cause of action against the breaching party, there are three ways that the standards could be indirectly enforceable:

- If a breach of the standards also constitutes a breach of contract (see below);

- If a breach of the standards also constitutes a breach of the APS Code of Conduct (see discussion below); or

- If a breach of the standards also constitutes a breach of any of the legislation covering protective security such as the *Crimes Act 1914* (Cth), the *Freedom of Information Act 1982* (Cth) and the *Privacy Act 1988* (Cth) (see Chapter 4).

Breach of contract

3.8 If compliance with the minimum standards of the PSM were made part of a contractual agreement (for example, between an agency and an employee, or an agency and a contractor), a breach of the standards by an employee or contractor could found a claim for breach of contract by the agency. In this regard, the PSM provides that a contract between an agency and a contractor must clearly say that the contractor is required to comply with the minimum standards for protecting security classified information as set out in the PSM.[cxi] Any additional agency-specific security requirements are to be separately specified in the contract or in a schedule to the contract.[cxii] The PSM also states:

> Agencies need to recognise the limitations inherent in example clauses in preparing [competitive tendering and contracting] documentation. It is not possible to develop a single set of standard documentation to suit all parties, circumstances, objectives, risks and desired outcomes. Agencies are therefore advised to obtain legal advice to ensure that the contract sets out in detail, and in a **legally enforceable manner**, the security requirements and outcomes identified by the agencies. [emphasis added][cxiii]

3.9 However, this does not necessarily provide any real penalty for a breach of the security standards. A contractor in breach of the PSM's security standards may find that its contract with the Commonwealth is terminated or not renewed. The Commonwealth's only other recourse for a breach of contract is likely to be a civil suit for damages. Monetary damages would be difficult to assess, relatively low in amount, and in any event unlikely to be any real compensation or penalty for the damage caused by the disclosure.

APS Code of Conduct

3.10 Section 13 of the *Public Service Act 1999* (Cth) sets out the Australian Public Service (APS) Code of Conduct, which binds APS employees, Agency Heads and statutory office holders.[cxiv] Among the requirements included in the Code of Conduct are the following:

- An APS employee must act with care and diligence in the course of APS employment.[cxv]

- An APS employee must comply with any lawful and reasonable direction given by someone in the employee's agency who has authority to give the direction.[cxvi]

- An APS employee, when acting in the course of APS employment, must comply with all applicable Australian laws.[cxvii]

  An employee must not make improper use of:

  (a) inside information; or
  (b) the employee's duties, status or power or authority;

  in order to gain, seek to gain, a benefit or advantage for the employee or for any other person.[cxviii]

3.11 There may be circumstances where a breach of the minimum standards could constitute a breach of the APS Code of Conduct. For example, a failure to comply with a directive to adhere to the minimum standards in the PSM, or to other particular minimum standards, could constitute a breach of s 13(2) or (5) of the *Public Service Act 1999* (Cth).

3.12 The Act provides that an Agency Head may impose the following sanctions against employees who have been found (under procedures established under the Act)[cxix] to have breached the Code of Conduct:

a) termination of employment;

b) reduction in classification;

c) re-assignment of duties;

d) reduction in salary;

e) deductions from salary by way of fine;

f) a reprimand.[cxx]

3.13 The Act does not specify sanctions for Agency Heads who have breached the Code of Conduct.

3.14 The *Public Service Regulations 1999* (Cth) provide that:

> An Agency Head may suspend an APS employee employed in the Agency from duties if the Agency Head believes on reasonable grounds that:
>
> (a) the employee has, or may have, breached the Code of Conduct; and
>
> (b) the employee's suspension is in the public, or the Agency's, interest.[cxxi]

Australian National Audit Office audits

3.15 Regardless of whether the minimum standards in the PSM are adequate and enforceable in principle, it is important to know whether they are complied with in practice.

3.16 The Australian National Audit Office (ANAO) has conducted a number of audits in relation to protective security matters addressed in the PSM. In one audit, the ANAO reviewed the security clearance and vetting policies and practices in a number of Commonwealth organisations to ascertain if the processes were being handled effectively and efficiently, and in accordance with Commonwealth policy as outlined in the PSM.[cxxii] The results of the audit highlighted that the 'management of personnel security needs to be improved in many respects to ensure compliance with the requirements of PSM 2000'.[cxxiii]

3.17 In a more recent audit, the ANAO considered whether the protective security practices and policies of seven Commonwealth agencies had established an appropriate security control framework based on the principles set out in Part E of the PSM.[cxxiv] The ANAO concluded 'that all agencies in the audit had made reasonable progress towards meeting their physical security responsibilities as outlined in the [PSM]'[cxxv] but identified a number of deficiencies across the agencies reviewed.[cxxvi]

Comparison with the US

3.18 In the United States, *Executive Order 13292—Further Amendment to Executive Order 12958, As Amended: Classified National Security Information* (EO 13292) issued by the US President prescribes a uniform system for classifying, safeguarding, and declassifying national security information, including information relating to defence against 'transnational terrorism'.[cxxvii] For example, EO 13292 sets out and describes the classification levels 'Top Secret', 'Secret' and 'Confidential';[cxxviii] deals with who has classification authority;[cxxix] duration of classification;[cxxx] identification and markings;[cxxxi] classification challenges;[cxxxii] and sets up an Interagency Security Classification Appeals Panel.[cxxxiii] EO 13292 sets out a number of classification prohibitions and limitations.[cxxxiv] For example, it prohibits the classification of information in order to:

> (a) conceal breaches of the law, inefficiency, or administrative error;
>
> (b) prevent embarrassment to a person, organization, or agency;
>
> (c) restrain competition; or
>
> (d) prevent or delay the release of information that does not require protection in the interest of the national security.[cxxxv]

3.19 EO 13292 is enforceable; breach of the order *per se* attracts sanctions. Section 5.5 of the Order provides:

> (a) If the Director of the Information Security Oversight Office finds that a violation of this order or its implementing directives has occurred, the Director shall make a report to the head of the agency or to the senior agency official so that corrective steps, if appropriate, may be taken.
>
> (b) Officers and employees of the United States Government, and its contractors, licensees, certificate holders, and grantees shall be subject to appropriate sanctions if they knowingly, wilfully or negligently:
>
> (1) disclose to unauthorized persons information properly classified under this order or predecessor orders;
>
> (2) classify or continue the classification of information in violation of this order or any implementing directive;
>
> (3) create or continue a special access program contrary to the requirements of this order; or

(4) contravene any other provision of this order or its implementing directives.

(c) Sanctions may include reprimand, suspension without pay, removal, termination of classification authority, loss or denial of access to classified information, or other sanctions in accordance with applicable law and agency regulation.

(d) The agency head, senior agency official, or other supervisory official shall, at a minimum, promptly remove the classification authority of any individual who demonstrates reckless disregard or a pattern of error in applying the classification standards of this order.

(e) The agency head or senior agency official shall:

(1) take appropriate and prompt corrective action when a violation or infraction under paragraph (b) of this section occurs; and

(2) notify the Director of the Information Security Oversight Office when a violation under paragraph (b)(1), (2) or (3) of this section occurs.[cxxxvi]

Question 12. Does the fact that the minimum standards in the Commonwealth Protective Security Manual are not of themselves enforceable present any problems for the protection of classified and security sensitive information? If so, in what way are the alternative methods of enforcement—such as contractual obligations, enforcement of the APS Code of Conduct and current legislative provisions outlawing unauthorised disclosure—inadequate?

Question 13. Should the minimum standards in the Commonwealth Protective Security Manual be made enforceable *per se* (as opposed to being enforceable because a breach of them may constitute a breach of contract, a breach of the APS Code of Conduct or a breach of legislation covering protective security matters)? If so, how?

Question 14. What should the appropriate penalties be for breach of the minimum standards in the Commonwealth Protective Security Manual?

Question 15. Is there any problem or issue within Australia's investigative agencies with respect to over-classification of information or abuse of the classification process that would warrant changes to the procedures in the Commonwealth Protective Security Manual? For example, should there be a standard stating that, if there is any significant doubt about the appropriate level of classification of information, it should be classified at the lower level?

Question 16. Should the Commonwealth Protective Security Manual include a standard that sets out the circumstances in which, or the purposes for which, the classification of information is prohibited?

Question 17. Should the minimum standards establish review procedures in relation to classification decisions made at the following times:[cxxxvii]

(a) when the classification decision is made;

(b) after the effluxion of time;[cxxxviii]

(c) when a classification decision is challenged; and

(d) when the release of classified or security sensitive information is necessary or threatened in court or tribunal proceedings?

Question 18. Should there be a security classification review panel independent of any one government agency to review security classification decisions?

Question 19. Are there any other issues arising from the Commonwealth Protective Security Manual that the ALRC ought to be considering?

4. Penalties for Unauthorised Disclosure

4.1 In considering whether existing mechanisms for the protection of classified and security sensitive information are adequate, it is relevant to look at the penalties currently in place for improper disclosure. Several pieces of Commonwealth legislation provide for penalties for the unauthorised disclosure of classified, security sensitive and other information. The ALRC will be considering the frequency with which these provisions have been used.

Unauthorised disclosure by Commonwealth officers

Public Service Act 1999 (Cth)

4.2 Section 13 of the *Public Service Act 1999* (Cth) sets out the Australian Public Service Code of Conduct, which binds APS employees, Agency Heads and statutory office holders (see Chapter 3). Among the requirements included in the Code of Conduct is that an employee must not make improper use of inside information or the employee's duties, status or power or authority in order to gain, seek to gain, a benefit or advantage for the employee or for any other person.[cxxxix]

4.3 The Act provides that an Agency Head may impose various sanctions against employees who have been found (under procedures established under the Act)[cxl] to have breached the Code of Conduct, including termination of employment, reduction in classification, deductions from salary by way of fine, and a reprimand.[cxli]

Crimes Act 1914 (Cth), s 70

4.4 Under the *Crimes Act 1914* (Cth), s 70, a Commonwealth officer who discloses information obtained in the course of employment where there is a duty not to disclose it is guilty of an offence. The maximum penalty for the offence is imprisonment for two years. This provision is cast very broadly. Unlike the espionage provisions discussed below, it does not distinguish between the disclosure of information that is harmful to the public interest and information that is not. In addition, there is no need for the prosecution to show that the officer knew that he or she was in breach of a duty not to disclose.[cxlii]

Intelligence Services Act 2001 (Cth)

4.5 Under s 39 of the *Intelligence Services Act 2001*, any ASIS employee, agent or contractor who makes an unauthorised communication of information related to ASIS functions is guilty of an offence. The penalty for a breach of s 39 is a fine of 120 penalty units, two years' imprisonment or both.[cxliii]

4.6 Section 41 of the *Intelligence Services Act 2001* creates an offence for any person to make public the identity of an ASIS agent or staff member other than the Director-General (or other people determined by the Director-General). It is also an

offence to make public any information from which the identity of the person could reasonably be inferred or established. The penalty for a breach of s 41 is a fine of 60 penalty units, one year's imprisonment, or both.[cxliv]

Australian Security Intelligence Organisation Act 1979 (Cth)

4.7 Section 81 of the ASIO Act relates to the operations of the Security Appeals Division of the Administrative Appeals Tribunal (AAT). The section creates an offence if a person who is or has been a member or an officer of the AAT makes a record of, or divulges or communicates to any person, any information acquired by reason of his or her office or employment under or for the purposes of the ASIO Act, or produces to any person a document furnished for the purposes of the ASIO Act. The penalty for an offence under this section is imprisonment for two years.

Australian Crime Commission Act 2002 (Cth)

4.8 Section 51 of the *Australian Crime Commission Act 2002* (Cth) makes it an offence for certain personnel of the Australian Crime Commission to record or divulge certain information. An offence under this section is punishable on summary conviction by a fine not exceeding 50 penalty units (currently $5,500) or imprisonment for a period not exceeding one year, or both.

Inspector-General of Intelligence and Security Act 1986 (Cth)

4.9 The role of the Inspector-General of Intelligence and Security is discussed in Chapter 12. Under the *Inspector-General of Intelligence and Security Act 1986* (Cth), personnel employed by the IGIS may not disclose, record or otherwise divulge information gathered in the course of their employment.[cxlv] The penalty for a breach of this section is $5,000, imprisonment for two years, or both.

Parliamentary Privileges Act 1987 (Cth)

4.10 Under s 13 of the *Parliamentary Privileges Act 1987* (Cth), a person shall not, without the authority of a House of the Federal Parliament or a parliamentary committee publish or disclose:

- a document that has been prepared for the purpose of submission, and submitted, to a House or a committee and has been directed by a House or a committee to be treated as evidence taken in camera;
- any oral evidence taken by a House or a committee in camera; or
- a report of any such oral evidence unless a House or a committee has published, or authorised the publication of, that document or that oral evidence.

4.11 The penalty for a breach of this section is $5,000 or imprisonment for 6 months for a natural person, or $25,000 in the case of a corporation.

4.12 These provisions are not specifically directed to classified and security sensitive information, but may catch the disclosure of such information that is otherwise covered by them.

Unauthorised disclosure generally

Criminal Code Act 1995 (Cth)

4.13 Section 91.1 of the *Criminal Code Act 1995* (Cth) contains the major offences relating to espionage and the transmission of classified information. These offences were removed from the *Crimes Act 1914* (Cth) as part of the reforms included in the *Criminal Code Amendment (Espionage and Related Offences) Act 2002*.[cxlvi] The new Criminal Code provisions contain essentially the same language as that in the previous Crimes Act provisions, but now refer to disclosing information about Australia's 'security or defence' (rather than 'safety or defence'). The penalties for all espionage offences have also been increased from seven to 25 years' imprisonment.

4.14 Section 91.1 creates offences relating to a person communicating, or making available, information or records concerning the Commonwealth's security or defence; or information or records concerning the security or defence of another country that the person acquired (directly or indirectly) from the Commonwealth. The offences include:

- where the person intends to prejudice the Commonwealth's security and defence and the person's act results in, or is likely to result in, the information being communicated or made available to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation (s 91.1(1)); and

- where a person gives the information without lawful authority and intending to give an advantage to another country's security or defence and the person's act results in, or is likely to result in, the information being communicated or made available to another country or a foreign organisation, or to a person acting on behalf of such a country or organisation (s 91.1(2)).

4.15 In commenting on the Criminal Code Amendment (Espionage and Related Offences) Bill, civil liberties groups made a number of criticisms of the proposed terms of s 91.1, including the following:

- The Bill no longer limited acts of espionage to classified information but extended it to a variety of information held or controlled by the government concerning security or defence;

- The change from 'safety or defence' to 'security or defence' meant that it would include the operations and methods of intelligence agencies, effectively stopping legitimate public debate on these matters; and

- No defence for whistleblowers was available.[cxlvii]

Crimes Act 1914 (Cth), s 79

4.16 Section 79 of the *Crimes Act 1914* (Cth) concerns unlawful disclosure of official secrets. The section contains a number of offences relating to the communication of official secrets to any person. A Commonwealth officer, or any person in receipt of information from a Commonwealth officer, may be guilty of an offence under this section. The penalty for communicating such information is seven years' imprisonment, and for receipt of the information is two years' imprisonment. To be guilty of an offence under this section a person must know or, by reason of its nature or the circumstances under which it came into his or her possession or control or for any other reason, ought to know that the information should not be communicated to a person not authorised to receive it.[cxlviii]

4.17 There are two types of offences under s 79: (a) those related to espionage, where an intention to prejudice the security or defence of the Commonwealth or a part of the Queen's dominions must be shown;[cxlix] and (b) those where the mere communication of the material is sufficient, with no need to show a specific purpose.[cl]

4.18 Section 79 is very similar to s 70 of the *Crimes Act*, discussed above. However, s 70 relates to a Commonwealth officer's legal duty under the *Public Service Act* and related regulations not to disclose information. Section 79 involves a broader duty that can arise, for example, from the nature of the information, and covers people other than Commonwealth officers.[cli]

Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002 [No 2]

4.19 An early version of the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002 [No 2] (the ASIO Bill) proposed the establishment of a scheme of 'approved lawyers'—legal practitioners whom the Minister had approved and in respect of whom the Minister had considered a security assessment—to be available to assist people being questioned in relation to a terrorism offence.[clii] In June 2003 the government proposed changes to the Bill, removing the requirement that a lawyer have a security clearance but providing for a range of other safeguards to protect the disclosure of classified and security sensitive information. One of these safeguards is a proposal to increase the penalty if a lawyer discloses any sensitive information while the person is detained under a warrant from two years' to five years' imprisonment.[cliii] The Bill as passed by the federal Parliament on 25 June 2003 included these proposals. The ASIO Bill is discussed further in Chapter 13.

Official Secrets Act 1989 (UK)

4.20 In the United Kingdom, civil servants (and other Crown employees) are subject to the *Official Secrets Act 1989* (UK). It is an offence under this Act to disclose official information in six specified categories without lawful authority and if the disclosure is damaging to the national interest. The categories are security and intelligence, defence, international relations, foreign confidences, information which might lead to the

commission of crime, and the special investigation powers under the *Interception of Communications Act 1985* (UK) and the *Security Services Act 1989* (UK).[cliv]

4.21 The *Official Secrets Act* has been criticised on the basis that there is no public interest defence available—for example, journalists may be prosecuted for receiving information—and because it is a crime to disclose information already in the public domain.[clv]

4.22 Among the best known cases involving the *Official Secrets Act* were the so-called *Spycatcher* cases in the late 1980s, in which the UK government unsuccessfully tried to stop publication in Australia and elsewhere of Peter Wright's book, *Spycatcher*. The book revealed a number of aspects of the work of MI5. The UK government sought injunctions against *The Guardian* and *The Observer* to stop them from publishing excerpts from the book, and commenced civil action in Australia to stop publication in Australia (which it lost).[clvi] In 1988 the House of Lords overturned the injunctions against the British newspapers.[clvii] After *Spycatcher*, the Act was amended in 1989 to permit criminal prosecutions only where the material in question is seriously harmful to national security.

Question 20. Are the current standards and levels of enforceability in relation to the unauthorised disclosure of classified and security sensitive information sufficient? Do additional criminal or procedural sanctions need to be developed?

Question 21. Does Australia need an Official Secrets Act?

5. Classified and Security Sensitive Information in Court

Introduction

5.1 A number of issues arise in assessing the use of classified and security sensitive information in court and tribunal proceedings, some of which threaten to impinge on certain basic civil liberties. These issues arise principally from the tension between the interest of the state in protecting such information by avoiding or limiting its disclosure, and the rights of individuals to a fair and open hearing. Some of these matters are canvassed further in Chapters 9–12, which deal with various types of hearings, such as criminal, civil, immigration and others.

5.2 There is actual or potential tension between the rights guaranteed in Australian and international law in relation to a fair hearing, and the operation of existing or proposed mechanisms designed to protect classified and security sensitive information. For example, legislative provisions enabling the closure of courts to the public may be in direct conflict with the right of an individual to a public trial. Similarly, provisions enabling hearings to be closed to one or more parties or their legal representatives may be in direct conflict with the right of an individual to be tried in his or her presence and to have the opportunity to examine the witnesses against him or her.

Right to a fair hearing

5.3 There are a number of key principles encompassed within the concept of a fair hearing. These include a person's right to a public hearing; the right to certain minimum procedural protections, such as being fully informed of the case against him or her; and the right to a full statement of the reasons for any decision or judgment.

Right to a public hearing

5.4 The International Covenant on Civil and Political Rights (ICCPR), to which Australia is a party, states in Article 14(1):

> In the determination of any criminal charge against him, or of his rights and obligations in a suit at law, everyone shall be entitled to a right to a fair and public hearing by a competent, independent and impartial tribunal established by law. The Press and the public may be excluded from all or part of a trial for reasons of morals, public order (*ordre public*) or **national security** in a democratic society, or when the interest of the private lives of the parties so require, or to the extent strictly necessary in the opinion of the court in special circumstances where publicity would prejudice the interests of justice; but any judgment rendered in a criminal case or in a suit at law shall be made public except where the interest of juvenile persons otherwise requires or the proceedings concern matrimonial disputes or the guardianship of children.[clviii] [emphasis added]

5.5 Article 14(1) applies to both criminal and civil proceedings, and arguably also to administrative proceedings.[clix] As the ICCPR allows for the closure of courts for national security reasons, it is important that the parameters of the term 'national security' are clearly defined. See discussion in Chapter 1.[clx]

5.6 Article 10 of the Universal Declaration of Human Rights[clxi] similarly provides that:

> Everyone is entitled in full equality to a fair and public hearing by an independent and impartial tribunal, in the determination of his rights and obligations and of any criminal charge against him.[clxii]

5.7 Some Australian legislation provides expressly for open hearings. For example, s 54 of the *Supreme Court Act 1933* (ACT) provides that evidence in any matter shall be given orally in open court, except as otherwise provided by legislation or unless the parties in any suit agree to the contrary. Rule 81A.18(1)(a) of the *Supreme Court Rules* (NT) provides that a pre-trial hearing is to be conducted by a judge in open court. Schedule 1, s 56 of the *Criminal Procedure Amendment (Justices and Local Courts) Act 2001* (NSW)[clxiii] provides that committal proceedings are to be heard as if in open court, subject to any other Act or law. Section 191 of that Act provides that summary proceedings before a court are to be heard in open court, subject to the provisions of any other Act or law.

Right to procedural protections

5.8 Certain procedural protections provided for in international instruments apply exclusively to criminal proceedings.[clxiv]

5.9 Article 14(3) of the ICCPR sets out the minimum guarantees to be accorded to a person in the determination of any criminal charge against him or her:

(a) To be informed promptly and in detail in a language which he understands of the nature and cause of the charge against him;

(b) To have adequate time and facilities for the preparation of his defence and to communicate with counsel of his own choosing;[clxv]

(c) To be tried without undue delay;

(d) To be tried in his presence,[clxvi] and to defend himself in person or through legal assistance of his own choosing; to be informed of, if he does not have legal assistance, of this right; and to have legal assistance assigned to him, in any case where the interests of justice so require, and without payment by him in any such case if he does not have sufficient means to pay for it;[clxvii]

(e) To examine, or have examined, the witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him;

(f) To have the free assistance of an interpreter if he cannot understand or speak the language used in court; and

(g) Not to be compelled to testify against himself or to confess guilt.[clxviii]

5.10 Article 11 of the Universal Declaration of Human Rights provides that:

> Everyone charged with a penal offence has the right to be presumed innocent until proven guilty according to law in a public trial at which he has had all the guarantees necessary for his defence.

5.11 The right to a fair trial is protected in Australia. In the High Court case of *Dietrich v R*, Gaudron J stated that:

> The fundamental requirement that a trial be fair … is not one that impinges on the substantive law governing the matter in issue. It may impinge on evidentiary and procedural rules; it may bear on where and when a trial should be held; in exceptional cases it may bear on whether a trial should be held at all. Speaking generally, the notion of 'fairness' is one that accepts that, sometimes, the rules governing practice, procedure and evidence must be tempered by reason and commonsense to accommodate the special case that has arisen because, otherwise, prejudice or unfairness may result. Thus, in some cases, the requirement results in the exclusion of admissible evidence because its reception would be unfair to the accused in that it might place him at risk of being improperly convicted, either because its weight and credibility cannot be effectively tested or because it has more prejudicial than probative value and so may be misused by the jury. …
>
> The requirement of fairness is not only independent, it is intrinsic and inherent. According to our legal theory and subject to statutory provisions or other considerations bearing on the powers of an inferior court or a court of limited jurisdiction, the power to prevent injustice in legal proceedings is necessary and, for that reason there inheres in the courts such powers as are necessary to ensure that justice is done in every case. Thus, every judge in every criminal trial has all powers necessary or expedient to prevent unfairness in the trial.[clxix]

5.12 The right to a trial by jury for indictable offences against Commonwealth law is preserved by s 80 of the *Australian Constitution*. This right applies regardless of the accused person's wishes. In *Brown v R*, the High Court held that an accused person's right under state law to waive a jury in a trial for an indictable offence does not apply to federal offences tried on indictment in that State.[clxx]

5.13 Some Australian legislation requires the accused to be present during proceedings. For example, *Criminal Procedure Amendment (Justices and Local Courts) Act 2001* (NSW), s 71 provides that:

> The accused person must be present when prosecution evidence is taken, unless this Division or any other Act or law permits the evidence to be taken in the accused person's absence.

5.14 Section 72(1) of that Act provides that:

> The Magistrate may excuse the accused person from attending during the taking of prosecution evidence if satisfied that the accused person will be represented by a barrister or solicitor while the evidence is taken or if satisfied that the evidence is not applicable to the accused person.

5.15 Section 73 of the Act states that evidence may be taken in the absence of an accused person who has not been excused from attending if

> (a) no good and proper reason is shown for the absence of the accused person, and
>
> (b) a copy of the relevant written statements, and copies of any proposed exhibits identified in the statements (or a notice relating to inspection of them) have been served on the accused person in accordance with this Act and the accused person has been informed of the time set by the Magistrate for taking prosecution evidence.

Abuse of process

5.16 In taking measures to ensure that a trial is fair, judges may, for example, order the severing of counts on an indictment; order the prosecution to elect to proceed on lesser charges than those contained in the indictment; or stay proceedings because of a potential abuse of process.[clxxi]

5.17 These powers can be used to deal with the issue of classified or security sensitive information in court proceedings. For example, in the recent prosecution of Simon Lappas, a former Defence Intelligence Organisation analyst, for passing classified information to an unauthorised person, the ACT Supreme Court upheld the prosecution's claim that certain documents not be disclosed on the basis of public interest immunity and ordered that they not be adduced as evidence but on the condition that the charge contained in the second count on the indictment be stayed.[clxxii] The Crown intended to tender 'empty shells' of the documents and to lead oral evidence about the general character of what was contained in them and to place a certain construction on the text of the documents that would lead to certain inferences being drawn. The trial judge, Gray J, noted:

> Presumably there could be no cross-examination on whether the interpretation accurately reflected the contents for that would expose the contents. Nor could a person seeking to challenge the interpretation give their own oral evidence of the contents for that would also expose those contents. The whole process is redolent with unfairness.[clxxiii]

5.18 His Honour concluded:

> I do not think the accused can have a fair trial unless far more of the text of the documents is disclosed to enable the accused, if he wishes to do so, to give evidence concerning it.[clxxiv]

5.19 It was central to the prosecution case to show that the documents would, in fact, have been useful to a particular foreign power. Gray J noted that, in fairness, the accused 'must have the opportunity of challenging any inference that the prosecution says can be drawn from the contents of the documents which might go to prove that intent', especially as he had never conceded his intent in that regard.[clxxv] His Honour observed that the fact that the executive government claimed public interest immunity at a late stage of the proceedings raised the issue of whether the accused could be

afforded a fair trial and also seemed to prevent the prosecution from adducing evidence highly relevant to its case.[clxxvi]

5.20 A defendant denied access to classified or security sensitive documents upon which the prosecution relies may be able to argue that his or her right to a fair trial is compromised because of that denial and his or her consequent inability to challenge or test part of the evidence. The burden of proving that the proceedings would be an abuse of process falls on the accused.[clxxvii] Where the prosecution has commenced and the trial judge considers that the denial of access to classified or security sensitive information would prejudice the preparation and presentation of the defence case, it may be appropriate for the trial judge to stay the proceedings or sever certain counts in the indictment.[clxxviii] A stay is to be exercised only in exceptional cases.[clxxix]

Question 22. What procedures have been adopted by courts and tribunals, including stays of proceedings or severing counts on an indictment, to ensure that proceedings involving classified or security sensitive information are fair? Are any further powers or procedures desirable? What, if any, limitations should be placed on the exercise of any existing or proposed powers?

Confidentiality orders and undertakings

5.21 One mechanism for the protection of classified and security sensitive information is the use of confidentiality undertakings to the court by parties and their legal advisers in respect of such information. In response to the federal government's proposal to introduce security clearances for legal aid lawyers representing defendants in national security cases (which is discussed in Chapter 13), lawyers have noted that they are often called upon to keep court matters confidential and can be bound by undertakings to the court.[clxxx]

5.22 The Victorian Bar has submitted that:

> Practitioners regularly give undertakings, supervised by the Court, in relation to confidential material. Breach of such undertakings is punishable by the Court as a contempt and is also subject to procedures before professional disciplinary bodies. It has never been suggested that the profession has abused this procedure.[clxxxi]

5.23 The New South Wales Bar Association has noted that 'various undertakings' were in place in the prosecution of Simon Lappas and that 'this is not an unusual situation with sensitive material before a court, and there is no apparent reason why this practice could not apply for [national security matters]'.[clxxxii] Confidentiality undertakings also have been used in litigation to protect commercially sensitive information. The following mechanisms, used either alone or in combination, have been identified as ways of limiting the disclosure of confidential information during legal proceedings:

- The parties may, by agreement or by court order, execute express undertakings in relation to documents which are found to contain commercially sensitive information.
- Access to the documents in question may be restricted by court order, for instance, the other party's lawyer and experts may only be permitted to inspect the documents …
- The documents may be edited or 'blacked out' in order to delete highly confidential information such as company's financial data.[clxxxiii]

5.24 In certain circumstances, it may be appropriate for expert witnesses to give an undertaking to the court that they will not divulge the contents of any classified or security sensitive information that forms part of their brief. For example, where expert witnesses are called to provide an opinion about whether the communication of certain classified or security sensitive information was likely to threaten national security, it may be appropriate to require them to give confidentiality undertakings to the court.[clxxxiv]

5.25 Apart from express undertakings, parties to litigation are subject to an implied undertaking to the court not to use or disclose information that they receive through the court's compulsory processes except for the purpose of those proceedings without the court's leave or the consent of the owner of the information. The undertaking applies to all forms of a court's compulsory process: discovery, subpoenas, interrogatories, and orders requiring production of affidavits and witness statements.[clxxxv] A breach of this undertaking (for example, by disclosing the information to the media or for the purpose of another court case) is a contempt of court.[clxxxvi] The undertaking ceases upon the information being admitted into evidence in open court.[clxxxvii] The Rules of the Federal Court of Australia provide that:

> Any order or undertaking, whether express or implied, not to use a document for any purpose other than those of the proceedings in which it is disclosed shall cease to apply to such a document after it has been read to or by the Court or referred to, in open Court, in such terms as to disclose its contents **unless the Court otherwise orders** on the application of a party, or a person to whom the document belongs.[clxxxviii] [emphasis added]

5.26 The Federal Court's powers to extend the application of an undertaking in relation to the use of a document introduces a level of flexibility in the Court's ability to deal with sensitive information.

5.27 Courts and tribunals also can make orders to protect the confidentiality of classified and security sensitive information by restricting access to the documents containing it.[clxxxix] The US Department of Justice issued a new interim rule on 28 May 2002 authorising immigration judges to issue protective orders and seal records relating to law enforcement or national security information in individual cases. The new rule also authorises judges to issue orders that prohibit detainees or their lawyers from publicly divulging the protected information.[cxc] The new rule limits 'what the respondent and his or her representatives may disclose about sensitive law enforcement

and national security information outside the context of those hearings.'[cxci] The rule prescribes sanctions for a breach of the protective order: if a detainee or a lawyer discloses information from a closed hearing, the lawyer may be barred from appearing in immigration court hearings and the detainee can be denied discretionary relief. The breadth and wording of the rule have been criticised, however:

> According to the language of the rule, a detainee could be punished if the lawyer reveals information without the client's permission and vice versa. In addition, the rule allows only one side—the government—to ask that proceedings be sealed.[cxcii]

5.28 The US Department of Justice's Military Commission Instruction No 5 of 30 April 2003 requires civilian defence counsel to agree that they will not make any public or private statements regarding any closed sessions of military commission proceedings or any classified information or material, or protected information.[cxciii]

5.29 Presumably, any disclosure of classified and security sensitive information in breach of any undertaking or order could also constitute a criminal offence under one or more of the relevant provisions in the *Crimes Act 1914* (Cth) or other federal legislation: see Chapter 4.

Question 23. To what extent are confidentiality undertakings used in court and tribunal matters involving classified or security sensitive information? From whom are such undertakings sought: the parties, their legal representatives, expert witnesses, or anyone else? Are any limitations placed on the use of confidentiality undertakings? Should there be any such limitations?

Question 24. Are confidentiality undertakings fair and effective in protecting classified or security sensitive information, either alone or in conjunction with other mechanisms such as hearings in camera? Are there any concerns with respect to the use of confidentiality undertakings to protect commercially sensitive information that may be relevant to their efficacy in protecting classified or security sensitive information?

Question 25. What are, or should be, the proper sanctions for a breach of a confidentiality order imposed by a court or tribunal, or a confidentiality undertaking given to a court or tribunal, in relation to the protection of classified or security sensitive information?

Hearings closed to the public

5.30 The principle of open justice is an essential feature of the common law judicial tradition. In *Dickason v Dickason*,[cxciv] the High Court unanimously applied the principle stated in *Scott v Scott*[cxcv] that there is no inherent power in the court to exclude the public, although that power may be conferred expressly by law. The High Court recognised that 'one of the normal attributes of a court is publicity.'[cxcvi] In

Russell v Russell,[cxcvii] the majority of the High Court held that it was beyond Parliament's constitutional power to pass legislation which required a state court to exercise federal jurisdiction in private. Gibbs J (as he then was) stated that the public conduct of proceedings:

> has the virtue that the proceedings of every court are fully exposed to public and professional scrutiny and criticism, without which abuses may flourish undetected. Further, the public administration of justice tends to maintain confidence in the integrity and independence of the courts. The fact that courts of law are held openly and not in secret is an essential aspect of their character.[cxcviii]

5.31 The Hon JJ Spigelman, Chief Justice of New South Wales, has commented that the principle of open justice 'should be understood as so fundamental an axiom of Australian law, as to be of constitutional significance'.[cxcix] 'Generally speaking, it is taken for granted that court proceedings are open to the public and may be freely reported.'[cc] Chief Justice Spigelman has noted that the exceptions to this principle are few and 'strictly defined'.[cci]

5.32 In the US, the right to a public trial is expressly guaranteed by the Sixth Amendment of the Constitution, which reads:

> In all criminal prosecutions, the accused shall enjoy the right to a speedy and public trial, by an impartial jury of the state and district wherein the crime shall have been committed, which district shall have been previously ascertained by law, and to be informed of the nature and cause of the accusation; to be confronted with the witnesses against him; to have compulsory process for obtaining witnesses in his favor, and to have the assistance of counsel for his defense.

5.33 One existing mechanism for dealing with classified and security sensitive information is the holding of hearings in camera and the powers of the court to make orders restricting publication of proceedings and restricting access to documents on the court file.[ccii]

5.34 A number of conclusions may be drawn from various judgments of the US Supreme Court in relation to closure of proceedings to the public:

> First, the accused, prosecutor and judge cannot simply agree to close the proceedings. Second, before denying the public full access to a criminal proceeding, the court must consider alternatives, including partial exclusion of the public or, in case of broad publicity problems, sequestration of the jury. Third, the judge must articulate in findings what overriding interest is being protected by closure. And, last, the closure must be as narrow as possible.[cciii]

5.35 One Australian lawyer has commented that:

> It is likely that 'national security interest' will lead to the prosecution requesting that terrorism trials, or parts of them, be held in closed court. That means that the media and the public will not know what is taking place. A sight and sound record of the closed proceedings must be available to public inspection several years later.

> No extradition should be permitted of a person whose arrest and confinement is based upon evidence not disclosed in an open court.[cciv]

5.36 Section 93.2 of the *Criminal Code Act 1995* (Cth)[ccv] allows a judge or magistrate at any time before or during a hearing of an application or proceedings before a federal court, a court exercising federal jurisdiction or a court of a Territory, to make the following orders if satisfied that it is in the interest of the security or defence of the Commonwealth:

> (a) order that some or all of the members of the public be excluded during the whole or a part of the hearing; or
>
> (b) order that no report of the whole or a specified part of, or relating to, the application or proceedings be published; or
>
> (c) make such order and give such directions as he or she thinks necessary for ensuring that no person, without the approval of the court, has access (whether before, during or after the hearing) to any affidavit, exhibit, information or other document used in the application or the proceedings that is on the file in the court or in the records of the court.[ccvi]

5.37 These are identical to the orders that a court can make under s 85B of the *Crimes Act 1914* (Cth). The difference is that under s 85B the court has to be 'satisfied that such a course is expedient in the interest of the defence of the Commonwealth'; whereas under s 93.2 the court has to be satisfied that 'it is in the interest of the security or defence of the Commonwealth.'[ccvii] It is unclear what (if any) practical difference exists in the effect of the two sections.[ccviii]

5.38 Other provisions in both Australian and overseas legislation also allow for in camera hearings and orders restricting the publication of proceedings.[ccix] For example, s 50 of the *Federal Court of Australia Act 1976* (Cth) allows the Court to make 'such order forbidding or restricting the publication of particular evidence, or the name of a party or witness, as appears to the Court to be necessary in order to prevent prejudice to the administration of justice or the security of the Commonwealth'.[ccx]

5.39 A recent example of in camera proceedings in Australia was the committal hearing in the *Lappas* Case, in which the classified documents allegedly passed by Lappas to an unauthorised person were tendered as evidence in camera, and defence counsel were given access at that time.[ccxi] A current example of an in camera proceeding at the international level is the trial of Slobodan Milosevic before the International Criminal Court.[ccxii]

5.40 Non-curial tribunals may also hold hearings in camera. For example, s 39A of the *Administrative Appeals Tribunal Act 1975* (Cth) sets out the procedure for certain hearings in its Security Appeals Division. Section 39A(5) of that Act states that proceedings are to be in private and that the tribunal is to determine who may be present at the hearing.

5.41 Hearings before the Federal Police Disciplinary Tribunal generally are to be held in public.[ccxiii] However, where the Tribunal is satisfied that it is desirable to do so in the public interest or by reason of the confidential nature of any evidence or matter, the Tribunal may:

> (a) direct that the hearing, or a part of the hearing, shall take place in private and give directions as to the persons who may be present; and
>
> (b) give directions restricting or prohibiting the publication or disclosure:
>
> (i) of evidence given before the Tribunal, whether in public or in private;
>
> (ii) of any matters contained in documents lodged with the Tribunal or received in evidence by the Tribunal; or
>
> (iii) of any finding or decision of the Tribunal in relation to the proceeding.[ccxiv]

5.42 The ALRC will be considering the current practices in Australian courts and tribunals in relation to closing, and restricting the reporting of, proceedings. This will involve a review of whether transcripts of applications to close or restrict access to proceedings are kept; who may access any such transcripts and under what conditions; and whether full written reasons are given when proceedings are closed or access to them is restricted.

When is closure justified under international law?

5.43 Article 14(1) of the ICCPR (set out above) allows a court to be closed for reasons of national security. As discussed in Chapter 1, the Commonwealth Protective Security Manual sets out the four levels of national security protective markings ('Restricted', 'Confidential', 'Secret' and 'Top Secret') which reflect the consequences of the compromise of the information.[ccxv] While leading information designated 'Top Secret' might well justify the closure of a court, it is unclear whether leading any information that has been properly marked with one of the other, lesser national security protective markings could justify the closure of a court, especially given Nowak's commentary that 'national security' for the purpose of the ICCPR requires proof of a 'grave case … of political or military threat to the entire nation'.[ccxvi]

5.44 In any event, it may well be that the designation of the material is not (or should not be) decisive but that a review of the sensitive material—particularised, independent and at the time of its proposed public use—should determine how it is to be used.

Media and public access

5.45 Public access to court proceedings is facilitated to a large degree by media reporting of court proceedings, which is necessarily dependant on the media having access to such proceedings either directly by being permitted to be present while the proceedings transpire or indirectly by being allowed access to relevant documents and transcripts. The ALRC is interested in hearing from media groups as to the particular

issues that face them, and through them the public generally, if their access to proceedings is restricted wholly or partially in order to protect classified or security sensitive information. Media groups have taken action in Australia challenging the closing of hearings to the public, and some media groups in the United States have recently taken court action challenging the closing of immigration hearings to the public.[ccxvii]

5.46 The legislation establishing many Australian courts expressly provides for public access to evidence and other documents produced in relation to proceedings in those courts. For example, s 131 of the *Supreme Court Act 1935* (SA) governs public access to evidence used in the South Australian Supreme Court. It sets out the categories of documents to which the Court must, on application by any member of the public, allow the applicant to inspect or copy. These documents include the transcript of evidence taken by the Court, any documentary material admitted into evidence in any proceedings, transcript of submissions by counsel, and transcript of the judge's summing up or directions to a jury.[ccxviii] Section 131 also specifies the categories of documents that a member of the public may inspect or copy but only with the permission of the Court. These include material that was not taken or received in open court and material the publication of which has been suppressed by the Court.[ccxix] If the Court grants permission to inspect or copy such material, it may impose any condition that it considers appropriate, including a condition limiting the publication or use of the material.[ccxx]

5.47 Rule 81A.09(1) of the *Supreme Court Rules* (NT) provides that a person may inspect and copy a document filed in a proceeding that is part of the record of proceedings of a trial. Rule 81A.09(2) restricts the ability of a person to inspect or copy a document that the NT Supreme Court has ordered remain confidential and provides that a person who is not a party to the proceedings may not, without the leave of the Court, inspect or copy a document that, in the opinion of the Registrar, should remain confidential to the parties. The record of proceedings of a trial consists of the indictment, the official tape recordings of the proceedings of the trial made by persons approved by the Chief Justice (although once an official transcript has been made, the official tape recording of the part of the proceedings transcribed ceases to be part of the record of proceedings) and the official transcript of the official tape recording.[ccxxi]

5.48 Some lower courts also have similar provisions in their legislation: see, for example, s 314 in Schedule 1 of the *Criminal Procedure Amendment (Justices and Local Courts) Act (2001)* (NSW).

Question 26. What, if any, safeguards should be imposed on the use of closed proceedings to protect classified and security sensitive information, the rights of the parties and of the public?

Question 27. Prior to closing a court to lead classified or security sensitive evidence, should there be a review of the classification decisions relating to the

classified or security sensitive evidence to be adduced? If so, who should be responsible for that review?

Question 28. Should a transcript of the closed proceedings be made? If so, who should have access to it and under what conditions?

Question 29. Should classified or security sensitive information protected by the use of closed hearings be subject to a review of its classification status as a matter of course some time after a closed hearing has concluded to facilitate later public access to the proceedings? If so, who would be responsible for this review and within what timeframe should it be conducted?

Question 30. Should there be any limits placed on the use which can be made of evidence not disclosed in open court? For example, should extradition be permitted of a person whose arrest and confinement has been based upon evidence not disclosed in open court?

Question 31. Should the media, or any other public interest bodies, be given the right in all, or any class of, proceedings to intervene on the question of the possible closure of, or restriction of access to or reporting of, proceedings?

Question 32. Are there any other issues from the perspective of the media arising from their access to proceedings being prohibited or restricted in order to protect classified or security sensitive information?

Hearings closed to one or more parties

5.49 In contrast to an in camera hearing where (unless the proceedings are ex parte) the hearing is held in the presence of the accused and his or her lawyer, some hearings are closed to one or more parties or their lawyers—usually the parties whose interests, rights or liberty are at stake. For example, the *Anti-Terrorism, Crime and Security Act 1981* (UK) aims, among other things, to improve the security of dangerous substances that may be targeted or used by terrorists.[ccxxii] Under the Act, the Secretary of State may, if necessary in the interests of national security, give directions to the occupier of certain premises, requiring denial of access to dangerous substances.[ccxxiii] A person aggrieved by such directions may appeal to the Pathogens Access Appeals Commission.[ccxxiv] Section 5(3) of that Act empowers the Lord Chancellor to make rules which:

> (b) enable the Commission to exclude persons (including representatives) from all or part of proceedings;
>
> (c) enable the Commission to provide a summary of evidence taken in the absence of a person excluded by virtue of paragraph (b);[ccxxv]

5.50 The *Special Immigration Appeals Commission Act 1997* (UK) allows rules to be made enabling the Special Immigration Appeals Commission to hold proceedings in the absence of any person, including the appellant and any legal representative appointed by him or her,[ccxxvi] having regard in particular to the 'need to secure that information is not disclosed contrary to the public interest.'[ccxxvii] The relevant law officer may appoint a person to represent the interests of an appellant in any proceedings from which the appellant and his or her lawyer are excluded.[ccxxviii] Appointed lawyers are not responsible to the person whose interests they are appointed to represent.[ccxxix] Part 7 of the Special Immigration Appeals Commission (Procedure) Rules 2003 includes provisions prescribing procedures to be followed where the Secretary of State wishes to rely on any material in proceedings before the Commission but objects to it being disclosed to the appellant or his or her representative.[ccxxx]

5.51 Some immigration hearings in the United States, the United Kingdom and Australia have been closed to the parties or their lawyers and the public. These are discussed in Chapter 11.

5.52 Excluding a person's lawyer from a criminal hearing would appear to violate that person's rights under Article 14(3)(b) and (d) of the ICCPR to communicate with, and be defended by, counsel of his or her own choosing.[ccxxxi] However, the international protections in this regard do not extend to a person having the right to counsel of his or her choice in civil or administrative proceedings.

5.53 The use of independent lawyers or lawyers with a security clearance in matters involving national security is discussed in Chapter 13.

Secret hearings

5.54 In some cases, even the fact that a hearing is taking place is shrouded in secrecy. As considered in Chapter 11, certain immigration hearings in the United States after September 2001 have been conducted in accordance with special procedures including closure of proceedings and restricting information confirming or denying whether such a case is on the docket or scheduled for hearing.[ccxxxii] The US Department of Justice has argued that opening the immigration hearings of people detained after 11 September 2001 could compromise its terrorism-related investigations.

5.55 Human Rights Watch has been critical of the secrecy associated with the US immigration hearings:

> The government's justification for blanket secrecy … sweeps too broadly. Its rationale would justify closing trials in any large criminal investigation. The Department of Justice's arguments would, for example, justify closing arrest rosters and trials in organized crime cases where there would be a danger that accomplices and associates might learn details about the progress made by law enforcement, tamper with evidence and threaten witnesses. The US justice system has mechanisms to ensure reasonable openness while preventing harm to an ongoing investigation, but has never allowed blanket secrecy over hundreds of cases on the mere allegation that

> criminals might learn something about the investigation if the prosecution were conducted publicly.[ccxxxiii]

5.56 Human Rights Watch has also commented that:

> Unsubstantiated speculations about potential damage to the government's investigation … should not be permitted to override the fundamental principle that arrests and hearings affecting a person's liberty should be public to ensure fairness and to prevent abuse of power.[ccxxxiv]

Secret evidence

5.57 One method of protecting classified or security sensitive information in investigations and proceedings is to deny parties and their lawyers access to such material. In effect, the government may seek to lead evidence in a court closed to the party against whom the evidence is lead. However, there are a number of concerns associated with the use of secret evidence. Apart from being inherently unfair, it could also encourage less rigorous investigations and prosecutions. Moreover, leading secret evidence in criminal matters clearly breaches protections afforded by Australian and international law for an individual to be tried in his or her presence and to have the opportunity to examine, or have examined any adverse witnesses.[ccxxxv]

5.58 Professor David Cole, who has represented at least 13 aliens against whom the US Immigration and Naturalization Service (INS) has sought to use secret evidence, has identified a number of concerns associated with secret evidence, which are set out below.[ccxxxvi] Although Professor Cole's concerns relate to the INS's use of secret evidence, they are capable of wider application to secret evidence generally. Cole argues that it is not possible to hold a fair adversary proceeding where one side presents its evidence behind closed doors—the adversary system is the best mechanism for determining truth but it depends on each side being able to examine and respond to the other's evidence.[ccxxxvii] In secret evidence proceedings, one party cannot cross-examine and often has no idea of what the evidence against him or her is.[ccxxxviii]

5.59 Cole asserts that the INS's use of secret evidence contains practically no safeguards against abuse and he cites various instances;: for example, he asserts that:

- The INS uses secret evidence where there is no legitimate need for the evidence to be secret because it has been improperly classified by another agency and the INS has no authority to declassify.[ccxxxix]

- Evidence often has been over-classified and there is no requirement that anyone review the classification decision.[ccxl]

- The INS also has failed to keep a record of many of its secret evidence presentations, thereby defeating meaningful review.[ccxli]

- There is no requirement that it first attempt to make its case without relying on secret evidence.[ccxlii]

5.60 There is a real concern that secret proceedings encourage reliance on questionable evidence, including double and triple hearsay. According to Professor Cole, the INS has relied on hearsay in its secret evidence presentations, often in the form of reports drafted by FBI agents relaying accusations by hearsay sources. When the secret evidence consists of hearsay, it is impossible even for the judge to question the sources.[ccxliii] In one case, the source of secret evidence against a party was his ex-wife, who had made numerous false accusations in the course of a custody battle over their child.[ccxliv] Rumour and innuendo collected by investigative agencies can be accorded too much weight when it becomes 'evidence'—especially in secret, when there is no opposing party to challenge it.

5.61 On 19 April 2001, a Bill was referred to the US House Subcommittee on Immigration and Claims, which, if enacted, would have ensured 'that no alien is removed, denied a benefit under the Immigration and Nationality Act, or otherwise deprived of his liberty, based on evidence that is kept secret from the alien.'[ccxlv] The Bill required that, before using classified information, the US Attorney General would have to certify that the same information could not reasonably be obtained from unclassified sources and that the agency providing the information had been asked to declassify it. This proposal

> aimed to ensure that information was not improperly classified, reflecting the … concern that in some cases the government would release information in later criminal proceedings that it earlier asserted could not be disclosed in immigration hearings.[ccxlvi]

5.62 No progress has been made on the Bill since that time. It has been suggested that the attacks on the World Trade Centre and the Pentagon on 11 September 2001 probably derailed the proposed legislation, which would have augmented procedural protections for aliens.[ccxlvii]

Question 33. To what extent are secret hearings and secret evidence used in Australia to protect classified and security sensitive information? What safeguards are, or should be imposed, on their use?

Question 34. Do an accused's right to a fair trial and the guarantees set out in Article 14(3) of the International Covenant on Civil and Political Rights rule out secret hearings and secret evidence in criminal matters? Should the minimum guarantees provided to accused persons under the Covenant be extended to parties in civil matters and administrative hearings?

Question 35. Should the fact that a hearing is taking place, even if it is closed to the public and to one or more parties or their legal representatives, ever be withheld from the parties affected or from the public?

Question 36. Should the normal rules of evidence (such as the rule against hearsay) apply to secret evidence?

Question 37. Should it be mandatory to have counsel representing an absent party's interests present at any secret hearings, or hearings where secret evidence is to be adduced (whether the party's counsel, an independent counsel or security-cleared counsel)?

Question 38. Before any secret hearing or the leading of any secret evidence, should there be a review of the classification status of the classified or security sensitive evidence? Who should be responsible for that review?

Question 39. Before any secret hearing or the leading of any secret evidence, should the Attorney-General (or other government official) certify that:

(a) he or she has sought to have the evidence declassified or reclassified prior to it being adduced; and

(b) that the same information could not reasonably be obtained from unclassified sources?

Question 40. Should a record of secret proceedings and secret evidence always be kept to assist, for example, in any appeal and review process? Who should have access to it and under what conditions?

5.63 See also the questions in Chapter 11 dealing with the use of secret evidence in immigration and similar hearings.

Right to statements of reasons

5.64 One important aspect of the right to a public trial is the right to (and public interest in) a public judgment.[ccxlviii] The right to a fair hearing encompasses the right to a statement of reasons for a judgment,[ccxlix] both generally on the merits of the case and in relation to procedural aspects of the hearing, including the use of classified and security sensitive information.

5.65 Some legislative provisions in the United Kingdom modify a person's right to receive a statement of reasons in administrative hearings. The *Special Immigration Appeals Commission Act 1997* (UK) provides that rules may 'make provision enabling proceedings before the Commission to take place without the appellant being given full reasons for the decision which is the subject of the appeal.'[ccl] Similarly, under the *Anti-Terrorism, Crime and Security Act 1981* (UK) the Lord Chancellor may make rules which 'provide for full particulars of the reasons for denial of access to be withheld from the applicant and from any person representing him'.[ccli]

Question 41. Should there be any limitation of the right of a party to proceedings involving classified or security sensitive information to receive full reasons in relation to any judgment or decision which affects him or her? If so, when?

Question 42. If the need to protect classified or security sensitive information is a ground for withholding a full statement of the reasons for a judgment or decision from a party to a proceeding involving such information, how can the content of the reduced reasons for decision be sufficiently meaningful and adequate to support any review or appeal?

Question 43. Should there be any limitation on the publication of written reasons for any judgment or decision in proceedings involving classified or security sensitive information?

6. Investigation and Pre-Trial Issues

6.1 A number of issues arise in relation to the protection of classified and security sensitive information in the investigation and pre-trial stages of a matter. Some of these issues overlap with those concerning the presentation of evidence in proceedings, which are discussed in Chapter 7.

Provision of material to suspects

Crimes Act 1914 (Cth)

6.2 The Terms of Reference ask the ALRC to consider s 23V of the *Crimes Act 1914* (Cth) in relation to the provision of material to suspects and any other relevant provisions. Section 23V(1) makes a confession or admission of a person interviewed as a suspect (whether under arrest or not) inadmissible as evidence against the person in proceedings for any Commonwealth offence unless it was tape-recorded, where it was reasonably practicable to do so,[cclii] and, in any other case, recorded in writing and read to the person so as to give him or her an opportunity to correct it.[ccliii] A copy of the written record is to be made available to the person and the reading of the record is to be tape-recorded.[ccliv]

6.3 Section 23V(2)(a) requires an investigating official to provide the person (or his or her lawyer) with a copy of the recordings of confessions or admissions, or the confirmation of such confessions or admissions, within seven days.[cclv] If a transcript of the tape-recording is prepared, a copy must be provided to the person or his or her lawyer within seven days under s 23V(2)(c) , but it is important to note that this section has no operation where no transcript is prepared. There is no obligation to create a transcript of a tape-recording—only to make it available to the person if one has been prepared.[cclvi]

6.4 A court may admit evidence obtained in breach of the requirements of s 23V where the court is satisfied that, in the special circumstances of the case, this would not be contrary to the interests of justice,[cclvii] or if it is satisfied that it was not practicable to comply with the section.[cclviii] Where evidence is admitted on these grounds, the judge must inform the jury of the non-compliance with the requirements of the section and give the jury such warning as is appropriate in the circumstances.[cclix]

6.5 Perhaps of most relevance to the current inquiry is s 23V(3) of the Act, which provides:

> Where a confession or admission is made to an investigating official who was, at the time when it was made, engaged in covert investigations under the orders of a superior, this section applies as if the acts required by paragraph (1)(b) and subsection (2) to be performed were required to be performed by the official at a time when they could reasonably be performed without prejudice to the covert investigations.

6.6 To assist it in evaluating the effectiveness of s 23V, the ALRC is interested in hearing from investigating agencies, and from members of the public and defence lawyers about current practices in withholding recordings and transcripts of confessions and admissions from suspects on the basis that it would prejudice a covert investigation, especially in circumstances involving the protection of classified and security sensitive information.

Question 44. What issues arise in relation to the withholding of recordings and transcripts of confessions and admissions (or other material) from suspects by Australia's investigating agencies—particularly on the basis that they would prejudice a covert investigation or in circumstances involving the protection of classified or security sensitive information?

Disclosure or discovery of sensitive information

6.7 In criminal proceedings the prosecution has an ethical obligation to disclose all material that is to be used in its case, as well as 'unused material' that the prosecution does not intend to rely upon as part of its case and 'either runs counter to the prosecution case (ie, points away from the defendant having committed the offence) or might reasonably be expected to assist the defendant in advancing a defence'.[cclx] An accused person does not carry any comparable obligation of disclosure on that basis that the prosecution is required to prove its case without assistance from the defence.

6.8 An accused's intention to introduce classified or security sensitive information into evidence is often part of a legitimate approach to the defence of the charges and not merely a tactical device to undermine the prosecution. But it might have the effect (or purpose) of 'greymail'—that is, presenting the government with the choice of either allowing the classified information to be disclosed, or dismissing or compromising the indictment or charges.

6.9 The following issues arise in this connection:

- How can the prosecution discharge its obligation of disclosure, which plays a significant part in ensuring the accused's right to a fair trial, while protecting classified and security sensitive information upon which it seeks to rely as part of the prosecution case, or which would otherwise arise in the case?

- How can an accused obtain pre-trial access to relevant classified and security sensitive information?

- Given the defence's limited obligations of disclosure in criminal matters, how can the prosecution deal with a defendant's intentions to lead classified and security sensitive information if it learns of this intention before or during the trial? Does the Australian system have safeguards against 'greymail' threats

where the defence threatens to divulge classified information during the course of a trial?

- In civil proceedings, where parties are under an obligation to discover all relevant non-privileged documents to each other and may be obliged to answer interrogatories, classified and security sensitive information might be disclosed in pre-trial procedures.

6.10 As discussed in Chapter 7, some mechanisms limiting the disclosure or discovery of classified or security sensitive information before trial also can be used when presenting evidence in court and tribunal proceedings. These mechanisms (including some used in overseas jurisdictions) include:

- substituting classified information with unclassified information;[cclxi]
- substituting a statement admitting relevant facts that the classified information would tend to prove;[cclxii]
- providing redacted (ie, edited) versions of documents containing classified or security sensitive information with the sensitive portions removed;
- providing a witness statement that omits sensitive material;[cclxiii]
- substituting an unclassified summary of the classified information;[cclxiv] and
- protective orders against disclosure and sealing orders (see below).

United States position

6.11 The US *Classified Information Procedures Act* [cclxv] (CIPA) addresses the greymail issue by providing a procedural framework for the disclosure and admission of classified information in criminal trials, requiring pre-trial court rulings on the admissibility of such evidence. CIPA does not curtail the admissibility of classified information; rather, it enables the government to ascertain prior to trial the classified information that the defendant seeks to admit at trial so that it can assess the effect of disclosure on national security.[cclxvi]

6.12 If a court rules that the classified information is discoverable, the government may invoke s 3 and 4 of CIPA. Section 3 requires the court, upon the government's request, to issue an order 'to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case'. Section 4 allows the court, upon 'sufficient showing':

- to authorise the government to delete specified items of classified information from discoverable documents;

- to substitute summaries of information; or

- to substitute a statement admitting relevant facts that the classified information would tend to prove. The government may demonstrate that the use of such alternatives is necessary in an in camera and ex parte submission to the court.[cclxvii]

6.13 Following discovery under s 4, there are three critical pre-trial stages in the handling of classified information under CIPA.[cclxviii] First, the defendant must notify the government and the court in writing if he or she reasonably expects to disclose classified information at trial or in pre-trial proceedings. The notice must specify in detail the classified information which the defendant intends to rely upon.[cclxix] If the defendant fails to comply with this procedure, the court may preclude the disclosure of any classified information that was not the subject of prior notification, and may prevent the defendant from examining any witness in relation to such information.[cclxx]

6.14 Secondly, upon a motion by the government, the court must hold a hearing pursuant to s 6(a) to determine the use, relevance and admissibility of the classified evidence. Prior to this hearing, the government must provide the defendant with notice of the specific classified information in issue.[cclxxi] The hearing is to be held in camera if the Attorney General certifies to the court that a public hearing may lead to the disclosure of classified information.[cclxxii]

6.15 Thirdly, following the s 6(a) hearing and formal findings of admissibility by the court, as an alternative to declassification and release of the information the government may move for an order permitting (in lieu of full disclosure) either a substitution of a statement admitting relevant facts that the classified information would tend to prove, or a substitution of a summary of the specific classified information.[cclxxiii] The court is required to grant such a motion if it finds that the statement or summary 'will provide the defendant with substantially the same ability to make his defense as would disclosure of the specific classified information'.[cclxxiv] In many cases 'the government will propose a redacted version of a classified document as a substitution for the original, having deleted only non-relevant classified information'.[cclxxv] Whenever the court rules after a s 6(a) hearing that the defendant may use classified information in his or her defence, the government is required to provide the defendant with the information which it anticipates it will use to rebut such information. If the government fails to provide this notice, the court may preclude it from using any such rebuttal information.[cclxxvi]

6.16 Some commentators have pointed to the unusual level of disclosure of the defence case that the CIPA procedures require:

> Because CIPA mandates pretrial relevancy determinations, effective use of CIPA by defense counsel may necessitate substantial disclosure of the defendant's case prior to trial, including aspects of the defendant's own testimony. … The goal is to force the government either to declassify the information needed by the defense or, if it refuses to do so, obtain dismissal of the charges.[cclxxvii]

6.17 Similarly:

> Many have argued that the requirement that a defendant disclose aspects of his defence in advance of trial coupled with the procedure for a court ruling in the abstract before the trial has begun, on whether proffered evidence is relevant and admissible, unfairly shifts the burden of proof to a defendant.[cclxxviii]

Sealing orders

6.18 Under CIPA, all in camera proceedings and hearings pursuant to the Act are sealed and preserved for the appellate record.[cclxxix] At the time of writing, the trial date of Zacarias Moussaoui, the alleged conspirator in the attacks on the World Trade Centre and Pentagon, had been indefinitely adjourned.[cclxxx] The case provides a recent example of how the US courts are handling the issue of classified information before trial. For example, in March 2003 the US Justice Department

> took the unusual step of filing its briefs … to the US Court of Appeals for the 4th Circuit under total secrecy. … Although portions of cases involving classified information often are filed and reviewed in secret, legal specialists said they could recall virtually no other examples of the government's filing an entire set of legal briefs under seal.[cclxxxi]

6.19 Much of the court record had been placed under seal by the Federal District Court out of concern that it might divulge national security secrets. A number of news organisations challenged the decision to place many prosecution and defence documents under seal without advance notice to the public on the ground that it violated the First Amendment of the US Constitution.[cclxxxii] In April 2003, the US Justice Department agreed that much of the secret court record could be made public but requested the trial judge to keep a handful of documents under seal because they 'disclose confidential sensitive details about foreign relations of the United States'.[cclxxxiii] In some cases the Justice Department said that it should be allowed to edit some of the documents before they were made public.[cclxxxiv]

6.20 In June 2003, a judge in New Jersey ordered the unsealing of transcripts of secret evidence presented in a closed court session in a case where it was alleged that the accused, Mohammed el-Atriss, had ties to terrorism and should be held on higher bail.[cclxxxv] A number of newspapers had applied for the release of the transcripts.

Ex parte proceedings

6.21 Another tool to protect classified or security sensitive information before trial (which may also be used during the course of proceedings) is the use of ex parte proceedings (ie, proceedings in the absence of one or more of the parties). The *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001* (the USA PATRIOT Act) provides a number of examples sanctioning the use of such proceedings. For example:

- Section 2712(e)(1) of the United States Code (which is found in Title 18, Chapter 121) provides that, upon the motion of the United States, the court shall

stay any action commenced under the section if it determines that civil discovery will adversely affect the ability of the government to conduct a related investigation or the prosecution of a related criminal case. Section 2712(e)(3) provides that, in requesting a stay, the government may submit evidence ex parte in order to avoid disclosing any matter that may adversely affect a related investigation or a related criminal case. If the government makes such an ex parte submission, the plaintiff is to be given an opportunity to make a submission to the court, not ex parte, and the court may request further information from either party.[cclxxxvi]

- Section 219(a)(3)(B) of the *Immigration and Nationality Act* provides that the Secretary of State, in consultation with the Secretary of the Treasury and the Attorney General, may consider classified information in designating a foreign terrorist organisation. Classified information is not to be disclosed for such time as it remains classified, except that it may be disclosed to a court ex parte and in camera for the purposes of judicial review. Section 219(b)(2) provides that review under the subsection shall be based solely upon the administrative record except that the government may submit, for ex parte and in camera review, classified information used in making the designation.[cclxxxvii]

Question 45. When and how do prosecutors disclose to, and withhold from, the defence classified or security sensitive information prior to trial? Are these methods effective? How is prejudice to the accused minimised? Are further safeguards required?

Question 46. Does a standard need to be set in Australia for unclassified summaries of classified information, ensuring that such summaries enable the defence to make out its case and to take any appropriate appeal?

Question 47. Does Australia need a statute or other provisions setting out a procedural framework for the disclosure and admission of classified and security sensitive information in criminal trials, possibly similar to the *Classified Information Procedures Act* (USA)? Should any such framework be incorporated in statute (such as the *Evidence Act 1995* (Cth) or the statutes establishing the various courts and tribunals) or court rules, or both?

Question 48. What methods are currently used by court, tribunals and parties in civil matters to regulate the discovery of classified or security sensitive information? Are these methods effective? Are these methods fair? How is prejudice to the parties minimised?

Question 49. Does Australia need statutory or other provisions setting out the procedural framework for the discovery and admission of classified and security sensitive information in civil and administrative hearings?

Other issues relating to investigations

6.22 Government agencies may receive demands (such as subpoenas) or requests for the release of information pursuant to certain statutory provisions (such as FOI legislation). The information sought may include classified or security sensitive information. In these circumstances, the agencies may have to take steps to protect the classified or security sensitive information. These steps could include resisting production of the documents based on a statutory exemption excusing production, a claim for public interest immunity (discussed in Chapter 8) or producing or releasing redacted versions of the documents, or versions where unclassified information is substituted for classified information.

Question 50. What methods are currently used by agencies and government departments to resist the production of classified or security sensitive information pursuant to a subpoena or a request for release of information pursuant to statutory provisions? Are these methods effective? Do they fairly balance the competing public interests in protecting classified and security sensitive information and in disclosure?

7. Presentation of Evidence in Court

7.1 Apart from the use of in camera and secret hearings, publication restrictions, and the use of security-cleared counsel (discussed in Chapters 5 and 13), consideration needs to be given to other mechanisms to present classified and security sensitive evidence during the course of court or tribunal proceedings, and the efficacy and fairness of such mechanisms. The presentation of evidence covers both oral testimony and the tendering of documents and other exhibits.

7.2 A distinction can be drawn between mechanisms to protect sensitive evidence and mechanisms to protect the *source* of sensitive evidence, although it is not certain whether this leads to any difference in principle or is just one of the variables to be taken into consideration by the court in determining how to proceed. As mentioned in Chapter 9, public interest immunity can protect the identity of an informant or of others supplying information to law enforcement authorities.[cclxxxviii]

Mechanisms to protect information

7.3 There are obviously some overlaps between the mechanisms used to protect classified and security sensitive information contained in documents in the discovery or pre-trial stages of a proceeding (discussed in Chapter 6) and the mechanisms used to tender documentary exhibits (or lead testimony) containing sensitive information during a trial or other hearing. The prosecution may seek to tender:

- documents with classified or sensitive material redacted or excised;
- unclassified summaries of classified material;
- documents in which classified information has been substituted with unclassified information; or
- a statement admitting relevant facts that the classified documents would tend to prove.

7.4 For example, in the Lappas trial, the prosecution intended to present 'empty shells of the documents, photocopies that ha[d] all the substantive text obliterated but show[ed] how they were laid out and how they were marked "Top Secret," "Not To Be Copied" and so on'.[cclxxxix] The prosecution also intended to lead some oral evidence of the 'character' of the documents in 'general terms so as not to place before the court the detail of what was contained within them'.[ccxc]

7.5 Section 8(b) of the *Classified Information Procedures Act* (USA) (CIPA) (discussed in detail in Chapter 6) provides that:

> The court, in order to prevent unnecessary disclosure of classified information involved in any criminal proceeding, may order admission into evidence, of only part of a writing, recording or photograph, or may order admission into evidence of the whole writing, recording, or photograph with excision of some or all of the classified information contained therein, unless the whole ought in fairness be considered.

7.6 Section 8(c) of CIPA provides:

> During the examination of a witness in any criminal proceeding, the United States may object to any question or line of inquiry that may require the witness to disclose classified information not previously found to be admissible. Following such an objection, the court shall take such suitable action to determine whether the response is admissible as will safeguard against the compromise of any classified information. Such action may include requiring the United States to provide the court with a proffer of the witness' response to the question or line of enquiry and requiring the defendant to provide the court with a proffer of the nature of the information he seeks to elicit.

7.7 The recent espionage trial of Brian Regan in the United States provides useful examples of an array of mechanisms employed to protect classified information, including blocking classified exhibits from public inspection and monitoring notes of the proceedings taken by the jury.

> Government and defense lawyers displayed confidential documents on … a high-tech overhead projector, the images viewed on television monitors facing away from spectators.
>
> Jurors could only take notes in special bluish-green notebooks … with each page numbered so that the court would know if they took any written information from the courtroom.
>
> In some cases, witnesses were asked to respond to handwritten statements from lawyers or to say whether they agreed with documents so secret that even their titles could not be mentioned in the courtroom.[ccxci]

7.8 The ALRC is interested in learning whether witnesses are ever questioned partially or wholly in written as opposed to oral form in Australian courts in order to protect classified or security sensitive information (or other forms of sensitive information, such as commercially sensitive information). If this practice has been used, was it fair and effective?

Mechanisms to protect sources of information

7.9 In cases involving classified or security sensitive information, including terrorism cases, security services may wish to protect the identity of an informant. In some cases, they may wish to protect the identity of members of the security services or other details of their operations.

7.10 Section 15XT(1) of the *Crimes Act 1914* (Cth) provides that:

> If the real identity of an approved officer or approved person[ccxcii] who is or was covered by an authorisation,[ccxciii] might be disclosed in proceedings before a court, tribunal or a Royal Commission or other commission of inquiry, then the court, tribunal or commission must:
>
> (a) ensure that the parts of the proceedings that relate to the real identity of the officer or person are held in private; and
>
> (b) make such orders relating to the suppression of the publication of evidence given by the court, tribunal or commission as will, in its opinion, ensure that the real identity of the officer or person is not disclosed.[ccxciv]

7.11 Other mechanisms to protect the identity of a witness or informant include referring to the witness or informant by letter or number only, making non-publication orders in relation to the person's identity, the use of a mask or voice distorter[ccxcv] and providing protective screens behind which a witness testifies, hidden from the public but in view of the defendant, jury and lawyers, who may therefore still observe the witness's demeanour.[ccxcvi]

German position

7.12 German courts have devised a method of dealing with evidence provided by informants who have been given a new identity and who can no longer appear in court. They accept the non-availability of these witnesses (usually undercover agents), do not require disclosure of their identity, and accept in substitution written statements made by them and the in-court testimony of the police officers who interrogated them. If the court requires additional information, it formulates written questions which are answered by the declarants without disclosing their identity to the court or the judge.[ccxcvii]

> Although aware of the problem that without knowing the identity of the declarant it was quite impossible to evaluate his credibility, the courts constantly refused suggestions not to admit such hearsay testimony but rather regarded it as a matter of careful evaluation. In addition, the courts emphasized that the probative effect of such evidence considered by itself would not provide an ample basis for conviction. In order to safeguard the interests of the accused they required further circumstantial evidence of uncontested probative value.[ccxcviii]

7.13 One person convicted of conspiring with a foreign intelligence service challenged the constitutionality of the German procedure on the ground that his rights to a fair trial and due process had been violated. The Federal Constitutional Court of Germany dismissed his complaint but set out some requirements for the validity of a conviction based on the exceptional procedure, including the following:

> 1. The executive decision to declare the prospective witness non-available in court must take place at the highest executive level, normally by a department directly headed by a member of the government.
>
> 2. Reasons must be given for this decision so as to enable the court to make an independent evaluation of its plausibility; the reasons must be as full as they can be without disclosing the secret to be protected.

3. There must be corroborating evidence confirming the hearsay evidence.[ccxcix]

4. In evaluating the evidence the court must take into account that the hearsay evidence is of less value than evidence heard in court directly and immediately.[ccc]

7.14 There are, of course, differences in the German civil law system and the Australian common law system. German criminal procedure is substantially non-adversarial and German law does not have a hearsay rule. The use of hearsay evidence from undisclosed sources has ramifications for an accused person's right to a fair trial, which includes a right to confront the witnesses against him or her.[ccci] The risks of hearsay evidence include a danger that the repetition will be inaccurate and the potential for fabrication of evidence. Some of the dangers associated with the use of hearsay evidence are mentioned in Chapter 5 in relation to the use of secret evidence.

Gagging orders

7.15 Other factors to take into account in considering the presentation of classified or security sensitive information in court proceedings are the methods to which parties can have recourse in seeking to prevent the presentation and revelation of such evidence. The most obvious method is a claim for public interest immunity (see Chapter 8).

7.16 Another example drawn from overseas is the use of gagging orders. In the recent treason trial in Zimbabwe of President Robert Mugabe's main political opponent, Morgan Tsvangirai, the Zimbabwean government made a gagging order against a key prosecution witness, citing national security concerns. The State Security Minister issued a certificate to the witness, a Canadian political consultant, ordering him not to reveal details of a contract he had with the government.[cccii] Garwe J eventually overruled the government's gagging order, enabling the treason trial to proceed. He ruled that details of the government contract had to be revealed, ordered an in camera proceeding and ordered that the evidence in that proceeding not be disclosed publicly by any person.[ccciii]

Question 51. Apart from closed courts, secret evidence, restrictions on reporting, and the use of security-cleared counsel, what other mechanisms are, or might be, used in Australian courts and tribunals to present classified and security sensitive information during proceedings? Are these mechanisms effective? Are they fair? Do they have proper safeguards against abuse?

Question 52. Have Australian courts or tribunals obtained testimony involving classified or security sensitive information in written, rather than oral, form in order to protect that information or its source? If so, has this practice been fair and effective?

Question 53. What mechanisms are, or might be, used by Australian court and tribunals to protect the identity of informants or confidential sources of classified or security sensitive information? Are these mechanisms effective? Are they fair? Do they have proper safeguards against abuse?

8. Public Interest Immunity

8.1 The Terms of Reference ask the ALRC to consider the operation of existing mechanisms designed to prevent the unnecessary disclosure of classified material or security sensitive material in the course of criminal or other official investigations and court or tribunal proceedings of any kind, including common law public interest immunity. Public interest immunity is also legislated for under s 130 of the *Evidence Act 1995* (Cth), and in the various evidence laws of the States and Territories.

8.2 A claim of public interest immunity (also called state interest immunity) is one of the most common ways in which information can be protected in court proceedings. The rule allows the court to limit a party's access to evidence before or during trial.[ccciv]

8.3 There is an obvious public interest in protecting information where its disclosure would affect national security or other critical state interests. The question for the ALRC in this inquiry is how effective the current application of public interest immunity is in protecting classified and security sensitive information and in striking the right balance between the public interest in protecting that information, the public interest in an open and transparent justice system and the private interests of the individuals involved in each case.

8.4 In the Lappas case, the prosecution sought to use 'empty shells' of two of the documents in proceedings and provide only very general oral summaries of their contents. The trial judge, Gray J, upheld the claim for public interest immunity and, because the defence could not then properly give evidence related to the contents of those documents, the prosecution on one of the charges against Lappas was stayed.[cccv]

Common law public interest immunity

8.5 The common law formulation of public interest immunity can be found in *Sankey v Whitlam*:

> [T]he court will not order the production of a document, although relevant and otherwise admissible, if it would be injurious to the public interest to do so.[cccvi]

8.6 In essence, public interest immunity operates as a balancing test. Courts limit the disclosure of information or documents on the basis that the public interest against disclosure outweighs the need for disclosure to ensure justice in a particular case.[cccvii]

8.7 Public interest immunity can be distinguished from a privilege (although it was called 'Crown privilege' in its early conception). In the case of privileges, only the party holding the information is able to invoke it on its own behalf whereas a claim of public interest immunity can be made by the state or by the court on its own motion. Where public interest immunity is applied, all evidence related to the relevant secret is excluded, including any secondary evidence held by third parties.[cccviii] Thus:

> If the document cannot, on principles of public policy, be read into evidence, the effect will be the same as if it were not in evidence, and you may not prove the contents of the instrument.[cccix]

8.8 The relevance of the material in question is an important element in the balancing exercise. The court must be satisfied that there is a legitimate forensic purpose in having access to the information. The more central the evidence is to the issues of the case, the more the balance may tip in favour of disclosure.[cccx] This may be one way to meet the risk of greymail, where a party's threat to disclose classified or security sensitive information will be defeated unless the court is satisfied that the party has a legitimate purpose or need to do so.

Evidence Act 1995 (Cth)

8.9 In the commentary on the common law doctrine of public interest immunity in the ALRC's *Evidence* interim report,[cccxi] the ALRC found no serious inadequacies in the common law approach overall, and recommended as little interference with the supervisory role of the courts as possible.[cccxii] However, the ALRC did recommend a change from the (then) accepted common law formula which required the judge, in determining whether to grant public interest immunity, to balance the competing interests at a general level. The ALRC supported a more specific formula balancing 'the nature of the injury which the nation or public service is likely to suffer, and the evidentiary value and importance of the documents in the particular litigation'.[cccxiii]

8.10 The ALRC also listed the considerations which should guide the courts in balancing the public interest in a given case:

- the importance of evidence in the proceeding;
- whether the proceeding is criminal;
- whether the evidence is adduced by the defendant or by the prosecution;
- the gravity of the charge; and
- the likely effect of the disclosure of the evidence.[cccxiv]

8.11 The *Evidence Act 1995* (Cth) substantially reflects the recommendations of the ALRC. Section 130(1) provides that

> if the public interest in admitting into evidence information or a document that relates to matters of state is outweighed by the public interest in preserving secrecy or confidentiality in relation to the information or document, the court may direct that the information or document not be adduced as evidence.

8.12 The ALRC's aim in proposing legislative amendments to public interest immunity was to create predictability while allowing the exercise of discretion where required. To this end, the *Evidence Act* includes guidelines aimed to promote consistency of application.[cccxv]

8.13 The factors outlined as comprising the public interest are consistent with those developed by the prior common law.[cccxvi] In *State of NSW v Ryan*,[cccxvii] the Federal Court held that there was no relevant difference, in relation to a public interest immunity claim for cabinet papers, between the common law as determined in *Sankey v Whitlam*[cccxviii] and the provisions of s 130.[cccxix] Similarly, von Doussa J found in *Chapman v Luminis Pty Ltd (No 2)*[cccxx] that the common law principles considered in *Aboriginal Sacred Sites Protection Authority v Maurice*[cccxxi] continued to apply under s 130.[cccxxii]

8.14 Section 130(1) indicates that the onus is on the party arguing that the public interest in preserving secrecy or confidentiality that relates to matters of state to show that this factor outweighs the public interest in admitting into evidence the information or document.[cccxxiii] This reflects the common law in that it does not confer absolute immunity on information relating to matters of state or an absolute right to protect the information,[cccxxiv] and appears to apply to both oral and documentary evidence.[cccxxv] Mechanisms used to protect evidence governed by the statute are the same as under the common law:

- evidence taken in camera;[cccxxvi]
- restriction of the publication of evidence;
- suppressing the names of parties and witnesses;[cccxxvii]
- limiting access to evidence to a party's legal advisors;[cccxxviii] and
- granting absolute immunity.

8.15 Section 130 varies from the common law in some minor respects. For example, some considerations raised in various decided cases are omitted from the list of relevant considerations listed in s 130(5) that a court must take into account in determining the competing public interests referred to in s 130(1). These include: whether the objection to disclosure is a class claim or a contents claim; whether a representative of government has supported non-disclosure of the information or document; the subject matter of the information or document; whether the information or document has contemporary importance or is only of historical interest; and whether the information or document was acquired on the basis that it would be kept confidential.[cccxxix]

8.16 While the Act is in most respects a restatement of the common law, it only applies to the admission of evidence.[cccxxx] Therefore the common law still applies in pre-trial contexts such as discovery, interrogatories and notices to produce whereas the Act applies to interlocutory proceedings, final hearings and on appeal. The exception to this is in New South Wales, where rules of court extend the operation of s 130 to ancillary processes.[cccxxxi]

8.17 A number of matters became unclear following the enactment of s 130. First, the expression 'information or a document that relates to matters of state' created an opportunity for the delineation of new boundaries concerning the scope of public interest immunity. Although it was predicted that the words would be given a wide interpretation by the courts, the implications of the word 'state' created uncertainty as to whether public interest immunity would be limited strictly to categories of governmental matters.[cccxxxii] In *R v Young,* NSW Chief Justice Spigelman indicated that the notion of public interest reflected in s 130 confines the application of public interest immunity to those subjects with a dimension that is 'governmental in character'.[cccxxxiii]

8.18 Some areas of controversy regarding the application of the section include whether indigenous cultural information with no connection to the government could fall within public interest immunity[cccxxxiv] and how courts can distinguish between the public and private activities of a state.[cccxxxv]

When is public interest immunity claimed?

8.19 Public interest immunity is available at common law at all stages of the judicial process, including issuing and answering subpoenas, ordering inspection following discovery, or in examining witnesses.[cccxxxvi] As noted above, s 130 of the *Evidence Act* applies only to the admission of evidence, not pre-trial procedures.[cccxxxvii]

Question 54. Should there be a difference in the treatment of claims for public interest immunity made before trial and at trial? Have any practical problems arisen from the application of the common law and the *Evidence Act 1995* (Cth), or from any difference between them?

Question 55. In determining a claim for public interest immunity, should the classification status of classified or security sensitive information be reviewed before or after its relevance is established?

Who claims it?

8.20 Under the concept of crown privilege, agents of the crown could claim on behalf of the government that disclosure of specified information would be against the public interest.[cccxxxviii] Subsequent development of the rule has extended the right to claim beyond a strictly prerogative right of the crown to other litigants and interested people.[cccxxxix] Claims may be made by a party to proceedings, a witness or the state.

8.21 Claims for public interest immunity are most commonly made by the government in relation to cabinet deliberations, high level advice to governments, communications or negotiations between governments, national security, police investigation methods, or in relation to the activities of ASIO and ASIS officers, police informers, and other types of informers.[cccxl]

Differences between criminal and civil matters

8.22 The courts' inclination to inspect documents subject to a claim of public interest immunity can vary according to whether the proceedings are criminal or civil.[cccxli] In criminal cases, courts are more readily prepared to inspect documents to determine if public interest immunity applies.[cccxlii] In *Alister v The Queen*, Brennan J (as he then was) stated:

> In a criminal case it is appropriate to adopt a more liberal approach to the inspection of documents by the court. The more liberal approach is required to ensure, so far as it lies within the court's power, that the secrecy which is appropriate to some of the activities of government furnishes no incentive to misuse the processes of the criminal law.[cccxliii]

8.23 In relation to criminal proceedings, an accused's interest in obtaining exculpatory materials generally prevails over a claim for public interest immunity, based on the overriding public interest in ensuring that innocent people are not condemned when their innocence can be proved.[cccxliv] This interest can outweigh a general public interest against disclosure of police information,[cccxlv] and state papers where a person's liberty is at stake.[cccxlvi] This principle also applies in regard to sources of police information, except documents and other evidence involving vital state interests.[cccxlvii] Similarly, the informer rule is treated differently at criminal trials if the accused person demonstrates that disclosure of the identity of the informer could assist the defence, whether by establishing innocence or by raising a reasonable doubt.[cccxlviii]

Question 56. Should claims for public interest immunity be treated differently in civil and criminal cases? If so, should this difference be reflected in legislation, regulations or court rules?

Class claims and contents claims

8.24 A claim for public interest immunity can be made because it is detrimental to the public interest to disclose the particular information contained in a document (a 'contents' claim) or because the document belongs to a class of documents which, in the public interest, should not be disclosed (a 'class' claim)—for example, Cabinet documents.

8.25 There is some controversy surrounding the concept of a class claim. In the UK, the Scott Inquiry considered whether it was appropriate that advice given to ministers be part of a blanket class of protected documents.[cccxlix] The argument advanced was that public servants must be allowed to give candid advice without fear. However, not all advice necessarily warrants such concerns. For example, information can be distinguished from advice or opinion, which may set out the thinking behind policy formulation in greater detail, and include arguments for and against the policy settled upon.[cccl]

8.26 Can classified or security sensitive information found a class claim for public interest immunity? Information relating to national security, such as defence secrets and documents concerning inter-governmental relations, has long been accepted as archetypically the sort of information that would be the subject of a claim for public interest immunity.[ccli] National security information will often be contained in the types of government documents that could be considered as part of a class claim. In *Alister*, Wilson and Dawson JJ noted that:

> The outstanding feature of the claim to immunity is the nature of the public interest which the Minister seeks to protect. Questions of national security naturally raise issues of great importance, issues which will seldom be wholly within the competence of the court to evaluate. It goes without saying in these circumstances that very considerable weight must attach to the view of what national security requires as expressed by the responsible Minister.[cclii]

8.27 However, Wilson and Dawson JJ were careful not to go so far as to say that the fact a document contained national security information was conclusive on the issue.[ccliii] In the case of documents dealing with matters of national security, while a court is highly likely to tip the balance in favour of suppression of the information, it is unlikely to do so as a matter of course without first scrutinising the government claims.[ccliv]

8.28 The ALRC is also interested in learning of cases in which only part of the document may rightfully be subject to a claim of public interest immunity. With respect to national security information, the Scott Inquiry expressed some concern that a blanket grant of immunity on the basis that some parts of a document contained sensitive information was not desirable and a closer look at the damage that could actually be caused by each part of the information was warranted.[cclv]

Question 57. Should class claims for public interest immunity be maintained or abolished?

Question 58. Should the fact that proposed evidence contains classified or security sensitive information of itself be sufficient basis for a claim of public interest immunity?

Ministerial certificates

8.29 In 1942, the House of Lords made a controversial decision that courts should accept without question a certificate issued by a minister certifying the government's view that the document or secret should be excluded in the public interest.[cclvi] Aronson and Hunter argue that the doctrine of conclusive certificates was abused by governments for many years, with certificates often being issued simply to protect the government from any claim of liability.[cclvii] In the UK, this doctrine was overturned in *Conway v Rimmer*.[cclviii]

8.30 In Australia, *Sankey v Whitlam* made it clear that the common law doctrine no longer regards ministerial certificate claims as conclusive, preferring the court as the ultimate guardian of public policy to ensure justice in each case.[cccli] On this fundamental issue, the courts have distinguished between governmental and public interest, increasingly holding that certain matters of public interest fall outside the ambit of government security concerns, such as child abuse informants and evidence of Aboriginal sacred sites.[ccclx]

8.31 Section 42D of the Northern Territory *Evidence Act 1939* allows the NT Attorney-General to issue a conclusive certificate that disclosure of a document or record in legal proceedings would not be in the public interest; however, this is the only state or territory legislation to do so.

Question 59. Should a ministerial certificate ever be conclusive on the question of public interest immunity or should the court always retain a discretion to inspect the material and determine for itself how it should be handled?

Question 60. Is it necessary or desirable to require every claim for public interest immunity to particularise the information in respect of which the claim is raised and the damage which it is feared would result from its disclosure? If so, what mechanisms could be used to achieve this?

9. Criminal Court Proceedings

Some preliminary distinctions

9.1 It is convenient to distinguish matters in which classified or security sensitive information is central to the prosecution (for example, in a prosecution for espionage or unauthorised disclosure of official secrets) and those in which such information is incidental. Obviously, the tension between the interest of the state in protecting such information by avoiding or limiting its disclosure, and the right of an individual to a fair hearing is more acute where classified or security sensitive information is central to the indictment.

9.2 It is also necessary to distinguish between cases in which the classified or security sensitive information relevant to a prosecution is known to both parties and those in which it is known only to the state. A defendant who is aware of the contents of classified or security sensitive information is in a superior position to a defendant who does not—for example, in determining whether or not, or to what extent, to challenge attempts by the Crown to avoid or limit the disclosure of such information; in deciding whether to lead or tender such evidence; and in preparing his or her defence generally. There is less risk that a departure from normal court procedures will result in unfairness to the defendant in such cases.

9.3 The case of Zacarias Moussaoui, the alleged conspirator in the attacks against the World Trade Centre and the Pentagon on 11 September 2001, provides a telling example of a matter where classified information is known only to the state. It illustrates the clash between the accused's right to information that could assist in his defence and the need to safeguard national security.[cccLxi] Judge Brinkema has warned prosecutors that she found merit in Moussaoui's demands for more information and has questioned whether the US government could give Moussaoui a fair trial in open court while keeping documents and information secret.[cccLxii] The US Justice Department has stated that it would be able to try Moussaoui in a civilian court while protecting his rights and government secrets, affirming US Attorney General Ashcroft's objection to moving the case to a military tribunal, even though some Pentagon and intelligence officials would prefer that option.[cccLxiii]

Prosecution of military and intelligence personnel

9.4 Prosecutions involving military and intelligence personnel are more likely to fall into the category of cases where the defendants are privy to classified or security sensitive information in the possession of the state.[cccLxiv] It is in these types of cases that, historically, defendants have made greymail threats to divulge classified information during the course of a trial. As mentioned in Chapter 6, the greymailing defendant presents the government with the dilemma of either disclosure of the classified information, or dismissing or compromising the indictment. It has been observed that:

> Graymail is particularly invidious because it is likely to be most successfully employed by former officials from the heart of the government machine who subsequently face trial … [cccLxv]

9.5 According to Lustgarten and Leigh, the lawyers representing Colonel Oliver North and Admiral Poindexter, who faced charges in the USA arising from the Iran-Contra affair, used the tactic with some success.[cccLxvi]

Prosecution of terrorists

9.6 Magner has queried whether the laws of evidence should apply to the trial on criminal charges of terrorists or alleged terrorists, and whether certain rules of evidence should be altered where the accused is suspected of being a terrorist.[cccLxvii] Magner submits that there is no obligation to apply the same rules of evidence to all cases or to all criminal cases:

> The suggestion that special rules of evidence might be appropriate is premised on the fact that the law of evidence recognizes several interests.
>
> … as terrorists have declared war on society in general, terrorist activities may represent a threat to the processes and personnel involved in the trial. Witnesses who appear in court to testify against terrorists may be in danger of violent retaliation by the terrorists' friends or colleagues. The court itself may be bombed. It may be that there is a strong public interest which justifies altering the rules which would normally be insisted upon in the interests of the highest standard of accuracy.[cccLxviii]

9.7 Magner suggests that one area of the law of evidence that might be modified for the purposes of trials of terrorists is the rules relating to public interest immunity.[cccLxix] She puts forward an alternative to the present regime whereby the court weighs the public interest in not disclosing information with the interests of justice in the particular case in order to decide whether or not to order disclosure:

> Where the case is a criminal prosecution for an act of terrorism, it may be appropriate instead for the court to accept that the information will not be disclosed and instead consider whether the information concerned is necessary for the case. If the information is vital and cannot be produced then it may be appropriate to dismiss the case.[cccLxx]

9.8 It is a matter for debate whether the nature of an alleged offence is, or should be, determinative of any rights enjoyed by, or withheld from, an accused, or whether it is simply another variable to be taken into account by a court in considering the procedure to be adopted in any particular case.

9.9 As discussed above (see Chapter 5), Article 14 of the International Covenant on Civil and Political Rights (ICCPR) guarantees the accused's right to a fair trial and sets out the minimum protections to be afforded to the accused in the trial process. Article 26 of the ICCPR provides that all persons are equal before the law and are entitled without discrimination to the equal protection of the law. However, in emergency

situations countries are allowed to derogate from the protections afforded by the ICCPR.

9.10 Other issues that arise in relation to the prosecution of terrorists are whether those prosecutions should be conducted in a normal civilian court, in a specialist terrorist court,[cccLxxi] or in military tribunals; and whether terrorist courts or military tribunals would afford the accused the normal protections in relation to receiving a fair trial. For example, on 13 November 2001, President Bush signed a Military Order that suspected terrorists could be tried in military tribunals rather than in the normal court system.[cccLxxii] (Military tribunals are discussed in Chapter 12).

Question 61. Is there a need to consider a special category of defendant where some of the normal protections usually afforded to a criminal accused are withheld in order to protect classified and security sensitive information?

Question 62. If so, what modifications of these protections should be considered? Would such modifications be consistent with Australia's obligations under international law?

Closure of criminal proceedings

9.11 The closure of criminal proceedings presents additional issues.[cccLxxiii] For example, the US Supreme Court has established procedural requirements that must be adhered to prior to closing a court in a criminal case in light of issues that arise from the First Amendment to the US Constitution.[cccLxxiv] Representatives of the press and general public must be given an opportunity to be heard on the question of their exclusion. Notice must be provided before the court is closed to ensure that the press and general public's opportunity to be heard is meaningful.[cccLxxv]

> If a trial court wants to close its courtroom following the hearing, it must issue specific findings of fact that 'closure is essential to preserve higher values [than the constitutional right of access] and is narrowly tailored to serve that interest'. One reason that this procedural component is so important is so 'that a reviewing court can determine whether the closure order was properly entered'.[cccLxxvi]

Question 63. Should Australian courts be required to give notice to the public, the press or other media of their intention to close criminal proceedings on grounds relating to the use of classified or security sensitive information, and to give the public, press and other media an opportunity to be heard on the question of their exclusion?

Guidelines

9.12 In the United States, the *Classified Information Procedures Act* (CIPA) required the US Attorney General to issue guidelines 'specifying the factors to be used by the Department of Justice in rendering a decision whether to prosecute a violation of Federal Law in which, in the judgment of the Attorney General, there is a possibility that classified information will be revealed'.[cccLxxvii] The resultant *Guidelines for Prosecutions Involving Classified Information* set out four factors that prosecutors should consider in ascertaining whether 'the need to protect against the disclosure of classified information outweighs other federal interests that would be served by proceeding with the prosecution':[cccLxxviii]

(i) the likelihood that classified information will be revealed if the case is prosecuted;

(ii) the damage to the national security that might result if classified information is revealed;

(iii) the likelihood that the government will prevail if the case were prosecuted; and

(iv) the nature and importance of other federal interests that would be served by prosecution.[cccLxxix]

9.13 As internal policy of the Department of Justice, the *Guidelines* do not create enforceable rights for the benefit of defendants.[cccLxxx] A decision by the Department of Justice not to prosecute pursuant to the *Guidelines* must be accompanied by written findings detailing the reasons for the decision.[cccLxxxi] The findings are to include:

1. the intelligence information which the Department of Justice officials believe might be disclosed;

2. the purpose for which the information might be disclosed;

3. the probability that the information would be disclosed; and

4. the possible consequences such disclosure would have on the national security.[cccLxxxii]

9.14 This raises the question whether, in Australia, the Prosecution Policy of the Commonwealth[cccLxxxiii]—which sets out the factors to be considered in making a prosecution decision—should be amended in any way to specify the factors that will be relied upon by the Commonwealth Director of Public Prosecutions (DPP) in making a decision to prosecute in a matter where there is a possibility that classified or security sensitive information will be revealed. The DPP's Statement on Prosecution Disclosure provides that an investigating agency[cccLxxxiv] is to provide the DPP with a schedule of potentially disclosable material which the agency considers may be immune from disclosure to the defence on public interest grounds, together with the reasons supporting such a conclusion.[cccLxxxv]

9.15 Among the examples given of such material are:

(a) material relating to the identity or activities of informants, undercover police officers or other persons supplying information to law enforcement authorities; …

(c) material revealing, either directly or indirectly, investigative techniques and methods relied upon by law enforcement agencies in the course of a criminal investigation (for example, covert surveillance techniques) or other methods of detecting crime; …

(e) material relating to national security;

(f) material received from an intelligence or security agency; …[cccLxxxvi]

9.16 The Statement on Prosecution Disclosure addresses the situation where the prosecutor considers that sensitive material should be disclosed to the defence as 'unused material' but the investigating agency disagrees and does not intend to claim public interest immunity:

> Where the Director considers that the prosecution cannot fairly continue without disclosure the Director will decide whether the prosecution should be continued or abandoned. In some cases, however, it may be possible to proceed on different charges which would not require the disclosure of the subject material.[cccLxxxvii]

9.17 Where a claim for public interest immunity is made but fails:

> the DPP will consider, following consultation with the investigating agency, whether the overall interests of justice require that the material be disclosed or, alternatively, that the prosecution be abandoned.[cccLxxxviii]

9.18 The prosecution also has an obligation to disclose to the defence matters affecting the credibility or reliability of prosecution witnesses.[cccLxxxix] Where the identity of a witness is the subject of a claim for public interest immunity, the question arises as to how the prosecution can discharge its obligations in this regard without revealing the witness's identity.[cccxc]

Question 64. Should guidelines be developed for the disclosure, withholding and use of classified and security sensitive information in criminal matters?

Question 65. Should the *Prosecution Policy of the Commonwealth* be amended to specify the factors that will be relied upon by the Director of Public Prosecutions in making a decision whether to prosecute where there is a possibility that classified or security sensitive information will be revealed?

Question 66. Do guidelines need to be developed outlining how the prosecution will discharge its obligation of disclosing to the defence matters affecting the credibility or reliability of a prosecution witness in cases where the identity of the witness is the subject of a claim for public interest immunity?

10. Civil Court Proceedings

10.1 It is not only in criminal prosecutions that the protection of classified or security sensitive material will arise as an issue. For example, Mrs Sandra Jenkins is currently suing the federal government for compensation arising from the suicide of her husband, Merv Jenkins, an Australian intelligence officer who was under investigation for allegedly passing classified information to allies. A key feature of this case could be her ability to obtain access to any classified or security sensitive information relevant to the presentation of her claims.

10.2 There are a number of different contexts in which the use of or access to classified or security sensitive information may be an issue in civil proceedings. For example, this would include claims:

- brought against a government department or agency by, for example, members of the defence forces, intelligence personnel or their dependents or estates;

- brought by the government against a private third party arising, for example, out of damage caused by that third party to property, the existence or significance of which the third party was unaware, or which would emerge if evidence that would normally be disclosed is produced; and

- against the government by private third parties, the evidence surrounding which involves classified or security sensitive information that would emerge in the normal course of that litigation.

10.3 In any of these categories, the classified or security sensitive information could be peripheral to the factual background to the case, or could be central to it and critical to the court's decision. The withholding of classified or security sensitive information could leave the third party unable to advance its case or its defence, and could leave the government itself unable to do so, stymied by its own need in the public interest to limit access to sensitive information. The court may find this restriction of access to be so unfair in the circumstances of a particular case that it determines that the case cannot proceed in the usual way and must be compromised in a manner determined by the requirements of justice overall rather than by the merits of the case.

10.4 In a civil case, a party may seek to obtain classified or security sensitive information through discovery. That party may not be aware of whether the particular information sought exists, what form it takes or the particular contents of any document. This lack of knowledge may lead to the risk of having its application for discovery rejected as a fishing expedition.[cccxci]

10.5 There are also cases where a governmental decision or action relating to national security is the heart of the claim, as in *Church of Scientology v Woodward.*[cccxcii] In that

case, the association and individual members of the Church of Scientology sued the Director-General of ASIO, the Attorney-General and the Commonwealth on various grounds for declarations that they were not security risks and on the basis that the Director-General had acted outside his authority under the ASIO Act in gathering and communicating information describing them as risks.

10.6 Although the church's claim was ultimately dismissed in the High Court, Mason J (as he then was) stated that ASIO's activities are subject to judicial review, although the revelation of security intelligence in legal proceedings would be detrimental to national security.[cccxciii] In addition, although security intelligence is 'not readily susceptible to judicial evaluation and assessment', the court can still determine whether it is relevant to security in a given instance.[cccxciv] Brennan J (as he then was) stated that discovery would not be given against the Director-General, save in a most exceptional case, as the secrecy of ASIO's work is essential to national security and will seldom yield to a public interest in the administration of civil justice.[cccxcv]

Public interest immunity in civil proceedings

10.7 In civil proceedings, where the Crown objects to the production of documents on the basis of public interest immunity, the court must have 'some concrete ground for belief which takes the case beyond a mere "fishing" expedition' that the documents should appear likely to support the case of the party seeking discovery before ordering that discovery take place.[cccxcvi] The party seeking to satisfy that onus must do so without access to the documents in question.[cccxcvii] Finally, lower courts should in all cases take the precaution of postponing disclosure pending any appeal.[cccxcviii]

10.8 Public interest immunity is a crucial aspect of civil proceedings involving national security. However, a successful claim for such immunity could well have the effect, intended or otherwise, that the other party may not be able to establish its claim or defence if the government can prevent sensitive evidence being brought out.[cccxcix]

10.9 Where national security is at the heart of the claim—for example, where the government is arguing that its actions in dispute related to national security—these arguments are particularly circular. As Lustgarten and Leigh suggest, suppression of the evidence prevents the court from forming an independent view of the government's claim that its action was based on reasons of national security.[cd]

> Control of information is a powerful tool—if the government claims that the information necessary to resolve the case cannot be disclosed without compromising national security, the court is faced with a direct choice between accepting the executive's assertion, ordering disclosure of the information (which amounts to saying it knows better), or trying to determine the substance of the case on inadequate information. The last option will, in the nature of things, usually result in the benefit of the doubt being given to the government.[cdi]

10.10 An impossible burden may be placed on the party against the government in such a case:

> The practical effect of requiring a person challenging a security decision to produce evidence which is virtually impossible to obtain is to nullify the judiciary's assertion that the rule of law nevertheless applies.[cdii]

10.11 In *Church of Scientology v Woodward*, Mason J conceded that a successful claim of Crown privilege (public interest immunity) makes the task of judicial review of ASIO activity difficult:

> The fact that a successful claim to Crown privilege handicaps one of the parties to litigation is not a reason for saying that the court cannot or will not exercise its ordinary jurisdiction; it merely means that the court will arrive at the decision on something less than the entirety of the relevant materials.[cdiii]

Question 67. What has been the experience and practice of courts and tribunals, and parties and practitioners appearing in them, in dealing with the protection and disclosure of classified or security sensitive information in civil matters? Are there problems with the disclosure, withholding or use of classified or security sensitive information? Has this meant that claims have not been pursued or that non-governmental parties have been unfairly disadvantaged?

Question 68. Should guidelines be developed for the disclosure, withholding or use of classified and sensitive information in civil matters?

11. Immigration and Similar Hearings

Introduction

11.1 The use of classified and security sensitive information in immigration and similar hearings can be distinguished from the use of such information in criminal hearings, principally on the basis that in immigration hearings the government usually seeks to adduce sensitive evidence that is unknown to the other party. By contrast, in criminal matters the government may find itself attempting to limit the disclosure of sensitive information by the accused.

11.2 In recent years, particular issues have arisen in Australia and overseas in relation to the use and protection of classified and security sensitive information in immigration, citizenship, passport and deportation cases. These are outlined below. One issue is whether the definitions of a 'threat to national security' or 'national security' in the context of immigration hearings are—or should be—any different from those in other cases, including criminal cases.[cdiv] Further, as discussed below, secret evidence increasingly has been used in immigration and similar hearings. This raises the basic issue whether secret evidence should be allowed in these (or any) hearings, especially as it is not allowed in criminal hearings.

International obligations

11.3 Article 32 of the Convention Relating to the Status of Refugees (the Refugee Convention)[cdv] provides that:

> 1. The Contracting States shall not expel a refugee lawfully in their territory save on grounds of national security or public order.
>
> 2. The expulsion of such a refugee shall be only in pursuance of a decision reached in accordance with due process of law. Except where compelling reasons of national security otherwise require, the refugee shall be allowed to submit evidence to clear himself, and to appeal and to be represented for the purpose before competent authority or a person or persons specially designated by the competent authority.

11.4 The Australian government has made a reservation with respect to Article 32 of the Convention and does not accept the obligations stipulated in the Article. However, Australia is bound by Article 13 of the International Covenant on Civil and Political Rights (ICCPR), which (though not limited to refugees) is in similar terms to Article 32 of the Refugee Convention. It provides:

> An alien lawfully in the territory of a State Party to the present Covenant may be expelled therefrom only in pursuance of a decision reached in accordance with law and shall, except where compelling reasons of national security otherwise require, be allowed to submit the reasons against his expulsion and to have his case reviewed by, and be represented for the purpose before, the competent authority or a person or persons especially designated by the competent authority.

11.5 The requirement that people facing expulsion be allowed to submit evidence against their expulsion carries an implicit requirement that they be allowed to know the case for expulsion.[cdvi]

> Keeping adverse allegations and/or evidence secret from such a person denies them an opportunity to refute the adverse material. The person is, therefore, denied the opportunity to make the best possible case against visa refusal to the decision-maker and/or to demonstrate to a reviewing authority that the refusal decision is based on a shaky foundation of 'fact' and/or inference. Moreover, if the providers and users of adverse material know that the material will not be scrutinised by others, they have less incentive to test rigorously that material for veracity themselves.[cdvii] …
>
> For this reason, too, it is not conducive to the making of correct decisions to keep adverse material secret.[cdviii]

11.6 Article 13 of the ICCPR is qualified by the rider 'except where compelling interests of national security otherwise require'. Measures adopted for national security reasons must conform to the principle of proportionality, which is well established in international human rights law.

> [T]he measure must be the least oppressive means available for promoting the national security goal, and additionally, the public interest gain must outweigh the cost to the affected individual. … The question and decision we now face is whether, post-September 11, the proportionality requirement will continue to be given real meaning.[cdix]

11.7 Other relevant articles in the Refugee Convention which are binding on Australia include:

- Article 9, which allows a Contracting State 'in times of war or other grave exceptional circumstances [to take provisional] measures which it considers to be essential to national security in the case of a particular person, pending a determination … that the person is in fact a refugee and that the continuance of such measures is necessary in his case in the interests of national security'.

- Article 33, which prohibits the expulsion or *refoulement* of a refugee to a territory 'where his life or freedom would be threatened on account of his race, religion, nationality, membership of a particular social group or political opinion',[cdx] unless 'there are reasonable grounds for regarding [the refugee] as a danger to the security of the country in which he is, or who, having been convicted by a final judgment of a particularly serious crime, constitutes a danger to the community of that country'.[cdxi]

Australia

11.8 The use of secret evidence by the federal government and ASIO recently attracted headlines in the case of 19-year-old Zak Mallah, who was refused an Australian passport based on an adverse security assessment. According to a newspaper report of the case:

> The [Administrative Appeals T]ribunal[cdxii] conducted in-camera hearings to protect the identity of ASIO agents who carried out the security assessment.
>
> Not even Mr Mallah's counsel could be present to cross-examine the ASIO evidence. The nature of ASIO's case and its sources have also been withheld although its counsel told the tribunal it would also rely on transcripts of media interviews.[cdxiii]

11.9 The *Administrative Appeals Tribunal Act 1975* (Cth) provides for hearings to be in public except in exceptional circumstances.[cdxiv] While the Administrative Appeals Tribunal (AAT) may determine who may be present at a hearing at any time,[cdxv] the Minister administering the *Australian Security Intelligence Organisation Act 1979* (Cth) may issue a certificate stating that the submissions proposed to be made by the Director-General of Security or other agency are of such a nature that disclosure would be contrary to the public interest as it would be prejudicial to the security or defence of Australia:

> If such a certificate is issued, and they usually are, the applicant and usually the applicant's representative cannot be present when the evidence is adduced.[cdxvi]

11.10 Asylum seekers in Australia who are permitted to apply for a protection visa[cdxvii] must satisfy, among other things, public interest criterion 4002 (found in the *Migration Regulations 1994*), which requires the applicant to be assessed by the competent Australian authorities not to be directly or indirectly a risk to national security.[cdxviii] ASIO carries out the security assessments to which public interest criterion 4002 refers.

11.11 The transparency of ASIO security assessments in immigration matters has been questioned; ASIO's allegedly erroneous security assessment of Mr Sultan, an asylum seeker from Kuwait has been cited as an example.[cdxix] Mr Sultan was refused a protection visa on two grounds, one being that he had failed to satisfy public interest criterion 4002 because he had been 'assessed by the competent Australian authorities to be directly or indirectly a risk to Australian national security.'[cdxx] Mr Sultan's lawyer complained to the Director-General of Security and the Inspector-General of Intelligence and Security, alleging defects in ASIO's security assessment process. Following an internal review by the Director-General of Security, which concluded, among other things, that 'ASIO relied on adverse reports from an overseas security service which were internally inconsistent' and that 'ASIO took no action to corroborate the allegations in the reports, contrary to internal guidelines', the Director-General of Security withdrew Mr Sultan's adverse security assessment.[cdxxi] Mr Sultan made a fresh application for a protection visa, which was granted.

11.12 Generally, the decision maker is not made aware of the actual information upon which ASIO has based its adverse security assessments.[cdxxii] Furthermore, there is no requirement that ASIO disclose adverse material to the applicant[cdxxiii] or provide a statement of its grounds for an adverse assessment.[cdxxiv] Taylor states that the:

> withholding of information from the protection visa decision-maker means that the decision-maker is not in a position to evaluate for himself or herself the seriousness of

> the danger posed by the applicant, let alone the proportionality between the danger to Australian security which is averted by removal of the applicant and the danger to which the applicant is thereby exposed.[cdxxv]…
>
> The manner in which the relevant legislation is presently drafted means that public criterion 4002 is 'incapable of being met if an adverse assessment is made by [ASIO]'.[cdxxvi]

11.13 Taylor suggests the creation of a specialist unit within the Refugee Review Tribunal (RRT) staffed by officers with security clearances at the same level as ASIO officers, empowered to review all aspects of protection visa decisions that rely partly or wholly on grounds presently reviewable only by the AAT[cdxxvii] and also empowered to review ASIO security assessments on their merits.[cdxxviii] She acknowledges that there will be some cases where reasons of national security genuinely justify maintaining the secrecy of certain sensitive information but warns that the mere assertion of national security grounds can be conducive to the abusive invocation of such grounds. As asylum seekers need to have access to adverse material in order to have a meaningful opportunity to argue a case against visa refusal, Taylor recommends that:

> upon review, the member of the RRT specialised unit conducting the review should have the power to disclose information to the applicant if satisfied, in the particular case, that the interests of the applicant served by disclosure outweigh the national security interest served by non-disclosure.[cdxxix]

11.14 Section 501(3) of the *Migration Act 1958* (Cth) gives the Minister the power to refuse or cancel a visa on character grounds if the Minister is satisfied that it is in the national interest to do so. This power can be used to refuse a protection visa to a person suspected of presenting a national security risk. The power only can be exercised by the Minister personally.[cdxxx] A decision made by the Minister is not reviewable by the RRT nor the AAT, although limited review is available in the courts.[cdxxxi]

Question 69. What procedures currently apply in Australia with respect to the making and review of security assessments in immigration, passport and similar hearings to protect classified and security sensitive information in such proceedings? Are they effective? Are they fair? What safeguards are in place or should be implemented?

Question 70. Should review tribunals such as the Migration Review Tribunal, Refugee Review Tribunal and Administrative Appeals Tribunal have specialist units within them staffed by officers with security clearances at the same level as ASIO or other intelligence officers, who are able to review all aspects of security assessments?

United Kingdom

11.15 On 1 April 2003, new powers came into effect in the UK allowing the government to strip immigrants holding dual nationality of British citizenship if they have done anything 'seriously prejudicial' to the 'vital interests of the United Kingdom or a British overseas territory'.[cdxxxii] A person who is given notice of a decision to deprive him or her of citizenship may appeal against the decision to an adjudicator appointed under the Act unless the Secretary of State certifies that the decision was taken

> wholly or partly in reliance on information which in his opinion should not be made public
>
> (a) in the interests of national security,
>
> (b) in the interests of the relationship between the United Kingdom and another country, or
>
> (c) otherwise in the public interest.[cdxxxiii]

11.16 In April 2003, Britain revoked the citizenship of Muslim cleric Abu Hamza al-Masri, who is said to have 'applauded' the attacks on the World Trade Centre and Pentagon. Al-Masri was the first person targeted under the new powers.[cdxxxiv] Home Secretary David Blunkett stated:

> We are not starting a kind of hunt round for people … who don't warrant it. I want to deal with people who our intelligence and security services believe are a risk to us.[cdxxxv]

11.17 Al-Masri's lawyer said that her client would resist the matter on the ground that removal of nationality breached European protocols on human rights. A director of Liberty, a leading civil rights group, stated:

> Any decision to strip someone of citizenship should be for a court, based on evidence of treason or similarly serious offences.[cdxxxvi]

11.18 The Special Immigration Appeals Commission (SIAC) was set up by the *Special Immigration Appeals Act 1997* (UK). This Act followed the ruling by the European Court of Human Rights against the British government in *Chalal v The United Kingdom*.[cdxxxvii] The European Court ruled that the procedures in place in the UK at the time for removing people whose presence was deemed not to be conducive to the public good because of national security reasons, relations with another country or any other political reason, contravened the European Convention on Human Rights. The previous system, known as 'the three wise men', involved a non-judicial panel that reviewed the decisions of the Home Secretary to remove people on the ground that their presence was not conducive to the public good. There was no right to be present to hear evidence adduced by the authorities (for example, Security Service officers), to be told of it or to cross-examine. The panel was enjoined to remember that the evidence had not been subject to cross-examination. Legal representation was excluded.[cdxxxviii] Leigh has criticised the procedures before the now defunct panel:

> They clearly lack the safeguards associated with processes whose possible outcome is so serious: specific notice of allegations, legal representation, and cross-examination. [The argument that decisions involving national security are non-justiciable] does not justify the refusal to allow intelligence information in individual cases to be tested by cross-examination. Issues of accuracy, potential bias and self-interest of informers, and alternative interpretations of the facts, could all be dealt with without calling into question the policy underlying the decision contested. … The real challenge is to devise legal procedures which preserve executive responsibility and protect confidentiality but also allow rigorous testing of the case on the appellant's behalf. It is here that an examination of possible alternative procedures is pertinent.[cdxxxix]

11.19 As noted in Chapter 5, the *Special Immigration Appeals Commission Act 1997* (UK) provides for rules to be made enabling SIAC to hold proceedings in the absence of any person, including appellants and any legal representatives appointed by them.[cdxl] The relevant law officer may appoint a person to represent the interests of an appellant in any proceedings from which the appellant and his or her lawyer are excluded.[cdxli] An appointed lawyer is not responsible to the person whose interests he or she is appointed to represent.[cdxlii]

> The Special Advocate is appointed from a list of … cleared counsel by the Attorney General's office. He is permitted to see all the closed evidence, but once he has seen this material he is not allowed to have any contact with the appellant.[cdxliii]

11.20 The *Anti-Terrorism, Crime and Security Act 2001* (UK) allows the detention of those whom the Secretary of State has certified as threats to national security and who are suspected of being international terrorists where their removal is not presently possible.[cdxliv] Detention is subject to regular independent review by SIAC. The Act is also intended to 'speed up the asylum claims for suspected terrorists. The Act excludes substantive consideration of asylum claims where the Secretary of State certifies their removal would be conducive to the public good'.[cdxlv]

United States of America

11.21 In the US, classified information is generally used against 'aliens' in three situations:[cdxlvi]

- in a special removal process to prevent the admission at the border of an alien believed to be a terrorist;[cdxlvii]
- to deny discretionary relief from deportation;[cdxlviii] and
- where aliens may be detained pending the final resolution of their immigration proceedings based on classified information.

11.22 The US Department of Justice broke with a long-established practice of open immigration hearings when it closed immigration proceedings for people detained by the US Immigration and Naturalization Service (INS) after 11 September 2001.[cdxlix] On 21 September 2001, Judge Michael Creppy, the Chief Immigration Judge in the United

States, pursuant to a direction by the US Attorney General, issued a memorandum to all immigration judges[cdl] advising of additional security procedures for certain cases in the immigration court required by the US Department of Justice. These procedures include the following features:

> 1) Because some of these cases may ultimately involve classified evidence, the cases are to be assigned only to judges who currently hold at least a security clearance; …
>
> 3) Each of these cases is to be heard separately from all other cases on the docket. The courtroom must be closed for these cases—no visitors, no family, and no press.
>
> 4) The Record of Proceeding is not to be released to anyone except an attorney … (assuming the file does not contain classified information).
>
> 5) The restriction on information includes confirming or denying whether such a case is on the docket or scheduled for a hearing. …[cdli]

11.23 Judge Creppy also ordered that special cases should not be posted on court calendars outside courtrooms and should be excluded from information provided on the Court's telephone information service.

11.24 Human Rights Watch has criticised the breadth of the directives in Judge Creppy's memorandum, arguing that:

> Immigration hearings should be presumptively open. If the government seeks to have an immigration hearing closed, it should present particularized justification that shows the need to conduct all or part of the proceedings in an individual case in secret for reasons of national security or to protect classified information. The final decision to close a hearing should be made by an immigration judge on a case-by-case basis. The INS should not assert a detainee's privacy or other individual interests as a basis for closing a hearing to the public unless the detainee has requested the hearings be closed for that reason.[cdlii]

11.25 A three-judge panel of the US Court of Appeals (6th Circuit) held Judge Creppy's directive to be an infringement of the First Amendment right of access.[cdliii] The Court of Appeals held that there was a First Amendment right of access to deportation proceedings[cdliv] and that curtailment of that right to protect the disclosure of sensitive information only could be justified where closing the court directly serves a compelling government interest and is narrowly tailored to achieve that end.[cdlv] Further, the interest is to be articulated and accompanied by findings specific enough to allow a reviewing court to determine whether the closure order was properly made.[cdlvi] The Court of Appeals found that, while the government's ongoing anti-terrorism investigation provided a compelling interest, Judge Creppy's directive was not narrowly tailored[cdlvii] and did not require particularised findings.[cdlviii] Judge Keith stated:

> The Executive Government seeks to uproot people's lives, outside the public eye and behind a closed door. Democracies die behind closed doors. The First Amendment, through a free press, protects the people's right to know that their government acts

> fairly, lawfully and accurately in deportation proceedings. When government begins closing doors, it selectively controls information rightfully belonging to the people. Selective information is misinformation.[cdlix]

11.26 The Court of Appeals identified the following values of open proceedings:[cdlx]

1. Public access acts as a check on the actions of the Executive by assuring us that proceedings are conducted fairly and properly.

2. Openness ensures that government does its job properly; that it does not make mistakes.

3. After the devastation of September 11 and the massive investigation that followed, the cathartic effect of open deportations cannot be overstated. They serve a 'therapeutic' purpose as outlets for 'community concern, hostility and emotion'.[cdlxi]

4. Openness enhances the perception of integrity and fairness.

5. Public access helps ensure that 'the individual citizen can effectively participate in and contribute to our republican system of self-government'.

11.27 However, the decision of the US Court of Appeals for the 3rd Circuit in *North Jersey Media Group v John Ashcroft*[cdlxii] is at odds with the decision of the 6th Circuit. The 3rd Circuit held that the press and public possess no First Amendment right of access to deportation proceedings and that the Attorney General had a right to close deportation hearings determined by him to present significant national security concerns:

> We are keenly aware of the dangers presented by deference to the executive branch when constitutional liberties are at stake, especially in times of national crisis, when those liberties are likely in greatest jeopardy. On balance, … we are unable to conclude that openness plays a positive role in special interest deportation hearings at a time when our nation is faced with threats of such profound and unknown dimension.[cdlxiii]

11.28 On 27 May 2003, the US Supreme Court declined to review the decision of the 3rd Circuit Court of Appeals, leaving undisturbed the decision which upholds the US government's right to conduct secret immigration hearings. However, outside the 3rd Circuit, the law on the legality of the Creppy directive remains unsettled.[cdlxiv]

Immigration and criminal proceedings compared

11.29 As noted in Chapter 5, some minimum procedural protections guaranteed by international law apply exclusively to criminal proceedings. In *Detroit Free Press v John Ashcroft*,[cdlxv] the US Court of Appeals for the 6th Circuit made a number of observations comparing the severity of the outcomes of deportation proceedings with criminal proceedings:

> A deportation proceeding, although administrative, is an adversarial, adjudicative process, designed to expel non-citizens from this country. '[T]he ultimate individual

stake in these proceedings is the same or greater than in criminal or civil actions'. *See N. Media Jersey Media Group, Inc. v Ashcroft*, 205 F.Supp 2d 288, 301 (DNJ2002). '[D]eportation can be the equivalent of banishment or exile,' *Delgadillo v Carmichal*, 332 US 388, 391 (1947), and the Court has taken note of the 'drastic deprivations that may follow when a resident of this country is compelled by our [g]overnment to forsake all the bonds formed here and go to a foreign land where he often [may] have no contemporary identification'. *Woodby v INS*, 385 US 267, 285 (1966). Moreover, '[t]hough deportation is not technically a criminal proceeding, it visits a great hardship on the individual and deprives him of the right to stay and live and work in this land of freedom'. *Bridges*, 326 US at 154. As such, '[t]hat deportation is a penalty—at times a most serious one—cannot be doubted. *Id* at 154.

11.30 In light of the serious consequences that flow from deportation and other similar proceedings, the question arises about what minimum protections should extend to persons facing these types of hearings. This issue is especially pertinent to the use of secret evidence in immigration matters, where the government may seek to lead such evidence in order to protect classified or security sensitive information. The observations in Chapter 5 relating to secret hearings and secret evidence are also relevant to immigration hearings.

Question 71. Should the protections afforded to accused people in criminal trials involving classified or security sensitive information—including the right to be tried in their presence, to defend themselves personally or through legal assistance of their choosing, and to examine the witnesses against them—extend to people facing all, or particular, types of immigration and similar hearings involving such information?

Question 72. If leading secret evidence to protect classified or security sensitive information is appropriate for all, or some, types of immigration and similar matters, what safeguards should be imposed on its use?

12. Parliamentary Committees, Tribunals and Specialist Courts

Parliamentary committees

12.1 Parliamentary committees serve an important function in the scrutiny of government activities. Section 49 of the *Australian Constitution* empowers both Houses of Parliament to require the attendance of witnesses to committees, and the giving of evidence and the production of documents required for the purpose of inquiring into government administration and public affairs.[cdlxvi]

12.2 As in court proceedings, where the government may not wish to present evidence because it would not be in the public interest, it may make a claim for public interest immunity in order to avoid complying with a request from a parliamentary committee.

12.3 *Odgers' Australian Senate Practice* notes that most committees are empowered to hear evidence in public or private.[cdlxvii] Estimates committees, however, must hear all evidence in public and cannot withhold matters considered by them from publication. Under s 13 of the *Parliamentary Privileges Act 1997* (Cth), it is an offence to publish or disclose, without the authority of a House or committee, a confidential submission, oral evidence taken in camera or a report of such evidence.[cdlxviii]

12.4 Before giving evidence, a witness must be offered the opportunity to have his or her evidence heard in camera. The witness will be asked for supporting reasons; this hearing may also take place in public or private. If a witness is not granted the opportunity to be heard in camera, reasons must be given for this decision.[cdlxix] Other protections may also be extended to witnesses, such as not publishing names in transcripts of evidence, or in reports.[cdlxx]

12.5 Parliament is a political arena and Evans notes a substantial difference in the way public interest immunity is dealt with in the Senate compared with the courts. Most importantly, the Senate passed a resolution in 1975[cdlxxi] asserting its right to examine claims of public interest immunity made before the Senate and its committees, and to determine whether material must be provided.[cdlxxii] However, Evans also notes that the Senate has not attempted to enforce demands for evidence or documents against a ministerial refusal to provide them.[cdlxxiii]

12.6 Evans notes that governments do not always comply with demands made by the Senate in this regard.[cdlxxiv] In the period 1998–2001, 56 orders for documents were made, with 15 refusals by the government.[cdlxxv]

12.7 Evans notes that the Senate has not resorted to any particular sanction for refusal to comply with an order to produce documents to allow assessment of public interest

immunity.[cdlxxvi] In many cases, the publicity attracted by the refusal to produce documents has had a significant effect. Evans suggests that other drastic measures, such as blocking legislation or preventing ministers from operating in the Senate, could be applied if a crisis were reached.[cdlxxvii]

12.8 Senate committees have considered the issue of developing procedures or criteria for determining whether a claim for public interest immunity should be granted, but the political nature of the issue has failed to lead to any resolution.[cdlxxviii]

> There appears to be a consensus that the struggle between the two principles involved, the executive's claim for confidentiality and the Parliament's right to know, must be resolved politically. In practice this means that whether, in any particular case, a government will release information which it would rather keep confidential depends on its political judgment as to whether disclosure of the information will be politically more damaging than not disclosing it, the latter course perhaps involving difficulty in the Senate or public disapprobation.[cdlxxix]

12.9 The Commonwealth Legislative Counsel has produced guidelines for official witnesses appearing before parliamentary committees.[cdlxxx] A number of these guidelines are relevant to the current inquiry. For example, they contain checks and balances regarding the use of public interest immunity. In relation to public interest immunity the guidelines state that:

- the Attorney-General's Department should be consulted on the appropriateness of making the claim in any particular circumstances; and

- as a matter of practice, before making a claim a Minister may explore with a committee the possibility of providing the information on a confidential basis or in camera.

12.10 The matters in relation to which a claim for public interest immunity may be made under the Guidelines are similar to the exemptions in the *Freedom of Information Act 1982* (Cth), including one for material which, if disclosed, could reasonably be expected to cause damage to national security, defence or international relations. Classified documents and oral information relating to documents having a national security classification of Confidential, Secret or Top Secret would normally fall into this category. Significantly for the issue of security sensitive information, the Guidelines note that documents without a formal classification still may be subject to a public interest immunity claim (and that classified documents still may be produced).

12.11 As noted above, most parliamentary committees may hear testimony in camera.[cdlxxxi] The Guidelines envision that this would take place where the Minister believes that the information should not be released but that it is nonetheless important for the committee to view it; or where the claim for non-disclosure does not relate specifically to one of the usual exemptions but is desirable for other reasons such as preserving the secrecy attached to an aspect of law enforcement. An application to

have a matter heard in camera may arise before testimony or in the course of giving testimony.[cdlxxxii]

Question 73. The ALRC is interested in receiving comment on whether the operation of the Guidelines for official witnesses appearing before, and the practices of, parliamentary committees provide a fair and effective system for balancing the public interest in protecting classified and security sensitive information and the public interest in open government.

Investigations by the Ombudsman

12.12 Government action can also be reviewed by the Commonwealth Ombudsman. The *Ombudsman Act 1976* (Cth) grants the Ombudsman powers to compel the production of documents and information relevant to an investigation under the Act.[cdlxxxiii] A range of national security-related decisions can be reviewed by the Ombudsman, including:

- departmental advice to a Minister on deportations;
- advice to a Minister not to grant citizenship;
- delays in advising a Minister to issue a passport; and
- actions of the Australian Federal Police in maintaining police files on a person.[cdlxxxiv]

12.13 The Ombudsman has extensive powers to compel the production of information in the course of an investigation. Section 9 of the Act allows the Ombudsman to require the production of any documents or furnishing of any information by any person, and to compel any person to answer questions relevant to an investigation. This information is not given directly to the complainant, but could become available as part of the 'particulars of an investigation', which the Ombudsman is required to provide at the end of an investigation.[cdlxxxv]

12.14 However, as in the case of an FOI exemption,[cdlxxxvi] the Act also allows the Attorney-General to issue a certificate stating that the 'disclosure would be contrary to the public interest if it would prejudice the security, defence or international relations of Australia'.[cdlxxxvii] Under the *Ombudsman Act*, this certificate removes the obligation to produce documents, furnish information and to answer questions. It also prevents disclosure of the relevant information to the complainant.[cdlxxxviii] Hanks, Lee and Morabito suggest that the issuing of a certificate could be open to administrative or judicial review, but argue that such an attempt would suffer a number of serious difficulties—a major one being that any attempt to review the Attorney-General's

statement of reasons could itself be subject to a claim that disclosure of the reasons would prejudice security.[cdlxxxix]

Question 74. The ALRC is interested in receiving comment on the issuing of Attorney-General's certificates under the *Ombudsman Act 1976* (Cth). Do they balance the public interest in protecting classified and security sensitive information and the public interest in open government?

Royal Commissions

12.15 Royal commissions are not formally bound by the same requirements of openness as courts or tribunals.[cdxc] They are not bound by the rules of evidence and can inspect any documents and call any witnesses they think fit.[cdxci] However, the doctrine of public interest immunity would seem to apply to inquiries and commissions as it does to court proceedings:

> The fact that the public interest requires certain documents to be withheld from forensic scrutiny and the secondary evidence of those documents must also be withheld in the public interest indicates the whole doctrine of public interest immunity would be rendered nugatory if it were not also to apply to non-judicial forums. The rationale of public interest immunity applies with no less force to tribunals and other bodies outside the ordinary court system.[cdxcii]

12.16 In relation to public interest immunity, Carmody makes the point that it would be hard to sustain an argument that the state should be powerless to protect information in an inquiry it has itself established. On the other hand, the state should not lightly deprive its own fact-finding body of documents and information that it requires in order to report properly.[cdxciii]

Question 75. Should the principles applied by courts and tribunals in determining how to handle classified and security sensitive information be modified in relation to royal commissions?

Specialist courts

12.17 Classified and security sensitive information is a recurrent feature of proceedings that involve military and intelligence personnel or those employed by specialist agencies, some of which are heard in specialist courts or tribunals. These specialist courts may have quite different rules regarding open hearings, presentation of evidence and the rights of defendants appearing before them.

12.18 No such specialist bodies are in general use in Australia. However, two bodies are routinely required to consider sensitive information: the Security Appeals Division

of the Administrative Appeals Tribunal (AAT) and royal commissions. Private investigations of the conduct of intelligence agencies also may be undertaken by the Inspector-General of Intelligence and Security.

Security Appeals Division of the AAT

12.19 The Security Appeals Division of the AAT can hear two types of matters:

- applications for review of a qualified or negative security assessment made by ASIO under s 54 of the ASIO Act; and

- applications under the *Archives Act* for access or partial access to an ASIO record held by the Australian Archives.[cdxciv]

12.20 The AAT cannot review security assessments conducted by other agencies.[cdxcv] In some cases, ASIO will conduct the investigation and another agency will issue the security assessment.[cdxcvi] In 2001–02, the Security Appeals Division received one application for access to ASIO records, and eight regarding security assessments.[cdxcvii]

12.21 In relation to reviews of security assessments, the AAT conducts a private hearing of the evidence and makes its findings in relation to the assessment, and the correctness of, or justification for, any opinion, advice or information contained in the assessment.[cdxcviii] Copies of the AAT's findings are provided to the applicant, the Director-General of ASIO, the Commonwealth agency to which the assessment was given and the Attorney-General. At various stages of the process, the Attorney-General and the Director-General of Security (the head of ASIO) have the power to issue certificates to exempt another agency from providing notice of an ASIO decision to an applicant or to prevent an applicant hearing submissions on the basis of public interest.[cdxcix]

12.22 A person may not always be aware that an adverse assessment has been made against him or her. Section 38(1) of the ASIO Act provides that, where an adverse security assessment is made against a person, the person must be informed within 14 days. However, the Attorney-General may issue a certificate to withhold the notice of making a security assessment where that withholding is essential for the security of the nation.[d]

12.23 On receiving notice of appeal, the Director-General of Security is required to present all material relevant to the assessment, favourable or unfavourable, to the AAT.[di] Where the Attorney-General has issued a certificate under s 38 of the ASIO Act, a copy of the certificate must be sent to the AAT. If the Attorney-General certifies that the submissions proposed to be made by the Director-General of Security are of such a nature that their disclosure would be contrary to the public interest because it would prejudice security or the defence of Australia, the applicant (and generally the applicant's legal representative) cannot be present when the evidence is adduced.[dii] The

Attorney-General also may prevent information about the reasons for the assessment being given to the person because of national security implications.[diii]

Question 76. Do the evidentiary or other procedures applied in the Security Appeals Division of the Administrative Appeals Tribunal with regard to classified and security sensitive information present any special issues peculiar to these proceedings?

Inspector-General of Intelligence and Security

12.24 Section 8 of the *Inspector-General of Intelligence and Security Act 1986* (Cth) (IGIS Act) allows the Inspector-General to undertake inquiries, at the request of a Minister or at the Inspector-General's own behest, into a number of matters relating to the operations of Australian intelligence agencies including:

- the compliance by that agency with the laws of the Commonwealth, the States and Territories;
- the compliance by that agency with directions or guidelines given to it by the responsible Minister;
- the propriety of particular activities of an intelligence agency;
- the effectiveness and appropriateness of the procedures of that agency relating to the legality or propriety of its activities; and
- the collection and communication of intelligence concerning particular individuals.[div]

12.25 Under s 17(1) of the IGIS Act, inquiries must be conducted in private and in such manner as the Inspector-General thinks fit, although unclassified versions of reports made to ministers may be released or discussed in annual reports. The IGIS has powers to obtain information, to require persons to answer questions and produce documents, to take sworn evidence and to enter agency premises.[dv] Under s 20 of the Act, the Inspector-General may obtain documents with a national security classification for the purposes of an inquiry where required but must make arrangements with the head of the agency for the protection of those documents while they remain in the Inspector-General's possession and for their return.

Military tribunals and courts martial

12.26 In Australia, military tribunals and courts are used to administer military justice in relation to defence personnel. The Commonwealth is given power to legislate in respect of military justice under s 51(vi) of the *Constitution*.[dvi] The *Defence Force*

Discipline Act 1982 (Cth) establishes the range of service offences, penalties and the service tribunals which try offences under the Act. Under Part VII of the Act, a service person may be tried by a summary authority,[dvii] a Defence Force magistrate[dviii] or a court martial.[dix] A Judge Advocate-General, who is a civilian judge of the Federal Court of Australia or State Supreme Courts, oversees the hearing of charges and appoints military officers in discharging functions.[dx]

12.27 A general court martial is composed of a President and at least four other members; a restricted court martial has a President and at least two other members.[dxi] Service personnel ranking higher than the accused are eligible to be members of the court; the President may be appointed from the most senior ranks of the forces.[dxii]

12.28 A judge advocate (who is appointed from a panel of judge advocates) sits on the court martial and instructs in matters of law and procedure.[dxiii] However, it is the President and members of the court martial who make the finding of guilt and other questions of fact, on the basis of a majority vote.[dxiv]

12.29 Courts martial and Defence Force Magistrate proceedings are public, but may be closed or unreported 'if the President or Defence Force Magistrate considers it necessary in the interests of the security or defence of Australia, the proper administration of justice or public morals'.[dxv]

12.30 The *Defence Force Discipline Act* allows for administrative review of disciplinary decisions by defence force officers.[dxvi] Decisions also may be reviewed by the Defence Force Appeals Tribunal (an arm of the Federal Court) and then by the Full Federal Court and the High Court.[dxvii] The review powers of the Defence Force Appeals Tribunal are similar to those of a civilian criminal court of appeal, with the ability to quash a verdict and order a re-trial, although there is also a power to substitute a correct charge.[dxviii]

12.31 The *Defence Force Discipline Act* adopts many of the principles of criminal law; for example, the burden of proof falls on the prosecution.[dxix] Chapter 2 of the Commonwealth *Criminal Code*, which sets out the principles of criminal responsibility, applies to the *Defence Force Discipline Act* by virtue of s 10 of that Act. An accused person has the right to be represented in the investigation process and during any proceedings under the Act.[dxx]

United States of America

Foreign Intelligence Surveillance Court (US)

12.32 The Foreign Intelligence Surveillance Court (FISC) was established in 1978, under the *Foreign Intelligence Surveillance Act* (US) (FISA). The Act establishes a legal regime for foreign intelligence surveillance separate from ordinary law enforcement surveillance rules.

12.33 The FISC is composed of seven Federal District Court judges appointed for staggered terms from different circuits. The US Attorney General applies to the Court for authorisation of electronic surveillance (such as wiretapping) within the US aimed at obtaining foreign intelligence information. These applications are reviewed by a single judge of the Court. The proceedings are conducted without the knowledge or presence of the other party and decisions are based on the evidence presented by the Department of Justice.[dxxi]

12.34 Criticisms made of the secret proceedings of the FISC include that:

- the records and files of the cases are sealed and may not be revealed, even to persons whose prosecutions are based on evidence obtained under warrants authorised under the FISA, except to a limited degree;

- there is no provision for the return of each executed warrant to the FISC, and no inventory of items taken; and

- there is no provision for certification that the surveillance was conducted according to the warrant.[dxxii]

12.35 In 2002, the FISA Review Court[dxxiii]—consisting of three federal appellate judges—made its first ruling, overturning a decision of the FISC to limit the government's bid for expanded surveillance powers. In a normal criminal case, the government must meet the 'probable cause' standard (a Fourth Amendment right) to obtain a wiretap on a suspect,[dxxiv] meaning that the government must show probable cause that an individual is committing, is about to commit or has committed a crime.[dxxv] The FISA Review Court held that a new, lowered standard for gaining a warrant—that probable cause is made out simply by the belief that 'the target of the electronic surveillance is a foreign power or the agent of a foreign power'—does not violate the Fourth Amendment protections given the important government interest in national security.[dxxvi] In March 2003, the US Supreme Court rejected a challenge to that ruling by the American Civil Liberties Union.[dxxvii]

Alien Terrorist Removal Court (US)

12.36 The Alien Terrorist Removal Court (ATRC), was established in 1996,[dxxviii] modelled on the special court created by the *Foreign Intelligence Surveillance Act* (discussed above). The ATRC's decisions can be appealed to the US Court of Appeals for the District of Columbia. The ATRC operates under special procedures which allow the removal of non-citizens who the government believes are terrorists, even if they are not in violation of any immigration laws. The ATRC has never been used, but there have been a number of criticisms about its design.

12.37 In establishing the ATRC, the US government asserted a need to protect national security in sensitive cases seeking the deportation of suspected non-citizen

terrorists.[dxxix] However, the normal court requirement to produce evidence could expose and endanger intelligence sources.[dxxx]

12.38 The ATRC works in the same way as the FISC: the Justice Department presents its case in secret to a judge, who may then authorise the Justice Department to commence deportation proceedings in a District Court. In the District Court proceedings, the defendant will see only a summary of the evidence that has been presented. The District Court then determines whether a case for deportation is made out.[dxxxi] The summary of the classified evidence which is presented to the defendant must be sufficient to enable the defendant to mount a defence.[dxxxii]

12.39 It has been suggested that this last requirement may prove to be problematic. The US Justice Department has claimed that if it prepares a summary for the defence that is too vague, it will not be approved by the judges. However, any greater detail defeats the purpose of having the evidence presented in secret.[dxxxiii] An attempt was made in 2001 to remove the requirement for a summary to be presented to the defendant by a proposed amendment to the USA PATRIOT Act. However, this was defeated in the Senate.[dxxxiv]

Military Commissions (US)

12.40 On 13 November 2001, US President Bush signed a Military Order that suspected terrorists could be tried in military commissions rather than civilian criminal courts. The Order directed the US Secretary of Defense to create military commissions and to take into custody anyone named by the President as subject to that Order.[dxxxv] The Order allows the commission to sit at any time and any place, inside or outside the United States. The Secretary of Defense is able to issue regulations setting out procedural protections.[dxxxvi] However, the Order also authorises the commissions to operate in secret, with no threshold requirement to show that secrecy is necessary.[dxxxvii]

12.41 The Department of Defense indicated in May 2003 that certain individuals had been identified for prosecution in the military commissions, although no action would be taken until they are formally named by the President.[dxxxviii] The Department has publicly released legal instructions on the operation of the commissions. For example, the Instruction on 'Qualification of Civilian Defense Counsel' states that defence counsel must be eligible for classification at level 'Secret' or higher, or must apply to be so authorised.[dxxxix] Military Commission Instruction No 7 notes that any punishment may be authorised by the commissions, including the death penalty.[dxl]

12.42 Military commissions or tribunals have a chequered history in the United States. Following World War II, the US Supreme Court upheld the use of military commissions to try Nazi saboteurs. However, this decision was subject to criticism.[dxli] Koh argues that 'on its face, the Order authorizes the Department of Defense to dispense with the basic procedural guarantees required by the Bill of Rights, the International Covenant on Civil and Political Rights, and the Third Geneva Convention of 1949'.[dxlii]

> Fundamentally, the Military Order undermines the constitutional principle of separation of powers. For under the order, the President directs his subordinates to create military commissions, determine who shall be tried before them and choose finders of fact, law and guilt. However detailed its rules and procedures may be, a military commission is not an independent court, and its commissioners are not genuinely independent decision makers.[dxliii]

Question 77. Does the protection of classified and security sensitive information require Australia to consider creating or adapting specialist tribunals or military commissions such as those in the United States of America?

13. Security Clearances

13.1 A key issue in this inquiry is whether individuals who are to gain access to classified or security sensitive information during investigations and proceedings should be required to obtain a security clearance, and the extent of any such clearance. This issue has been enlivened by the government's recent proposed changes to legal aid guidelines and the regime governing cases involving classified and security sensitive information generally, which are discussed below.

Protective Security Manual

13.2 Part D of the Commonwealth Protective Security Manual (PSM) outlines the Commonwealth's minimum standards and procedures for granting and maintaining a personnel security clearance. The personnel security clearance system is aimed primarily at Commonwealth employees, although it can be applied to contractors and others who need access to classified information or areas.[dxliv] The Commonwealth expects that the number of people who need to be security cleared to perform their work will be kept to a minimum.[dxlv]

13.3 The PSM acknowledges that the clearance process is discriminatory and intrusive.[dxlvi] It entails a thorough evaluation of the requirements of a specific position to ascertain the level of clearance necessary, and requires the clearance, once issued, to be monitored and periodically reviewed.[dxlvii] Among the principles identified in the PSM relating to personnel security are the following:

- Security clearances should only be required where the need for access to security classified information has been clearly established.[dxlviii]
- Only people with the appropriate security clearance and a legitimate need to know may access security classified information or areas.[dxlix]
- The procedures used to process and issue a security clearance for a person to access security classified information should be uniform.[dl]

13.4 The Commonwealth's clearance system is based on negative vetting—which aims to identify anything in the subject's background or lifestyle likely to pose a security risk—as opposed to positive vetting—which entails an extensive examination into the subject's life until suitability for clearance has been established beyond reasonable doubt.[dli]

Review of security clearance decisions

13.5 National security assessments for Designated Security Assessments Positions that need clearances to information classified as Top Secret, Secret or Confidential require an ASIO security assessment. Individuals have the right to have any qualified

or adverse assessment by ASIO reviewed by the Security Appeals Division of the Administrative Appeals Tribunal.[dlii] The AAT may affirm, vary or set aside ASIO's security assessment and substitute its own assessment, or remit the matter to ASIO for reconsideration.[dliii]

Security clearance of lawyers

Legal Aid changes

13.6 Under changes proposed by the federal government in January 2003:

> In any matter relating to Australia's national security, legal assistance may be granted to engage legal representatives only if the representatives hold, or obtain before the grant is made, security clearances at the appropriate level.[dliv]

13.7 If these proposals were put into effect, lawyers would be unable to access classified documents without a security clearance.

> The Commonwealth is currently looking at options for addressing the absence of a statutory power to require the defence in national security cases to obtain appropriate security clearances. In the interim, it is appropriate that the Commonwealth takes all steps necessary to ensure that legally aided persons can be properly defended.[dlv]

13.8 The government's changes attracted criticism from lawyers and civil liberties groups, in particular because the proposed rules are contrary to an important principle covering the provision of Legal Aid—namely, that its recipients are treated in exactly the same manner, in terms of their legal representation, as clients who pay for their own lawyers.[dlvi] The ALRC understands that the government's intention was never to distinguish legal aid lawyers from other lawyers—the government's proposals ultimately extended to all lawyers participating in cases involving classified or security sensitive information.[dlvii]

13.9 The proposals also raise issues about the role of executive government, through ASIO, in deciding who represents defendants in national security cases. The CEO of the Law Council of Australia and former federal Attorney-General, Michael Lavarch, has said:

> It would be very disturbing if a person was denied the ability to choose their own representative and rather, the state imposed one.[dlviii]

13.10 Lavarch has argued instead that, if a particular lawyer represented cause for concern in relation to their handling of classified information, the matter should be brought before a judge, who could impose the appropriate restrictions.[dlix]

13.11 The NSW Law Society's Criminal Law Committee has opposed the changes on the basis that

> the security of any classified documents can be sufficiently assured by the court and by practitioners observing their professional obligations as officers of the court.

> Further, it would impose an arbitrary and unacceptable limitation on the right of people to be represented by the lawyer of their choice.[dlx]

13.12 The President of the NSW Council for Civil Liberties has argued that the rules could lead to lawyers not acting in the best interests of their clients if 'fully representing' them meant they could have their security clearance withdrawn:

> They'd be worried that hanging over their head is their security rating and their ability to perform that work in the future.[dlxi]

13.13 The federal Opposition has stated that issues about access to classified documents are evidentiary ones, which historically have been resolved by courts and tribunals.[dlxii]

13.14 The Attorneys-General of Victoria, NSW, South Australia and Queensland have opposed the federal government's proposed changes, with the strong backing of the Victorian and NSW Bar Associations.[dlxiii]

13.15 As discussed in Chapter 5, the Victorian Bar has submitted that the federal government's proposals appear to ignore procedures developed by the courts to ensure confidentiality of sensitive or privileged material, including the giving of undertakings, the taking of evidence in camera and the making of orders in relation to the publication of information. The Victorian Bar argues that there has been no suggestion that these procedures are not working. It also argues that there is no parallel between independent legal practitioners, who are officers of the court, and public servants employed by the executive government who are required to obtain security clearances. The Victorian Bar submitted:

> The practical implications and difficulties in the asserted policy and proposed guidelines are immense. It seems to be assumed that national security implications will be apparent at the outset of legal proceedings. That is not the reality. It may be that only in cross-examination at committal or at trial that a document will emerge raising national security. Solicitors and counsel will have done substantial work and be fully engaged in the defence. They may be unwilling or unable to obtain the appropriate security clearance, or be able to do so in a timely fashion. Even the proposed exception for urgent matters applies only where 'access to information relating to national security is not required for the proper conduct of the applicant's case'. That may not be ascertainable at the time the referral needs to be made.[dlxiv]

13.16 The Victorian Bar queried whether the Commonwealth would fund security clearances of a pool of lawyers in advance, and if so, queried the number and mix of seniority of lawyers who would be cleared in advance.[dlxv]

13.17 The NSW Bar Association criticised the government's proposal as 'unprincipled, impractical and discriminatory'. It did, however, agree that in certain cases for specific matters it may be appropriate for lawyers and others involved in the case to hold a specific security clearance. It noted that the Commonwealth had not

defined ‘matters relating to Australia’s national security’, which, it suggested, is a wide-ranging, imprecise expression.

> Is the Commonwealth seeking to impose the clearance requirement only in matters arising under the recent tranche of ‘national security’ legislation—or that and the *Crimes Act 1914*, *ASIO Act 1979* and related legislation—or in any matter that some Commonwealth minister or bureaucrat claims involve ‘national security’?[dlxvi]

13.18 The NSW Bar Association queried whether other participants in court hearings also would be required to hold a clearance, noting that, if they were not, the implication arose that lawyers posed a greater threat to national security. It also noted that, if lawyers were to seek clearance in advance of actual need, it was unclear what level of clearance they should be seeking.

13.19 The NSW Bar Association also noted the time lags involved in obtaining security clearances—for higher level clearances, this usually takes months, and for some clearances it can take more than a year.[dlxvii] The NSW Bar Association concluded:

> In practice, if legal practitioners need to have a security clearance … before they can have access to the prosecution’s case, there can be no legal representation of choice by the accused. A person appearing before a magistrate after arrest will either [sic] have to be represented by practitioners who already have a security clearance (at the moment probably who do regular work for the Commonwealth, in particular for defence and security agencies). It is unlikely practitioners with clearances will be readily available to appear in a magistrates court when bail is sought.[dlxviii]

Wider changes

13.20 The government’s proposals concerning the security clearances of lawyers have been extended beyond legal aid lawyers. In signing the Terms of Reference for this inquiry, the Attorney-General announced that new measures had been designed ‘to overcome the procedural and evidentiary problems associated with prosecuting criminal offences involving sensitive or classified material’ including ‘requiring legal representatives who require access to the information to be security cleared at the appropriate level’.[dlxix]

13.21 An early version of the Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002 [No 2] (ASIO Bill), which was not passed, provided for ‘approved lawyers’; ie, legal practitioners whom the Minister had approved and in respect of whom he or she had considered a security assessment.[dlxx] Persons detained under a warrant[dlxxi] were to have the right to contact an approved lawyer unless exceptional circumstances existed to delay that right for up to 48 hours (for example, if the Minister was satisfied that it was likely that a terrorism offence was being committed).[dlxxii] On 11 June 2003, the government proposed changes to the ASIO Bill relating to access to a lawyer:

> The current regime would be replaced with a scheme that provides for the provision of a lawyer of choice, with a range of safeguards to protect the disclosure of sensitive information. Under this proposal the lawyer would not have to hold a security

> clearance. However, under this proposal, the Bill will provide for the making of regulations which may prohibit or regulate access to information which is controlled on security grounds. As the lawyer would not have access to classified information there would be no requirement that they be security cleared.[dlxxiii]

13.22 This proposal also allows ASIO to apply to the prescribed authority to prevent access by the subject of a warrant to his or her lawyer of choice. The prescribed authority can deny a person access to his or her lawyer of choice where it is satisfied that allowing access may alert a person involved in a terrorism offence to the investigation or may result in the damage or destruction of things that may be required to be produced under the warrant.[dlxxiv] This proposal was retained in the final version of the Bill that was passed by Parliament on 25 June 2003.[dlxxv]

13.23 The question arises whether there should be different mechanisms or procedures for clearing lawyers depending on the circumstances of a case. For example, had the ASIO Bill referred to above been passed in its earlier form, should the vetting procedure for 'approved lawyers' acting for persons who had been detained under warrant have been the same as, or more stringent than, any proposed vetting procedure for lawyers acting in any matter, whether criminal, civil or administrative, involving classified or security sensitive information? Proposed clause 34AA of the Bill provided that:

> (1) The Minister may, by writing, approve a legal practitioner for the purposes of this Division.
>
> (2) The Minister must not approve a legal practitioner unless:
>
> (a) the practitioner is enrolled as a legal practitioner of a federal court or of the Supreme Court of a State or Territory and has been enrolled for at least 5 years; and
>
> (b) the practitioner has, by writing, consented to being approved and the consent is in force; and
>
> (c) the Minister has considered:
>
> (i) a security assessment (as defined in Part IV)[dlxxvi] in respect of the practitioner; and
>
> (ii) any other material that the Minister considers is relevant to the question whether to approve the practitioner.

13.24 Other issues for this inquiry, if lawyers are to be security cleared, are whether there should be a further requirement that they have practised for a minimum period of time before being allowed to appear in a matter involving classified or security sensitive information; and whether any particular types of case involving classified or security sensitive information would warrant more stringent vetting of lawyers.

Issues arising from the submissions

13.25 Is there any basis in principle for asserting that lawyers as a group should be exempt from security clearances to which public servants are subject if they are to get access to classified or security sensitive information? One point of distinction is that lawyers are bound by their duties as officers of the court. However, it is certainly not a novel concept to impose additional professional requirements on lawyers and other professionals in order for those professionals to carry on a particular aspect of their profession. For example, lawyers wishing to give immigration advice must be registered as migration agents. Initial applications for registration with the Migration Agents Registration Authority must supply an Australian Federal Police Criminal Check for each name by which they have been known. Lawyers who wish to hold themselves out as having specialist accreditation must meet certain criteria.[dlxxvii] Law professors who wish to be admitted to practice must meet the requirements of the relevant state or territory admission board. The need for further or special qualifications also applies to other professions. People who carry on a financial services business must hold a financial services licence, subject to some exceptions.[dlxxviii] Accountants, for example, are not exempt from the requirement to be licensed to give specific advice on superannuation.[dlxxix]

13.26 Another issue is whether the measures currently in place for admission as a solicitor or barrister are sufficient, or whether they rely too heavily on disclosures and references provided by applicants for admission rather than independent or active vetting by the relevant admission authority. For example, applicants who have never held a practising certificate in NSW must disclose in their applications for a practising certificate if they have committed certain offences and acts of bankruptcy.[dlxxx] They must also disclose whether they have been the subject of any professional disciplinary proceedings or convicted of, or charged with, an indictable offence in any jurisdiction.

13.27 In Victoria, the Legal Practice (Admission) Rules 1999 set out the qualifications for admission to the legal profession by a local applicant. One of the prerequisites is that the 'applicant is of good reputation and character and a fit and proper person to be admitted.'[dlxxxi] The Council of Legal Education or the Board of Examiners may make any inquiries it thinks fit concerning an application for admission including inquiries in relation to 'the fitness of the applicant to be admitted in Victoria.'[dlxxxii] The Legal Practice (Admission)(Amendment) Rules 2003 (Vic) came into operation on 1 March 2003. Their objective is 'to alter the requirements in relation to certification of an applicant for admission.'[dlxxxiii] The Rules provide that among the documents to be provided by local and overseas applicants for admission are 'two affidavits as to character in the form set out in Schedule 9 each made by an acceptable deponent.'[dlxxxiv]

13.28 The Standing Committee of Attorneys-General is proposing the development of a nationally consistent regulatory regime for the legal profession. A Model Bill has been prepared for the purposes of consultation, which does not necessarily reflect the views of members of the Standing Committee or any government. Part 3 of the Model Bill deals with the admission of local legal practitioners. The purpose of Part 3 is to 'provide a nationally consistent system for the admission of legal practitioners in the interests of the administration of justice and for the protection of consumers of legal

services.'[dlxxxv] Clause 309 sets out the matters that the Supreme Court or certifying body may take into account in considering whether a person is suitable for admission as a legal practitioner. These factors include:

> (a) whether the person is of good fame and character;
>
> (b) whether the person is an insolvent under administration;
>
> (c) whether the person has been convicted of an offence in Australia or a foreign country, and if so:
>
> (i) the nature of the offence; and
>
> (ii) the time that has elapsed since the offence was committed; and
>
> (iii) the person's age when the offence was committed;[dlxxxvi] …
>
> (g) whether the person
>
> (i) is the subject of current disciplinary action in another profession or occupation in Australia or a foreign country; or
>
> (ii) has been the subject of disciplinary action of that kind that has involved a finding of guilt, however expressed;
>
> (h) whether the person's name has been removed from an official roll of legal practitioners in Australia or an official roll of lawyers in a foreign country, and the person's name has not been restored; …
>
> (j) whether the person has contravened, in Australia or a foreign country, a law about trust money or a trust account;
>
> (k) whether the person is subject to an order under this Act [dlxxxvii] or a corresponding law disqualifying the person from being employed by, or a partner of, a legal practitioner or from managing a corporation that is an incorporated legal practice; …[dlxxxviii]

13.29 Clause 316 deals with the investigation of an applicant's eligibility and suitability for admission as a practitioner. It provides:

> (1) To help it consider whether or not an applicant is eligible or suitable for admission as a local legal practitioner, the certifying body may:
>
> (a) ask the applicant for any further documents or information the certifying body requires; or
>
> (b) make any investigations or inquiries it considers appropriate; or
>
> (c) refer a matter to the Supreme Court for directions.

13.30 Significantly, the notes to clause 316 state that 'the power of the certifying body to obtain police or medical reports is a matter for each jurisdiction.'

13.31 The ALRC is investigating whether the various legal practitioner admission boards of the States and Territories engage in any active vetting to ascertain whether applicants are fit and proper to enter the profession, and in particular whether those boards conduct criminal background checks of applicants to the profession, either as a matter of course, in certain circumstances only, or at all. To date, the ALRC's enquiries indicate that the various admission boards do not conduct criminal background checks of applicants.

Impact on a fair trial

13.32 An important issue arises in considering the ramifications of requiring certain lawyers to be security cleared in light of the right of an accused to receive a fair trial[dlxxxix] and to be tried without undue delay. Article 14(3)(c) of the International Covenant on Civil and Political Rights provides that an accused shall be tried without undue delay.

> This guarantee relates not only to the time by which a trial should commence, but also the time by which it should end and judgement be rendered; all stages must take place without undue delay.[dxc]

13.33 For reasons beyond his or her control an accused may be unable to obtain representation by a cleared lawyer because, for example, no cleared lawyers are available within a particular geographical location, or the lawyers the accused has approached had been refused—or refused to seek—a security clearance, or there would be undue delay associated with the lawyer's obtaining the relevant security clearance.[dxci] Where does the accused stand?

13.34 In *Dietrich v The Queen*, the majority of the High Court of Australia held that, where a trial judge is faced with an application for an adjournment or a stay by an indigent accused charged with a serious offence who, through no fault on his or her part, is unable to obtain legal representation, in the absence of exceptional circumstances the trial should be adjourned, postponed or stayed until legal representation is available.[dxcii]

> If in those circumstances, an application that the trial be delayed is refused and, by reason of the lack of representation of the accused, the resulting trial is not a fair one, any conviction of the accused must be quashed by an appellate court for the reason that there has been a miscarriage of justice in that the accused has been convicted without a fair trial.[dxciii]

13.35 The *Dietrich* principles have been strictly applied to cases where an accused charged with a serious offence is forced to go to trial without legal representation.[dxciv] They might also apply where an indigent accused charged with a serious offence involving a matter of national security is unable, through no fault of his or her own, to obtain a legally aided lawyer cleared at the appropriate level, effectively leaving the accused with no legal representation. In such cases, it would appear that the mandate of a fair trial would require the trial judge to adjourn or stay the proceedings until legal representation is available. It remains to be seen whether the *Dietrich* principle could

be extended to a non-indigent accused charged with a serious offence in circumstances where the defence lawyer needed to be security-cleared and the accused, through no fault of his or her own, was unable to obtain a lawyer cleared at the appropriate level, or insisted on a lawyer of his or her choice who did not have the necessary clearance.

Overseas examples of clearance requirements for lawyers

13.36 Maher notes that the US Military Rules of Evidence authorise the military judge, at the request of the government, to issue a protective order requiring security clearances 'for persons having a need to examine the information in connection with preparation of the defense' prior to disclosure to the defence.[dxcv] Maher also raises the issue of an accused deliberately choosing civilian or military counsel who he or she knows will not be cleared.[dxcvi]

13.37 More recently, legal instructions have been put in place for the trial of potential war criminals by US Military Commissions if the US President names individuals to be considered for prosecution.[dxcvii] US Department of Defense Military Commission Instruction No. 5, dealing with the qualification of 'civilian defense counsel', refers to access by counsel to material classified at the level of Secret or higher based on security clearances.[dxcviii]

13.38 Under the Instruction, counsel who state their willingness to submit to a background investigation must be prepared to pay the actual costs of processing the security clearance. This issue has not yet been publicly considered in Australia, but raises further difficulties concerning the approval, selection and availability of lawyers to appear in cases concerning classified or security sensitive information.

13.39 Defence counsel may be required to be security cleared in criminal cases in the United States under the *Classified Information Procedures Act* (CIPA). Section 3 of that Act provides that:

> Upon motion of the United States, the court shall issue an order to protect against the disclosure of any classified information disclosed by the United States to any defendant in any criminal case in a district court of the United States.

13.40 The US Department of Justice has noted that the 'protective order must be sufficiently comprehensive to ensure that access to classified information is restricted to cleared persons'.[dxcix] This requirement presumably extends to the lawyers involved in any case covered by the CIPA. However:

> The requirement of security clearances does not extend to the judge or to the defendant (who would likely be ineligible, anyway). Some defense counsel may wish to resist this requirement by seeking an exemption by order of the court. The prosecutor should advise defense counsel that, because of the stringent restrictions imposed by federal regulations, statutes and Executive Orders upon the disclosure of classified information, such tack may prevent, and will certainly delay, access to classified information.[dc]

13.41 The security procedures established under the CIPA provide that:

> The government may obtain information by any lawful means concerning the trustworthiness of persons associated with the defense and may bring such information to the attention of the court for the court's consideration in framing an appropriate protective order pursuant to Section 3 of the Act.[dci]

13.42 The US Department of Justice has recently drafted further anti-terrorism legislation in the form of the proposed *Domestic Security Enhancement Act 2003*, also known as PATRIOT ACT II (draft).[dcii] Section 108 of that Act would amend the *Foreign Intelligence Surveillance Act 1978* to permit the FISA Court of Review, in its discretion, to appoint a lawyer with appropriate security credentials to defend the judgment of the FISA Court when the United States appeals a ruling to the FISA Court of Review.[dciii]

13.43 In Canada, independent security-cleared counsel appear before hearings conducted by the Security Intelligence Review Committee (SIRC).[dciv] The SIRC appoints counsel to assist it from a panel of security-cleared lawyers.

> Two tasks of counsel to SIRC are particularly important: cross-examining in the *in camera* portion of the proceedings (one counsel described this as attempting 'to fill the vacuum of the complainant's absence') and negotiating with counsel for [the Canadian Security Intelligence Service (CSIS)] on the form of evidence to be disclosed from this portion of the hearings. Additionally, counsel acting for SIRC will liaise with the complainant's counsel to ensure that the questions the latter wishes to see answered are put in the closed session … However, counsel to SIRC, complainants' counsel, and SIRC all expressed scepticism about the practical utility of this facility. … without knowledge of CSIS's evidence, counsel to the complainant faced inevitable difficulties in preparing for this vicarious cross-examination.[dcv]

Security clearance of judges and magistrates

13.44 Should judges and magistrates also be required to obtain security clearances for matters involving classified or security sensitive information? Any such requirement could strike at the heart of judicial independence and the separation of powers doctrine. The ALRC understands that it is not the government's intention to require judges and magistrates to be security cleared.

13.45 Depending on how it might be implemented, such a proposal also could have an adverse impact on an accused's right to be tried without undue delay—for example, if classified or security sensitive information unexpectedly came to light during the course of a part-heard trial, requiring the judge at that stage to obtain a security clearance could cause undue delay. Further complications could arise if a judge who had part-heard the matter declined to submit to a security check or was refused a security clearance. A security clearance is not required for judges in the USA under the *Classified Information Procedures Act*[dcvi] (CIPA) 'but such clearance shall be provided upon the request of any judicial officer who desires to be cleared'.[dcvii]

Security clearance of other people involved in court hearings

13.46 The question also arises whether other people involved in the court process, apart from lawyers, would have to obtain a security clearance in matters involving national security or where classified and security sensitive information is involved. Conceivably, this might include jurors,[dcviii] court staff,[dcix] court reporters, translators and others. For example, expert witnesses may need to be given access to classified or security sensitive information in order to give an opinion as to whether the communication of such information posed a threat to national security. The US Attorney's Manual states that 'when interviewing witnesses, classified information may only be discussed if the witnesses have appropriate security clearances and the agency that classified the information has approved such disclosure'.[dcx]

13.47 The Victorian Bar has submitted that a proposal for jurors to have some sort of security clearance before being able to participate in a trial involving matters of national security should never be countenanced.[dcxi] This could create some pressure to move towards trials without juries, although there is strong support for juries in federal criminal matters.[dcxii]

13.48 The security procedures established pursuant to CIPA do not require 'an investigation or security clearance of the members of the jury' nor are they to be construed as interfering with the 'functions of a jury including access to classified information introduced as evidence'.[dcxiii] However, they provide that:

> After a verdict has been rendered by a jury, the trial judge should consider a government request for a cautionary instruction to jurors regarding the release or disclosure of classified information contained in documents they have reviewed during the trial.[dcxiv]

13.49 Section 206 of the draft PATRIOT ACT II would amend:

> Rule 6(e)(2)(B) of the Federal Rules of Criminal Procedure to make witnesses and persons to whom subpoenas are directed subject to grand jury secrecy rules in cases where serious adverse consequences may otherwise result, including danger to the national security or to the life or physical safety of an individual, flight from prosecution, destruction of or tampering with evidence, intimidation of a potential witness, or other serious jeopardy to an investigation. The provision would permit witnesses and recipients of grand jury subpoenas to consult with counsel regarding the subpoena and any testimony, but would impose the same secrecy obligations on counsel.[dcxv]

Security clearance of investigators

13.50 The Terms of Reference ask the ALRC to consider mechanisms to protect classified and security sensitive information in the course of investigations, as well as proceedings. With this in mind, the issue arises whether investigators or other persons who may gain access to classified or security sensitive information are already covered by the standards set out in the Commonwealth Protective Security Manual or whether some further procedure might be appropriate.

Sector-specific clearances

13.51 Threats of terrorism have brought the security of critical infrastructure to the fore. The federal government has acknowledged the significant role that the private sector has to play in managing the new security environment.[dcxvi] In April 2003 the government launched the Trusted Information Sharing Network for Critical Infrastructure (TISN). The Attorney-General stated that:

> The TISN will provide a forum for the owners and operators of Australia's critical infrastructure to exchange information on security-related issues. …
>
> The network comprises a number of sector groups, including emergency management, transport and distribution, banking and finance, telecommunications, health and food supplies.[dcxvii]

13.52 In addition to the TISN, under the government's counter-terrorism plans more private sector workers will be considered for security clearances to possess or gain access to confidential material. Some private sector officials in the transport, ports, legal, aviation and chemical sectors already have security clearances enabling them to access sector-specific sensitive material.[dcxviii]

Question 78. What are the arguments for and against requiring security clearance of:

(a) all, or any category of, lawyers in all, or any category of, matters involving classified or security sensitive information;

(b) judges or magistrates who do or may hear any matters involving classified or security sensitive information;

(c) any other individuals or categories of people involved in court or tribunal hearings involving classified or security sensitive information; for example, jurors, court staff, court reporters, translators and witnesses; and

(d) investigators or other people who may gain access to classified or security sensitive information during the course of an investigation, at least to the extent that they are not already covered by the Commonwealth Protective Security Manual?

Question 79. Would requiring judges and magistrates to obtain a security clearance improperly impinge on the independence of the judiciary and the separation of powers doctrine?

Question 80. If judges and magistrates did require security clearances in appropriate cases, would this necessitate a pool of judges and magistrates

cleared in advance of need? As a practical matter, how would this pool be determined?

Question 81. What would be the nature and level of any security clearances required of lawyers, judges, magistrates and others involved in court and tribunal proceedings?

Question 82. If any of the categories of people involved in court and tribunal proceedings are to be security-cleared, what procedures, if any, should be put in place in relation to the monitoring of their security clearances? In particular, would the principles relating to the revalidation and re-evaluation of security clearances as set in the Commonwealth Protective Security Manual apply?

Question 83. Who should pay for any such security clearances and any appeals from adverse or qualified clearance decisions? Will requirements to security clear lawyers, judges and magistrates, and other people involved in court and tribunal hearings have a negative impact on the costs of getting access to, and dispensing, justice?[dcxix]

Question 84. Are existing mechanisms to protect classified and security sensitive information in court proceedings (such as confidentiality undertakings, in camera hearings and publication restrictions) adequate to protect classified and security sensitive information used in court and tribunal hearings? Do they remove the need for lawyers, or judges and magistrates, or other people involved in court and tribunal hearings, to obtain security clearances?

Question 85. Are the character checks already in place to ascertain whether a person is 'fit and proper' for admission as a solicitor or barrister and to hold a practising certificate sufficient to allay concerns over their handling of classified and security sensitive information?

Question 86. Is it feasible to have an independent lawyer selected from a panel of security-cleared lawyers in any types of matters involving classified or security sensitive information to protect the interests of a party who is not (and whose lawyer is not) security cleared?

Question 87. What standards and procedures are currently in place in relation to security clearing individuals from the private sector to enable them to access sector-specific sensitive information? Are any such standards and procedures uniform across the private sector? Are they an effective mechanism in protecting classified and security sensitive information?

Abbreviations and Acronyms

AAT	Administrative Appeals Tribunal
ACC	Australian Crime Commission
AFP	Australian Federal Police
ALRC	Australian Law Reform Commission
ANAO	Australian National Audit Office
APS	Australian Protective Service *or* Australian Public Service
ASIO	Australian Security Intelligence Organisation
ASIO Act	*Australian Security Intelligence Organisation Act 1979* (Cth)
ASIO Bill	Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002 [No 2]
ASIS	Australian Secret Intelligence Service
ASVS	Australian Security Vetting Service
ATRC	Alien Terrorist Removal Court (USA)
AUSTEO	For Australian Eyes Only
CIA	Central Intelligence Agency (USA)
CIPA	*Classified Information Procedures Act* (USA)
Crimes Act	*Crimes Act 1914 (Cth)*
CSIS	Canadian Security and Intelligence Service
DIMIA	Department of Immigration and Multicultural and Indigenous Affairs
DIO	Defence Intelligence Organisation
DSD	Defence Signals Directorate
EO 13292	*Executive Order 13292—Further Amendment to Executive Order 12958, As Amended: Classified National Security Information* (USA)
FBI	Federal Bureau of Investigation (USA)
FISA	*Foreign Intelligence Surveillance Act* (USA)
FISC	Foreign Intelligence Surveillance Court (USA)
FOI	Freedom of information
FOI Act	*Freedom of Information Act 1982* (Cth)
ICCPR	International Covenant on Civil and Political Rights
IGIS	Inspector-General of Intelligence and Security
IGIS Act	*Inspector-General of Intelligence and Security Act 1986* (Cth)
INS	Immigration and Naturalization Service (USA)
IPPs	Information Privacy Principles [under the *Privacy Act*]

LECD	Law Enforcement Coordination Division [of the Attorney-General's Department]
MRT	Migration Review Tribunal
NCTC	National Counter-Terrorism Committee
NPPs	National Privacy Principles [under the *Privacy Act 1988* (Cth)]
ONA	Office of National Assessments
PII	Public interest immunity
Privacy Act	*Privacy Act 1988* (Cth)
PSM	Commonwealth Protective Security Manual
Refugee Convention	The *Convention Relating to the Status of Refugees* 1951 as amended by the *Protocol Relating to the Status of Refugees* 1967
RRT	Refugee Review Tribunal
SIAC	Special Immigration Appeals Commission (UK)
SIRC	Security Intelligence Review Committee (Canada)
TISN	Trusted Information Sharing Network for Critical Infrastructure
USA PATRIOT Act	*Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act of 2001* (USA)
USC	United States Code

ENDNOTES

Chapter 1

i Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, C 29, para 6.21.
ii Ibid, C 5, para 1.3.
iii Ibid, C 9, para 2.4.
iv See Ch 2.
v Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, C 6, para 1.4. It is worth noting the distinction drawn between public interest and government interest: there may be occasions when the two do not coincide.
vi Ibid, C 29, para 6.22.
vii Ibid, C 31, para 6.29–6.34.
viii Ibid, C 31–C 32, para 6.32–6.34.
ix Ibid, C 30, para 6.24.
x Ibid, C 32, para 6.35–6.42.
xi Ibid, C 33–C 34, para 6.41–6.43.

xii Ibid, C 29, para 6.23–6.25.
xiii Ibid, C 27, para 6.12.
xiv L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994) Clarendon Press, Oxford, 321–322.
xv Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, C 27, para 6.14.
xvi Ibid, C 28, para 6.17.
xvii Ibid, C 34, para, 6.45.
xviii The PSM only notes that 'it may be appropriate to regularly review the security classification of agency information, for example, after a project or sequence of events is completed or when a file is withdrawn from or returned from use': Ibid, C 35, para 6.49.
xix The enforceability of the security standards in the PSM is discussed in Ch 3.
xx J Markon, *Convicted Spy Accepts Life Sentence*, Washington Post, <www.washingtonpost.com/wp-dyn/articles/A1276-2003Mar20.html>, 21 March 2003.
xxi *Australian Law Reform Commission Act 1996* (Cth), s 24(2). These are also considered in Ch 5 and 11.
xxii *Australian Security Intelligence Organisation Act 1979*, s 4.
xxiii The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill [No 2] 2002 (Cth), which passed through Parliament on 25 June 2003, will give ASIO substantial 'police powers' of detention and investigation.
xxiv Australian Secret Intelligence Service, *The Australian Secret Intelligence Service*, <www.asis.gov.au/asiscorpinfo.html>, 29 May 2003. See also *Intelligence Services Act 2001* (Cth), s 11.
xxv *Intelligence Services Act 2001* (Cth), s 15.
xxvi Defence Intelligence Organisation, *About the Defence Intelligence Organisation*, <www.defence.gov.au/dio>, 29 May 2003.
xxvii Defence Signals Directorate, *About DSD*, <www.dsd.gov.au/dsd/index.html>, 29 May 2003.
xxviii Office of National Assessments, *About ONA*, <www.ona.gov.au>, 29 May 2003. The government announced in late May 2003 that a new elite security body would be set up within the Department of Prime Minister and Cabinet, reporting directly to the Prime Minister. Few details were available when this Paper went to press.
xxix Australian Crime Commission, <www.crimecommission.gov.au/index>, 17 June 2003.
xxx Inspector-General of Intelligence and Security, *About IGIS*, <www.igis.gov.au/fs_about.html>, 29 May 2003.
xxxi *Parliamentary Joint Committee on ASIO, ASIS and the DSD*, <www.aph.gov.au/house/committee/pjcaad/role.htm>, 29 May 2003.
xxxii M Sassella, 'Reviewing Particular Decisions Made by ASIO: The Security Appeals Division of the Administrative Appeals Tribunal' (Paper presented at Security in Government Conference, Canberra, 1 April 2002), 2. See also Ch 12.
xxxiii D Collins, 'Spies Like Them' (2002) 24 *Sydney Law Review* 505, 505.
xxxiv *Canadian Security and Intelligence Service Act 1985*, s 2, as cited in Ibid, 506.

xxxv Canadian Security and Intelligence Service, <www.csis-scrs.gc.ca/eng/menu/faq_e.html>, 23 June 2003.
xxxvi Communications Security Establishment, <www.cse.dnd.ca/en/about_cse/about_cse.html>, 23 June 2003.
xxxvii MI5, *Responsibilities of MI5*, <www.mi5.gov.uk/responsibilities/responsibilities.htm>, 29 May 2003.
xxxviii D Collins, 'Spies Like Them' (2002) 24 *Sydney Law Review* 505, 512.
xxxix Ibid, 513.
xl Ibid, 520. On 1 March 2003, the functions of the US Customs Service were transferred to the Directorate of Border and Transportation Security within the Department of Homeland Security. As part of this transition, the functions of the US Customs Service and other border and security agencies were reorganised into the Bureau of Immigration and Customs Enforcement: see <www.bice.immigration.gov/graphics/>.
xli Central Intelligence Agency, *About the CIA*, <www.cia.gov/cia/information/info.html>, 29 May 2003.
xlii Ibid.
xliii D Collins, 'Spies Like Them' (2002) 24 *Sydney Law Review* 505, 520.
xliv Ibid, 521. The Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill [No 2] 2002 (Cth), which passed through Parliament on 25 June 2003, will give ASIO substantial 'police powers' of detention and investigation.
xlv D Collins, 'Spies Like Them' (2002) 24 *Sydney Law Review* 505, 522.
xlvi *Homeland Security*, <www.whitehouse.gov/homeland/index.html>, 29 May 2003.

Chapter 2

xlvii H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney, 92.
xlviii Ibid, 92. The First Amendment to the US Constitution reads: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.'
xlix The ALRC has considered a number of these issues in the past: ALRC 12 (1979) *Privacy and the Census*; ALRC 22 (1983) *Privacy*; ALRC 77 (1995) *Open Government: A Review of the Freedom of Information Act 1982*; ALRC 85 (1998) *Australia's Federal Record: A Review of the Archives Act 1983.*
l ASIS, ASIO, ONA and the Inspector-General of Intelligence and Security, amongst others. See H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney.
li Ibid, 132.
lii See *Freedom of Information Act 1982* (Cth), s 55(1) and 58(1). See H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney, 133.

liii *Re Anderson and the Australian Federal Police* (1986) 11 ALD 355.

liv Ibid, para 120. See H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney.

lv H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney, 124.

lvi J Ashcroft, *Memorandum for Heads of all Federal Departments and Agencies re The Freedom of Information Act*, 12 October 2001.

lvii The ALRC recently conducted a major inquiry which considered matters of 'genetic privacy', and in so doing considered privacy law in considerable detail: see Australian Law Reform Commission, *Essentially Yours: The Protection of Human Genetic Information in Australia*, ALRC 96 (2003), Commonwealth of Australia.

lviii *Privacy Act 1988* (Cth), s 14 (IPPs), Sch 3 (NPPs).

lix Ibid, s 40.

lx Ibid, s 44.

lxi Ibid, s 45.

lxii Ibid, s 55A.

lxiii Ibid, s 14, Principle 11.

lxiv Federal Privacy Commissioner, *Correspondence*, 3 June 2003.

lxv Examples in Australia of whistleblowing include the whistleblowing by a former senior Defence official in February 2002 that Defence security had asked ASIO to bug Labor MP Laurie Brereton's parliamentary office, and his allegation in May 2003 that the ASIO official who had received the request had been placed under surveillance by ASIO: L Wright, 'ASIO "Tailed Own Man" after Brereton Story', *The Canberra Times*, 1 May 2003.

lxvi These include the *Whistleblowers Protection Act 1993* (SA), the *Whistleblowers Protection Act 1994* (Qld), the *Public Interest Disclosure Act 1994* (ACT), the *Whistleblowers Protection Act 2001* (Vic), the *Public Interest Disclosures Act 2002* (Tas) and the *Protected Disclosures Act 1994* (NSW). On 20 March 2002 the Whistleblowers Protection Bill 2002 was introduced into the Western Australian Parliament. The title of the Bill was amended on 7 May 2002 to the Public Interest Disclosure Bill 2002. The second reading of the bill took place on 11 March 2003 in the Legislative Council; the third reading took place on 12 March 2003. There is no legislation in the Northern Territory providing protection for whistleblowers. However, the Northern Territory Law Reform Committee has recently recommended that 'if the Legislative Assembly of the Northern Territory sees fit to enact Whistleblower legislation, then the provisions of the Victorian and Tasmanian statutes be adopted as the general model for such legislation': Northern Territory Law Reform Committee, *Report on Whistleblowers Legislation*, Report No 26 (2002), 2.

lxvii See for example, *Public Interest Disclosure Act 1994* (ACT), s 35; and *Protected Disclosures Act 1994* (NSW), s 21. Section 21 of the NSW Act provides that the limitation of liability has effect 'despite any duty of secrecy or confidentiality or any other restriction on disclosure (whether or not imposed by an Act) applicable to the person'.

lxviii See for example, *Protected Disclosures Act 1994* (NSW), s 20 and *Whistleblowers Protection Act 2001* (Vic), s 18.

lxix See for example, *Public Interest Disclosure Act 1994* (ACT), s 29, and *Whistleblowers Protection Act 1994* (Qld), s 43.

lxx Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, Commonwealth of Australia, Canberra, 1. The Committee stated that 'the Bill contains deficiencies in some of its provisions, the remedy of which will require further consideration and redrafting': Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, Commonwealth of Australia, Canberra, 12.

lxxi Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, Commonwealth of Australia, Canberra, 1. The Commonwealth Ombudsman appeared before the Committee and 'strongly supported the introduction of whistleblower legislation extending across the whole Commonwealth employment area': R McLeod, 'Blowing the Official Whistle' (Paper presented at Transparency International Whistleblowing Symposium, Sydney, 6 August 2002), 2.

lxxii The APS Code of Conduct is set out in the *Public Service Act 1999* (Cth), s 13. The Code of Conduct is briefly discussed in Ch 3.

lxxiii 'Commissioner' is defined as the Public Service Commissioner appointed under the Act: Ibid, s 7.

lxxiv 'Merit Protection Commissioner' is defined as the Merit Protection Commissioner appointed under the Act: Ibid, s 7.

lxxv Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, Commonwealth of Australia, Canberra, 1. Note that employees of the Australian Government Solicitor, Australian Maritime Safety Authority and Civil Aviation Safety Authority are not covered by the *Public Service Act 1999* (Cth) and are thus not covered by s 16: See Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, Commonwealth of Australia, Canberra, 21.

lxxvi *Australian Security Intelligence Organisation Act 1979* (Cth), s 86.

lxxvii See the Australian Public Service Commission website, which lists all APS agencies at<www.apsc.gov.au/apsprofile/agencies.htm>.

lxxviii Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Commonwealth), cl 3. Note that para (c) of this definition is not included in the definition of 'public interest disclosure' in the *Public Interest Disclosure Act 1994* (ACT), s 3.

lxxix Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Commonwealth), cl 5(1); *Public Interest Disclosure Act 1994* (ACT), s 4(1).

lxxx Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Commonwealth), cl 5(2). Note that the types of 'disclosable conduct' covered by *Public Interest Disclosure Act 1994* (ACT), s 4(2), include grounds like those specified in para (a)–(d) listed in para 2.24, as well as a conspiracy or attempt to engage in such conduct.

lxxxi *Public Interest Disclosure Act 1994* (ACT), s 15; and Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Commonwealth), cl 14. Under the *Whistleblowers Protection Act 2001* (Vic), s 5 a 'natural person' in specified

circumstances may disclose 'improper conduct' or 'detrimental action' as defined in s 3 of the Act. *Whistleblowers Protection Act 1994* (Qld), s 19 and 20 provide respectively that anybody may disclose danger to a person with a disability or to the environment from particular contraventions and that anybody may disclose a reprisal as a result of whistleblowing.

lxxxii *Protected Disclosures Act 1994* (NSW), s 8 provides that to be protected by the Act, a disclosure must be made by a public official to the bodies specified in the Act. *Public Interest Disclosures Act 2002* (Tas), s 6 provides that a public officer or a contractor who has entered into a contract with a public body may in specified circumstances disclose 'improper conduct' or 'detrimental action' as defined in s 3 of the Act. *Whistleblowers Protection Act 1994* (Qld), s 15–18 provide that a public officer may disclose official misconduct, maladministration, negligent or improper management affecting public funds, and danger to public health or safety or the environment.

lxxxiii Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, Commonwealth of Australia, Canberra, 5. The Northern Territory Law Reform Committee recommended that if whistleblower protection legislation is enacted by the Legislative Assembly of the Northern Territory, the class of persons to be protected should not be in the category of 'public officer' as in the Tasmanian legislation or 'natural persons' as in the Victorian legislation but, rather in the category of 'any person' as in the South Australian legislation: Northern Territory Law Reform Committee, *Report on Whistleblowers Legislation*, Report No 26 (2002), 2.

lxxxiv *Public Interest Disclosure Act 1994* (ACT), s 16.

lxxxv *Whistleblowers Protection Act 2001* (Vic), s 7. See also *Public Interest Disclosures Act 2002* (Tas), s 8.

lxxxvi Under cl 15 a person making an anonymous disclosure must identify themselves to the head of a proper authority as specified in the Act. The Committee suggested that the Bill provide for anonymous disclosures to be deemed 'protected disclosures' under the legislation in the event that the identity of the person making the disclosure became known: Finance and Public Administration Legislation Committee, *Public Interest Disclosure Bill 2001 [2002]*, Commonwealth of Australia, Canberra, 9.

lxxxvii For example, *Public Interest Disclosure Act 1994* (ACT), s 33, if a public official without reasonable excuse makes a record of, or wilfully discloses to another person, confidential information gained through the public official's involvement in the administration of the Act, the penalty is 50 penalty units. 'Confidential information' includes information about the identity of the person who makes a public interest disclosure or against whom such a disclosure is made. Under the Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Commonwealth), cl 34, the penalty for a breach of confidentiality is also 50 penalty units. The penalty for a breach of confidentiality under the *Whistleblowers Protection Act 1994* (Qld), s 55 is 84 penalty units; while under the *Whistleblowers Protection Act 2001* (Vic), s 22 and the *Public Interest Disclosures Act 2002* (Tas), s 23 the penalty is six months' imprisonment, 60 penalty units or both.

lxxxviii The offence of knowingly or recklessly making a false or misleading statement with the intention that it be acted upon as a public interest disclosure carries the penalty of 100 penalty units or imprisonment for one year or both, if the offender is a natural person, and 500 penalty units if the offender is a body corporate under Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Commonwealth), cl 35 and *Public Interest Disclosure Act 1994* (ACT), s 34. Under *Protected Disclosures Act 1994* (NSW), s 28, the offence of wilfully making a false statement to, or misleading or attempting to mislead an investigating authority, public authority or public official carries the maximum penalty of 50 penalty units or imprisonment for 12 months or both. Intentionally providing information to an appropriate entity that is false or misleading in a material particular, intending that it be acted upon as a public interest disclosure carries the maximum penalty of 167 penalty units or 2 years imprisonment under *Whistleblowers Protection Act 1994* (Qld), s 56. The offence of knowingly making a false disclosure carries the penalty of 240 penalty units or 2 years imprisonment or both under the *Whistleblowers Protection Act 2001* (Vic), s 106.

lxxxix The offence of engaging in, or attempting or conspiring to engage in, an unlawful reprisal carries the penalty of 100 penalty units or imprisonment for one year or both if the offender is a natural person, and 500 penalty units if the offender is a body corporate under Public Interest Disclosure (Protection of Whistleblowers) Bill 2002 (Commonwealth), cl 26 and *Public Interest Disclosure Act 1994* (ACT), s 25. More stringent penalties are found in *Whistleblowers Protection Act 2001* (Vic), s 18 which provides for a penalty of 240 penalty units or two years imprisonment or both for a person who takes 'detrimental action' (as defined) against a person in reprisal for a protected disclosure; and in the *Whistleblowers Protection Act 1994* (Qld), s 42 which provides for a penalty of 167 penalty units or two years imprisonment for the offence of reprisal.

xc T Wang, *The New Homeland Security Agency and Whistleblowers* (2002) The Century Foundation, 4.

xci Agent Rowley testified before Congress that supervisors in FBI headquarters impeded attempts by agents in Minneapolis to obtain a warrant after 11 September 2001 to examine Moussaoui's laptop computer, which was found to contain information suggesting his complicity in the attacks: Ibid, 2.

xcii Ibid, 2. Other whistleblowing by FBI employees includes allegations by Sibel Edmonds and John Cole of 'mismanagement and lax security—and in one case possible espionage—among those who translate and oversee some of the FBI's most sensitive, top secret wiretaps in counterintelligence and counter terrorist investigations': J Grimaldi, *2 FBI Whistle-Blowers Allege Lax Security, Possible Espionage*,<http://foi.missouri.edu/whistleblowing/2fbiwhistleblowers.html>, 19 June 2002. Edmonds was fired after reporting her concerns.

xciii *Homeland Security Act 2002* (USA), s 883.

xciv J Peckenpaugh, *Homeland Security Employees Will Retain Whistleblower Rights*, <http://foi.missouri.edu/whistleblowing/homelandsecurity1.html>, 20 November 2002.

xcv Ibid.

xcvi C Grassley, *Press Release: Grassley Seeks Whistleblower Protections for New Federal Employees—Senator Says Public Safety and Security at Stake*, <http://grassley.senate.gov/releases/2002/p02r6-26b.htm>, 26 June 2002.
xcvii ARTICLE 19 and Liberty are both UK-based non-governmental organisations concerned to protect civil liberties, including freedom of speech. ARTICLE 19, named after Art 19 of the Universal Declaration of Human Rights, 'works worldwide to combat censorship by promoting freedom of expression and access to official information': see website of ARTICLE 19 at <www.article19.org/>.
xcviii ARTICLE 19 and Liberty, *Secrets, Spies and Whistleblowers Freedom of Expression and National Security in the United Kingdom* (2000), The Guardian, see <www.article19.org/docimages/791.htm>, Rec 13.
xcix *Protected Disclosures Act 2000* (NZ), s 12–14. Section 13 sets out special rules in relation to the internal procedures of the Department of the Prime Minister and Cabinet, the Ministry of Foreign Affairs and Trade, the Ministry of Defence and the New Zealand Defence Force, insofar as they relate to the disclosure of information concerning the international relations of the Government of New Zealand or intelligence and security matters.
c *The Johannesburg Principles on National Security, Freedom of Expression and Access to Information*, UN Doc E/CN.4/1996/39 (1995). The Principles are not binding on Australia.
ci ARTICLE 19 and Liberty, *Secrets, Spies and Whistleblowers Freedom of Expression and National Security in the United Kingdom* (2000), The Guardian, see <www.article19.org/docimages/791.htm>, 1.2.

Chapter 3

cii See the webpage of the Protective Security Coordination Centre at <www.ag.gov.au/protectivesecurityHome.nsf/HeadingPagesDisplay/Protective+Security+Manual?OpenDocument>.
ciii The classification system is discussed in Ch 1.
civ Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, C 10, para 2.7.
cv Ibid, C 10, para 2.8.
cvi Ibid, C 26, para 6.9.
cvii Ibid, C 30, para 6.26.
cviii Ibid, A 18, para 5.1.
cix Ibid, C 19, para 4.17.
cx Ibid, A 6, para 1.9.
cxi Ibid, F 37, para 6.8.
cxii Ibid, F 37, para 6.8.
cxiii Ibid, F 36, para 6.4.
cxiv See *Public Service Act 1999* (Cth), s 14: 'Statutory office holder means a person who holds any office or appointment under an Act, being an office or appointment that is prescribed by the regulations for the purposes of this definition'.
cxv Ibid, s 13(2).

cxvi Ibid, s 13(5).
cxvii Ibid, s 13(4).
cxviii Ibid, s 13(10).
cxix Agency Heads are required to establish procedures for determining whether an APS employee in their agency has breached the Code of Conduct: Ibid, s 15(3). Under this provision, the procedures must, among other things, have due regard to procedural fairness.
cxx Ibid, s 15(1).
cxxi *Public Service Regulations 1999* (Cth), Reg 3.10.
cxxii See Australian National Audit Office, *Personnel Security—Management of Security Clearances*, Report 22 (2001–2002), Commonwealth of Australia.
cxxiii Ibid, para 19. For example, the audit found that all but one organisation had a large number of security clearances overdue, noting that a failure to maintain the currency of security clearances breached Part D, section 8 of the PSM: para 14. In this regard the ANAO recommended that 'organisations consider taking concerted efforts to overcome the current backlog in the conduct of security clearances as a matter of priority and ensure these processes are carried out in a timely manner in the future': Rec 8. The audit also found that most organisations did not have an up-to-date protective security risk assessment as required by Part B of the PSM (para 15) and that there was non-compliance with the requirements of Part D, section 10 of the PSM in relation to maintenance, administration and disposal of personal security records; and non-compliance with the requirements of Part D, section 6 of the PSM in relation to maintenance of clearance documentation, including interview reports: para 17.
cxxiv See Australian National Audit Office, *Physical Security Arrangements in Commonwealth Agencies*, 23 (2002–2003), Commonwealth of Australia.
cxxv Ibid, para 11.
cxxvi These deficiencies included that, to varying degrees, agencies were not educating their staff, contractors and clients of agency security standards, and were not undertaking periodic comprehensive security risk assessments: Ibid, para 13. In relation to the protection of security classified information, the ANAO recommended that 'agencies ensure their security risk assessments, implemented security controls, and documented security procedures adequately address all requirements for the storage, handling and processing of any security-classified information as discussed in Part E, section 7 of the PSM': Rec 5.
cxxvii W Clinton, *Executive Order 12958—Classified National Security Information*,<www.usdoj.gov/oip/foia_updates/Vol_XVI_2/page5.htm> was amended by W Clinton, *Executive Order 13142—Amendment to Executive Order 12958—Classified National Security Information*, 19 November 1999 and again by G Bush, *Executive Order 13292—Further Amendment to Executive Order 12958, As Amended: Classified National Security Information*, 25 March 2003.
cxxviii G Bush, *Executive Order 13292—Further Amendment to Executive Order 12958, As Amended: Classified National Security Information*, 25 March 2003, s 1.2. It is interesting to note that the provision in an earlier version of this Executive Order that, if there were any significant doubt about the appropriate level of classification of information, it should be classified at the lower level, has been removed: see W

Clinton, *Executive Order 12958—Classified National Security Information*, <www.usdoj.gov/oip/foia_updates/Vol_XVI_2/page5.htm> s 1.3(c).

cxxix G Bush, *Executive Order 13292—Further Amendment to Executive Order 12958, As Amended: Classified National Security Information*, 25 March 2003, s 1.3.

cxxx Ibid, s 1.5.

cxxxi Ibid, s 1.6.

cxxxii Ibid, s 1.8.

cxxxiii Ibid, s 5.3.

cxxxiv Ibid, s 1.7.

cxxxv Ibid, s 1.7(a).

cxxxvi Ibid, s 5.5.

cxxxvii The PSM, C 34, para 6.45 states that agencies should limit the duration of the classification and establish review procedures, but the requirement to establish review procedures is not expressed as a minimum standard.

cxxxviii The minimum standard in the PSM provides that 'agencies must consider whether a time limit for a classification can be set': Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, C 98, para 6.46.

Chapter 4

cxxxix *Public Service Act 1999* (Cth), s 13(10).

cxl Agency Heads are required to establish procedures for determining whether an APS employee in their agency has breached the Code of Conduct: Ibid, s 15(3). Under this provision, the procedures must, among other things, have due regard to procedural fairness. The *Public Service Act* and APS Code of Conduct are discussed further in Ch 3.

cxli Ibid, s 15(1).

cxlii L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18(5) *Criminal Law Journal* 254, 257.

cxliii *Intelligence Services Act 2001* (Cth), s 39(1). The ASIO Act does not have a similar provision: ASIO officers are deemed to be Commonwealth officers for the purposes of the *Crimes Act 1914* (Cth) and are therefore covered by s 70 of that Act: see ASIO Act, s 91.

cxliv A similar provision is found in the ASIO Act, s 92.

cxlv *Inspector-General of Intelligence and Security Act 1986* (Cth), s 34.

cxlvi Espionage offences had previously been found in Part VII of the *Crimes Act 1914* (Cth). Ch 2 of the *Criminal Code* (a schedule to the *Criminal Code Act 1995* (Cth)) sets out the general principles of criminal responsibility that apply to all offences against the *Crimes Act 1914* (Cth): *Crimes Act 1914* (Cth), s 3BA.

cxlvii NSW Council for Civil Liberties, *Submission on the Criminal Code (Espionage and Related Offences) Bill 2002*, <www.nswccl.org.au/docs/pdf/EspionageBill2002.pdf>, 21 May 2003. See the discussion of whistleblowers' protections in Ch 2.

cxlviii *Crimes Act 1914* (Cth), s 79(1)–(10).

cxlix Ibid, s 79(2), (5), (8) and (9).
cl Ibid, s 79(3), (4) and (6).
cli L Tsaknis, 'Commonwealth Secrecy Provisions: Time for Reform?' (1994) 18(5) *Criminal Law Journal* 254, 265, citing *Grant v Headland* (1977) 77 ACTR 29.
clii Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill [No 2] 2002 (Cth), cl 34AA.
cliii Office of the Attorney-General, *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002—Government Proposals*, 11 June 2003.
cliv See <www.cabinet-office.gov.uk/guidance/one/directory.asp?intID=80> (21 May 2003).
clv Some of these comments would seem to apply to the *Crimes Act 1914* (Cth), s 79 as well.
clvi See L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994) Clarendon Press, Oxford, 280.
clvii BBC News, *Troubled History of the Official Secrets Act*, <http://news.bbc.co.uk/1/hi/uk/216868.stm>, 17 June 2003.

Chapter 5

clviii See also Art 6(1) of the European Convention on Human Rights and its Five Protocols, which is in similar terms to Art 14(1) of the ICCPR but is not binding on Australia.
clix The Human Rights Committee has broadly interpreted the phrase 'suit at law'. See M Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993) NP Engel, 250. For example, in *VMRB v Canada* (Unreported, 235/1987), the Committee did not exclude the possibility that deportation proceedings may be 'suits at law'.
clx It has been commented that 'national security' for the purpose of the ICCPR requires proof of a 'grave case … of political or military threat to the entire nation': M Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993) NP Engel, 212. See also discussion below under heading 'When is closure justified under international law?'
clxi The Universal Declaration of Human Rights was adopted by the General Assembly of the United Nations on 10 December 1948 in Paris. Australia was involved in the development of the Universal Declaration and adopted (or 'ratified') the statement in 1948—one of the original countries to do so. The Universal Declaration is not legally binding. It sets out principles and objectives and carries moral weight. However, many laws, human rights covenants and conventions have been based on the principles set forth in it. See website of Human Rights and Equal Opportunity Commission at<www.hreoc.gov.au/human_rights_dialogue/understanding.html>.
clxii The Convention on the Rights of the Child, to which Australia is a party, contains in Art 40(2)(b)(iii) a guarantee that every child alleged or accused of having infringed the penal law is entitled to 'have the matter determined without delay by a competent, independent and impartial authority or judicial body in a fair hearing according to law, in the presence of legal or other appropriate assistance and, unless it

is considered not to be in the best interest of the child, in particular, taking into account his or her age or situation, his or her parents or legal guardians'.

clxiii This Act amends the *Criminal Procedure Act 1986* (NSW).

clxiv This is the case in respect of Art 14(3) of the ICCPR, which is binding on Australia, and Art 6(3) of the European Convention on Human Rights and its Five Protocols, which is not binding on Australia. Note also that *International Criminal Court Act 2002* (Cth), Sch 1, Art 67 sets out the minimum guarantees to be afforded to an accused in the determination of any charge.

clxv The issue of choice of counsel is addressed in Ch 13.

clxvi Note that *International Criminal Court Act 2002* (Cth), Sch 1, Art 63 provides that the accused shall be present during the trial. However, if the accused disrupts the trial, the 'Trial Chamber may remove the accused and shall make provision for him or her to observe the trial and instruct counsel from outside the courtroom, through the use of communications technology, if required. Such measures shall be taken only in exceptional circumstances after other reasonable alternatives have proved inadequate, and only for such duration as is strictly required'.

clxvii The provision of legal aid services is discussed in Ch 13.

clxviii Art 4 of the ICCPR allows State Parties to take measures that derogate from their obligations under the Covenant in a 'time of public emergency which threatens the life of the nation' provided that such measures are not inconsistent with their other obligations under international law and are not discriminatory. Note also that the Convention on the Rights of the Child, Art 40(2)(b)(ii) contains a guarantee that every child accused of having infringed the penal law is entitled to 'be informed promptly and directly of the charges against him or her, and, if appropriate, through his or her parents or legal guardians, and to have legal or other appropriate assistance in the preparation and presentation of his or her defence'.

clxix *Dietrich v The Queen* (1992) 177 CLR 292, 362–364.

clxx *Brown v R* (1986) 160 CLR 171.

clxxi M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 536.

clxxii *R v Lappas and Dowling* (ACTSC, Gray J, 26 November 2001). In July 2000 Lappas was charged with official secrets offences under *Crimes Act 1914* (Cth), s 79(2). In 2001 additional espionage charges were brought under *Crimes Act 1914* (Cth), s 78(1): Department of the Parliamentary Library Information and Research Services, *Bills Digest No 117: Criminal Code Amendment (Espionage and Related Offences) Bill 2002*, Appendix. The *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth), Sch 1 repealed *Crimes Act 1914* (Cth), s 78. The offence of espionage has now been transferred to *Criminal Code Act 1995* (Cth), ch 5. The second count on the indictment of Lappas alleged that he, for a purpose intended to be prejudicial to the safety or defence of the Commonwealth, communicated to an unauthorised person two documents that were intended to be directly or indirectly useful to a foreign power. This case is also discussed in Ch 8 in the discussion on public interest immunity.

clxxiii *R v Lappas and Dowling* (ACTSC, Gray J, 26 November 2001), para 14.

clxxiv Ibid, para 24.

clxxv Ibid, para 21.
clxxvi Ibid, para 18–19.
clxxvii *Tan v Cameron* [1992] 2 AC 206.
clxxviii For example, the *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(e)(2) provides that, if the government refuses to disclose classified information and a defendant is prevented from disclosing or causing the disclosure of classified information, the court shall dismiss the indictment. However, where the court determines that dismissal of the indictment will not serve the interests of justice, it may instead dismiss specified counts of the indictment, find against the government on any issue to which the classified information relates, or strike or preclude all or part of the testimony of a witness.
clxxix M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 537. The circumstances in which a stay has been granted include where pre-charge and post-charge delay is likely to prevent a fair trial (*Jago v District Court (NSW)* (1989) 168 CLR 23; *Adler v District Court (NSW)* (1990) 19 NSWLR 317; *Aitchison v DPP* (31 October 1996, Supreme Court of the ACT, unreported)); where delay meant that medical records were destroyed (*R v Davis* (1995) 57 FCR 512); where an accused facing charges for serious indictable offences is without legal representation through no fault of his own (*Dietrich v The Queen* (1992) 177 CLR 292 and *Craig v South Australia* (1995) 131 ALR 595); and where pre-trial publicity is likely to prevent a fair trial: (*R v Connell (No 3)* (1993) 8 WAR 542).
clxxx I Munro, 'Fight Looms on Security Checks', *The Age* (Melbourne), 5.
clxxxi The Victorian Bar, *Submission CSSI 1*, 8 April 2002. The Victorian Attorney-General, Mr Robert Hulls, has stated that 'an undertaking to the court (to guard confidences) has been appropriate in the past and a breach of that undertaking is a contempt of court.': I Munro, 'Fight Looms on Security Checks', *The Age* (Melbourne), 5.
clxxxii New South Wales Bar Association, *Submission CSSI 2*, 11 April 2003.
clxxxiii Hall & Wilcox Lawyers, *To Discover or Not To Discover ... That is the Question? (in Weekly Words of Wisdom)*, <www.hallandwilcox.com.au/pages/news/weekly_wisdom_pdf_weekly%20words%207.3.2003.pdf>, 7 March 2003. The redaction, or editing out, of sensitive information is considered in Ch 6 and 7.
clxxxiv For example, in the recent spy trial of Brian Regan in the USA, two national security experts for the defence testified that the intelligence that Regan was carrying when he was arrested could not have harmed the USA if sold to a foreign government: *Spy Suspect Was Harmless, Witnesses Say*, The Miami Herald, <www.miami.com/mld/miamiherald/news/nation/5125499.htm>, 7 February 2003.
clxxxv Australian Government Solicitor, *Legal Briefing Number 56: Contempt of Court—How it Can Affect You*, <www.ags.gov.au/publications/briefings/br56.html>, 25 June 2000.
clxxxvi Ibid. See also Federal Court Rules, O 35 r 11, which sets out the order the Court can make where a person fails to fulfil a binding undertaking to the Court following a motion by any party for such order. The rule does not affect the powers of the Court to punish a person for contempt.

clxxxvii See *McCabe v British American Tobacco Australia Services Limited* [2002] VSC 150. See also *Eltran Pty Ltd v Westpac Banking Corporation (*1990) 98 ALR 141 and *Sentry Corporation v Peat Marwick Mitchell & Co* (1990) 24 FCR 463.
clxxxviii Federal Court Rules, O 15 r 18.
clxxxix See, for example, the discussion below under the heading 'Hearings closed to the public' on *Crimes Act 1914* (Cth), s 85B(1)(b) and (c) in relation to in camera hearings.
cxc Human Rights Watch, *Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees* (2002), Human Rights Watch, New York, see <www.hrw.org/reports/2002/us911/USA0802.pdf>, 27.
cxci Ibid, 27.
cxcii Ibid, 28.
cxciii Department of Defense (USA), *Military Commission Instruction No 5*, 30 April 2003. These instructions are ready for the trial of alleged war criminals by US military commissions if US President Bush decides to name individuals to be considered for prosecution.
cxciv *Dickason v Dickason* (1913) 17 CLR 50, 51, 54.
cxcv *Scott v Scott* [1913] AC 417, 473.
cxcvi *Dickason v Dickason* (1913) 17 CLR 50, 51.
cxcvii *Russell v Russell* (1976) 134 CLR 495. The legislation in issue was the *Family Law Act 1975* (Cth), s 97(1).
cxcviii Ibid, 520–521.
cxcix The Hon JJ Spigelman, 'Seen To Be Done: The Principles of Open Justice—Part 1' (2000) 74 *Australian Law Journal* 290, 292 and generally.
cc See G Nettheim, 'Open Justice and State Secrets' (1986) 10 *Adelaide Law Review* 281, 1.
cci The Hon JJ Spigelman, 'Seen To Be Done: The Principles of Open Justice—Part 1' (2000) 74 *Australian Law Journal* 290, 294 [citations omitted].
ccii For example, in the case of Jack Roche, who is accused of plotting to bomb the Israeli embassy in Canberra with three al-Qaeda members, a suppression order in the Western Australia District Court prohibited publication of the police statement of facts, Mr Roche's statement and witness statements: M Russell and N Lawton, 'Top Al-Qaeda "in Canberra Plot"', *The Courier Mail* (Brisbane), 2 May 2003, 7.
cciii C Maher, 'The Right to a Fair Trial in Criminal Cases Involving the Introduction of Classified Information' (1988) 120 *Military Law Review* 83, 125. The closure of criminal proceedings is discussed in Ch 9.
cciv H Selby, 'A Middle Way to Countering Terror', *The Canberra Times*, 11.
ccv This section was introduced into the *Criminal Code Act 1995* (Cth) by *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth). Ch 2 of the *Criminal Code* (a schedule to the *Criminal Code Act 1995* (Cth)) sets out the general principles of criminal responsibility that apply to all offences against the *Crimes Act 1914* (Cth): *Crimes Act 1914* (Cth), s 3BA.
ccvi A person who contravenes an order made, or a direction given, under the section commits an offence, the penalty for which is imprisonment for 5 years: *Criminal Code Act 1995* (Cth), s 93.2(3).

ccvii *Criminal Code Amendment (Espionage and Related Matters) Act 2002* (Cth), s 90.1 provides that 'security or defence of a country includes the operations, capabilities and technologies of, and methods and sources used by, the country's intelligence or security agencies'. The Revised Explanatory Memorandum to the Criminal Code Amendment (Espionage and Related Matters) Bill states that by 'extending the application of this provision to take account of security interests, clause 93.2 responds to the changing nature of the security and defence environment, which has also influenced other provisions in the Bill'.

ccviii The ALRC is expressly required to consider the operation of s 85B of the *Crimes Act 1914* (Cth) by the Terms of Reference.

ccix Examples of international provisions include the *Rome Statute of the International Criminal Court 1998*, Art 64(7) (which provides that the Trial Chamber may determine that special circumstances require certain proceedings to be in closed session to protect confidential or sensitive information), Art 72(5)(d) and 72(7)(a)(i) (which provide for in camera or ex parte hearings to protect national security information); *Criminal Code [RS 1985, c C-46] 1985* (Canada), s 486(1); *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6; *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001* (USA), s 106 and 411; and *Official Secrets Act 1989* (UK), s 11(4).

ccx See also *Federal Magistrates Act 1999* (Cth), s 13(7); *Service and Execution of Process Act 1992* (Cth), s 127(4); *Defence (Special Undertakings) Act 1952* (Cth), s 31 and *Nuclear Non-Proliferation (Safeguards) Act 1987* (Cth), s 40.

ccxi Department of the Parliamentary Library Information and Research Services, *Bills Digest No 117: Criminal Code Amendment (Espionage and Related Offences) Bill 2002*, Appendix.

ccxii See *Milosevic Complains about Closed Court Sessions*, AFP,<http://news.suc.org/bydate/2002/October_24/3.html>, where it is reported that the war crimes trial of Milosevic has been largely held in closed session—the public galleries are closed and the testimony of witnesses cannot be revealed.

ccxiii *Complaints (Australian Federal Police) Act 1981* (Cth), s 74(1).

ccxiv Ibid, s 74(2).

ccxv Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, C 31–32 para 6.29–6.34. See also Ch 3.

ccxvi M Nowak, *UN Covenant on Civil and Political Rights: CCPR Commentary* (1993) NP Engel, 212.

ccxvii See Ch 11. In the United States there is also the issue of whether camera coverage of terrorism trials should be allowed. Families and victims of attacks on the World Trade Centre and the Pentagon are allowed to watch the trial of Zacarias Moussaoui (an alleged co-conspirator in those attacks) by closed circuit television pursuant to legislation: L Dalgish, G Leslie and P Taylor (eds), *RCFP White Paper Homefront Confidential Second Edition: How the War on Terrorism Affects Access to Information and the Public's Right to Know*, The Reporters Committee For Freedom of the Press, <www.rcfp.org/homefrontconfidential/index.html>, 1 September 2002.

ccxviii *Supreme Court Act 1935* (SA), s 131(1).

ccxix Ibid, s 131(2).
ccxx Ibid, s 131(3).
ccxxi *Supreme Court Rules* (NT), r 81A.39(1) and (5).
ccxxii *Explanatory Notes to Anti-Terrorism, Crime and Security Act 2001* (UK), point 3.
ccxxiii *Anti-Terrorism Crime and Security Act 2001* (UK), s 64. Schedule 5 of the Act lists the relevant pathogens and toxins. Section 58(3) of the Act provides that the Secretary of State may not add any pathogen or toxin to the Schedule 'unless he is satisfied that the pathogen or toxin could be used in an act of terrorism to endanger life or cause serious harm to human health.'
ccxxivIbid, s 70.
ccxxv Ibid, Sch 6, s 5(2)(b) provides that, in making rules, the Lord Chancellor shall have regard to the need to ensure 'that information is not disclosed contrary to the public interest'.
ccxxvi*Special Immigration Appeals Commission Act 1997* (UK), s 5(3)(b).
ccxxvii Ibid, 5(6)(b).
ccxxviii Ibid, s 6(1).
ccxxixIbid, s 6(4). There are other legislative provisions denying certain individuals access to particular information in proceedings not involving national security. For example, under the *Mental Health Act 1990* (NSW), s 276(3), a legal representative before the Mental Health Tribunal must have regard to a warning given by a medical practitioner that it may be harmful to communicate to a specified person certain information contained in medical records; and the lawyer is not then obliged to disclose that information to that person.
ccxxx See *Special Immigration Appeals Commission (Procedure) Rules 2003* (UK), Rule 37, which provides that the Secretary of State may not rely upon 'closed material' being material that the Secretary of State wishes to rely upon in proceedings before the Commission, but which the Secretary of State objects to disclosing to the appellant or his representative, unless a special advocate has been appointed to represent the interests of the appellant. The Secretary of State must file with the Commission, and serve on the special advocate 'a) a copy of the closed material; b) a statement of his reasons for objecting to its disclosure; and c) if and to the extent that it is possible to do so without disclosing information contrary to the public interest, a statement of the material in a form which can be served on the appellant.'
ccxxxiExcept for reasons such as the lawyer's conflict of interest or being a witness in his or her client's matter.
ccxxxii M Creppy, *Memorandum from M Creppy, Chief Immigration Judge to All Immigration Judges and Court Administrators attaching Instructions for Cases Requiring Additional Security*, 21 September 2001. See also *In re Washington Post Co* 807 F2d 383 (4th Cir, 1986), a civilian federal case where the public was excluded from virtually all of the criminal proceedings: a plea hearing and a sentence hearing. On motion, the hearings were not reflected in the court docket. The Fourth Circuit found that the District Court had failed to give adequate notice to the public of the pending closure and had not taken reasonable steps to allow members of the public

who wanted to attend an opportunity to comment upon or object to the court's closure: *In re Washington Post Co* 807 F2d 383 (4th Cir, 1986), 390.

ccxxxiii Human Rights Watch, *Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees* (2002), Human Rights Watch, New York, see <www.hrw.org/reports/2002/us911/USA0802.pdf>, 30.

ccxxxiv Ibid, 5.

ccxxxv See ICCPR, Art 14(3) set out in Ch 5.

ccxxxvi The INS was dissolved on 1 March 2003. Its enforcement and service functions were transferred to the new US Department of Homeland Security: Lawyers Committee for Human Rights, *Imbalance of Powers—How Changes to US Law & Policy Since 9/11 Erode Human Rights and Civil Liberties (Abridged version)* (September 2002–March 2003), New York, see <www.lchr.org/pubs/descriptions/imbalance_digest.pdf>, 14.

ccxxxvii D Cole, *Statement of Professor David Cole, Georgetown University Law Center on the Use of Secret Evidence in Immigration Proceedings and HR 2121 before the House Judiciary Committee*, <www.fas.org/sgp/congress/2000/cole.html>, 23 May 2000, 2.

ccxxxviii Ibid, 6.

ccxxxix Ibid, 2.

ccxl Ibid, 10.

ccxli Ibid, 2.

ccxlii Ibid, 7.

ccxliii Ibid, 11–12.

ccxliv Ibid, 3–4. This was in the matter of Hany Kiareldeen, who spent 19 months in prison 'solely on the basis of secret evidence—an uncorroborated bare-bones hearsay report that neither he nor his lawyers ever had an opportunity to see': D Cole, *Statement of Professor David Cole, Georgetown University Law Center on the Use of Secret Evidence in Immigration Proceedings and HR 2121 before the House Judiciary Committee*, <www.fas.org/sgp/congress/2000/cole.html>, 23 May 2000, 3.

ccxlv Secret Evidence Repeal Bill 2001 (USA).

ccxlvi K Snyder, 'A Clash of Values: Classified Information in Immigration Proceedings' (2002) 88(2) *Virginia Law Review* 447, 472.

ccxlvii Ibid, 450. See also the discussion of the Alien Terrorist Removal Court, which allows the use of secret information to remove aliens, in Ch 12.

ccxlviii See ICCPR, Art 14 set out in para 5.4 and 5.9.

ccxlix Of course, a statement of reasons is not given at the verdict stage of a criminal trial as all the jury is required to pronounce is whether the accused is guilty or not guilty in respect of each count on the indictment. However, statements of reasons for judgment should be given in civil and administrative hearings, and in relation to interlocutory applications in criminal proceedings, including decisions on the admission or exclusion of evidence.

ccl *Special Immigration Appeals Commission Act 1997* (UK), s 5(3)(a).

ccli *Anti-Terrorism Crime and Security Act 2001* (UK), Sch 6, s 5(3)(a). 'Denial of access' refers to a direction made by the UK Secretary of State, in the interests of

national security, to deny access to the occupier of any relevant premises to certain pathogens and toxins as set out in the Act: s 64.

Chapter 6

cclii *Crimes Act 1914* (Cth), s 23V(1)(a).
ccliii Ibid, s 23V(1)(b).
ccliv Ibid, s 23V(1)(b).
cclv Where both an audio and video recording are made, the audio recording or a copy of it is to be made available to the person or his or her legal representative, and the investigating official is to inform them that an opportunity will be provided, on request, for viewing the video recording: Ibid, s 23V(2)(b).
cclvi *Lai-Ha v McCusker* [2000] FCA 1173 (Emmett J).
cclvii *Crimes Act 1914* (Cth), s 23V(5).
cclviii Ibid, s 23V(6).
cclix Ibid, s 23V(7).
cclx Commonwealth Director of Public Prosecutions, *Statement on Prosecution Disclosure*, <www.cdpp.gov.au/cdpp/StatementOnProsecutionDisclosure.pdf>, E2.
cclxi For example, Judge Lamberth gives the example of substituting the fact that the USA has a CIA station in a particular country (which is probably classified because it would impair the foreign relations with that country if it were disclosed) with the information that the USA has a CIA station in a 'foreign country, or even in a Latin American country': R Lamberth, *An Interview with Judge Royce C Lamberth*, Administrative Office of the US Courts, <www.uscourts.gov/ttb/june02ttb/interview.html>, 1 June 2002.
cclxii The *Evidence Act 1985* (Cth), s 48(1)(a) provides that a party may adduce evidence of the contents of a document by adducing evidence of an admission made by another party to the proceeding as to the contents of the document in question, although s 48(3) limits the use of such evidence.
cclxiii Commonwealth Director of Public Prosecutions, *Statement on Prosecution Disclosure*, <www.cdpp.gov.au/cdpp/StatementOnProsecutionDisclosure.pdf> F13 provides: 'Where part only of a witness statement contains sensitive material in some cases it may be appropriate to request the witness to make a second statement omitting the sensitive material. The second statement will then be disclosed to the defence, either as part of the prosecution case or because it is unused material, and the defence informed that the first statement is withheld on the ground that it is subject to public interest immunity'.
cclxiv Professor David Cole has been critical of the standard of declassified summaries of secret evidence provided by the US Immigration and Naturalization Service to aliens, stating that the summaries 'are often so general as to be entirely unhelpful'. He advocates the use of summaries which would give aliens 'a meaningful opportunity to respond': D Cole, *Statement of Professor David Cole, Georgetown University Law Center on the Use of Secret Evidence in Immigration Proceedings and HR 2121 before the House Judiciary Committee*, <www.fas.org/sgp/congress/2000/cole.html>, 23 May 2000. This raises the issue of whether there should be a legislative standard set for such

summaries. The *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(c) sets the standard in criminal matters that such a summary must provide the defendant 'with substantially the same ability to make his defense as would disclosure of the specified classified information'.

cclxv *Classified Information Procedures Act 18 USC App 1–16 1982* (USA).

cclxvi See *United States v Baptista-Rodriguez*, 17 F.3d 1354, 1363 (11th Cir, 1994).

cclxvii *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 4; Department of Justice (USA), *Criminal Resource Manual*, <www.usdoj.gov/usao/eousa/foia_reading_room/usam> 2054, Synopsis of Classified Information Procedures Act.

cclxviii Department of Justice (USA), *Criminal Resource Manual*, <www.usdoj.gov/usao/eousa/foia_reading_room/usam> 2054, Synopsis of Classified Information Procedures Act.

cclxix *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 5(a). All classified information to be relied upon must be identified, regardless of whether it is contained in documents or anticipated testimony: see *United States v North 708 F Supp 399 (DDC, 1988)*, 399–400.

cclxx *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 5(b).

cclxxi Ibid, s 6(b)(1). 'When the United States has not previously made the information available to the defendant … the information may be described by generic category, in such forms as the court may approve, rather than identification of the specific information of concern to the United States': *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(b)(1).

cclxxii *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(a).

cclxxiii Ibid, s 6(c).

cclxxiv Ibid, s 6(c). In *United States v Fernandez* 913 F.2d 148 (4th Cir, 1990) and in *United States v North* 708 F Supp 399 (DDC, 1988) the court ultimately rejected the proposed substitutions for relevant classified information, thereby 'derailing the prosecutions': See S Pilchin and B Klubes, 'Using the Classified Information Procedures Act in Criminal Cases: A Primer for Defense Counsel' (1994) 31 *American Criminal Law Review* 191, 212–213. The government may institute an interlocutory appeal from a court order rejecting substitutions, summaries or admissions of relevant classified information: *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(e)(2).

cclxxvDepartment of Justice (USA), *Criminal Resource Manual*, <www.usdoj.gov/usao/eousa/foia_reading_room/usam> 2054, Synopsis of Classified Information Procedures Act.

cclxxvi *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(f).

cclxxvii S Pilchin and B Klubes, 'Using the Classified Information Procedures Act in Criminal Cases: A Primer for Defense Counsel' (1994) 31 *American Criminal Law Review* 191, 208 (citations omitted).

cclxxviii K Martin, *The Right to a Fair Trial in the United States when Official Secrets are Involved*,<www.hfhrpol.waw.pl/Secserv/fairtrial_us.html>.

cclxxix *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 6(d). The defendant may seek reconsideration of a court's determination prior to or during the trial.
cclxxxThe case of Zacarias Moussaoui is discussed further in Ch 9.
cclxxxi J Markon, *US Files Terror Briefs in Secrecy*, Washington Post, <www.washingtonpost.com/ac2/wp-dyn/A27772-2003Mar13.html>, 27 March 2003.
cclxxxii The text of the First Amendment to the US Constitution is set out in Ch 2, fn xlviii.
cclxxxiii P Shenon, *Some Secret Documents in Terror Case Can Be Unsealed*, The New York Times,<www.nytimes.com/2003/04/22/international/world special/22SUSP.html>, 21 April 2003.
cclxxxiv Ibid.
cclxxxv D Russakoff, 'NJ Judge Unseals Transcript In Controversial Terror Case', *The Washington Post*, 25 June 2003, A03.
cclxxxvi *Uniting and Strengthening America by Providing Appropriate Tools Required to Intercept and Obstruct Terrorism Act 2001* (USA), s 223 amends (among other sections) Chapter 121 of Title 18 of the United States Code.
cclxxxvii Ibid, s 411 amends (among other sections) s 219 of the *Immigration and Nationality Act* (8 USC s 1189).

Chapter 7

cclxxxviiiPublic interest immunity is discussed in Ch 8.
cclxxxix *R v Lappas and Dowling* (ACTSC, Gray J, 26 November 2001), para 2. See also discussion of case in Ch 5 and 8.
ccxc Ibid, para 2.
ccxci *Jury Begins Deliberating in Regan Espionage Case*, Associated Press, <www.sunspot.net/news/nationworld/bal-te.espionage11feb11,0,69298464.story?c...>, 11 February 2003.
ccxcii 'Approved officer' and 'approved person' are defined in *Crimes Act 1914* (Cth), s 15XA.
ccxciii'Authorisation' is defined in s 15XA as an authorisation that is in force under s 15XG or 15XH of the Act.
ccxciv*Crimes Act 1914* (Cth), s 15XT(2) provides that the section does not apply to the extent that the court, tribunal or commission considers that the interests of justice require otherwise.
ccxcv E Magner, 'Is a Terrorist Entitled to the Protection of the Law of Evidence?' (1988) 11(3) *Sydney Law Review* 537, 558.
ccxcviI Leigh, 'Secret Proceedings in Canada' (1996) 34 *Osgoode Hall Law Journal* 113, 118.
ccxcvii See E Magner, 'Is a Terrorist Entitled to the Protection of the Law of Evidence?' (1988) 11(3) *Sydney Law Review* 537, 559 and H Reiter, 'Hearsay Evidence and Criminal Process in Germany and Australia' (1984) 10 *Monash University Law Review* 51, 69–70.

ccxcviii H Reiter, 'Hearsay Evidence and Criminal Process in Germany and Australia' (1984) 10 *Monash University Law Review* 51, 69–70.

ccxcix Ibid, 70 citing the summary of the decision in W Zeidler, 'Court Practice and Procedure under Strain: A Comparison' (1982) 8 *Adelaide Law Review* 150, 158.

ccc E Magner, 'Is a Terrorist Entitled to the Protection of the Law of Evidence?' (1988) 11(3) *Sydney Law Review* 537, citing the summary of the decision in W Zeidler, 'Court Practice and Procedure under Strain: A Comparison' (1982) 8 *Adelaide Law Review* 150, 158. The European Court of Human Rights also dismissed a complaint about a similar procedure used by Austrian courts with regard to undercover agents. The petitioner alleged a violation of the European Convention on Human Rights, Art 6(3)(d), which protects an accused's right 'to examine or have examined witnesses against him and to obtain the attendance and examination of witnesses on his behalf under the same conditions as witnesses against him' in an Austrian criminal trial. The European Court dismissed the petition as the Austrian court had assessed the hearsay evidence with proper care and had not based its findings exclusively on the hearsay testimony. Reiter expresses the view that an out-of-court examination by a delegated judge would be a preferable way of obtaining evidence from undercover agents, with the result of the examination being subsequently produced during the hearing: H Reiter, 'Hearsay Evidence and Criminal Process in Germany and Australia' (1984) 10 *Monash University Law Review* 51, 70–71.

ccci See International Covenant on Civil and Political Rights, Art 14(3)(e) set out in Ch 5.

cccii *Witness Gag Order Holds up Zimbabwe Treason Trial*, <www.sabcnews.co.za/africa/southern_africa/0,1009,52783,00.html>, 11 February 2003, and C Chinaka, *Zimbabwe Seeks Gag on Deal with Treason Witness*, Reuters, <http://famulus.msnbc.com/FamulusIntl/reuters02-10-051733.asp?reg=AFRICA>, 10 February 2003.

ccciii S Mapenzauswa, *Zimbabwean Judge Overrules Gag Order, Trial Resumes*, Reuters, <http://famulus.msnbc.com/FamulusIntl/reuters02-12-115203.asp?reg=AFRICA>, 12 February 2003.

Chapter 8

ccciv M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 597.

cccv *R v Lappas and Dowling* (ACTSC, Gray J, 26 November 2001).

cccvi *Sankey v Whitlam* (1978) 142 CLR 1, 38 (Gibbs ACJ).

cccvii A Ligertwood, *Australian Evidence* (3rd ed, 1998) Butterworths, 350.

cccviii M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 597.

cccix *Cooke v Maxwell* (1817) 171 ER 614, 615.

cccx J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, 474.

cccxi Australian Law Reform Commission, *Evidence*, Vol 2, ALRC 26 (Interim) (1985), Australian Government Publishing Service, Canberra.
cccxii Ibid, 490.
cccxiii Ibid, 491, citing *Alister v R* (1983) 50 ALR 41, 44–45 (Gibbs CJ).
cccxiv Ibid, 491.
cccxv *Evidence Act 1985* (Cth), s 130(4).
cccxvi J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, 470.
cccxvii *State of NSW v Ryan* (1998) 101 LGERA 246.
cccxviii *Sankey v Whitlam* (1978) 142 CLR 1.
cccxix J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, 472.
cccxx *Chapman v Luminis Pty Ltd (No 2)* (2000) 100 FCR 229.
cccxxi *Aboriginal Sacred Sites Protection Authority v Maurice* (1986) 10 FCR 104.
cccxxii J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, 475.
cccxxiii S Odgers, *Uniform Evidence Law* (4th ed, 2000) LBC Information Services, Sydney, 343.
cccxxiv J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, 469.
cccxxv Ibid, 471.
cccxxvi *Scott v Scott* [1913] AC 417, cited in A Ligertwood, *Australian Evidence* (3rd ed, 1998) Butterworths, 368.
cccxxvii *R v Mr C (1993)* 67 A Crim R 562, cited in Ibid, 368.
cccxxviii *Church of Scientology of California v DHSS* [1979] 1 WLR 723, cited in Ibid, 368.
cccxxix S Odgers, *Uniform Evidence Law* (4th ed, 2000) LBC Information Services, Sydney, 342.
cccxxx M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 599.
cccxxxi J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, 468. For example, in relation to civil proceedings, see *Supreme Court Rules* (NSW), Pt 23 (Discovery and Inspection of Documents).
cccxxxii S Odgers, *Uniform Evidence Law* (4th ed, 2000) LBC Information Services, Sydney, 341.
cccxxxiii *R v Young* (1999) 46 NSWLR 681, 693, cited in J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, 471.
cccxxxiv S Odgers, *Uniform Evidence Law* (4th ed, 2000) LBC Information Services, Sydney, 342.

cccxxxv J Anderson, J Hunter and N Williams, *The New Evidence Law: Annotations and Commentary on the Uniform Evidence Acts* (2002) Lexis Nexis Butterworths, Chatswood, 471.
cccxxxvi A Ligertwood, *Australian Evidence* (3rd ed, 1998) Butterworths, 352.
cccxxxvii M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 599.
cccxxxviii A Ligertwood, *Australian Evidence* (3rd ed, 1998) Butterworths, 353.
cccxxxix *Sankey v Whitlam* (1978) 142 CLR 1, 44 (Gibbs ACJ).
cccxl M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 597.
cccxli *Alister v R* (1983) 50 ALR 41, 81 (Brennan J). Public interest immunity in civil proceedings is discussed further in Ch 10.
cccxlii S McNicol, *Law of Privilege* (1992) Law Book Co, Sydney, 394–5.
cccxliii *Alister v R* (1983) 50 ALR 41, 81 (Brennan J).
cccxliv *Marks v Beyfus* (1890) 25 QBD 494, 498 (Lord Esher MR), cited in *Sankey v Whitlam* (1978) 142 CLR 1.
cccxlv *D v National Society for the Prevention of Cruelty to Children* [1978] AC 232, 232 (Lord Simon of Glaisdale), cited in *Sankey v Whitlam* (1978) 142 CLR 1, 62.
cccxlvi *Sankey v Whitlam* (1978) 142 CLR 1.
cccxlvii *Rogers v Home Secretary* (1973) AC 388, 407, cited in D Byrne and J Heydon, *Cross on Evidence: Australian Edition* (1996) Butterworths, Sydney, [27043].
cccxlviii *R v Keane* [1994] 2 All ER 478, cited in Ibid, [27043].
cccxlix I Leigh, *Reforming Public Interest Immunity*, Journal of Current Legal Issues, <www.webjcli.ncl.ac.uk/articles2/leigh2.html>, 12 June 2003, 4.
cccl Ibid, 4.
cccli *Sankey v Whitlam* (1978) 142 CLR 1, 57 (Stephen J).
ccclii *Alister v R* (1983) 50 ALR 41, 64 (Wilson and Dawson JJ).
cccliii Ibid, 64 (Wilson and Dawson JJ).
ccccliv S McNicol, *Law of Privilege* (1992) Law Book Co, Sydney, 406.
ccclv I Leigh, *Reforming Public Interest Immunity*, Journal of Current Legal Issues, <www.webjcli.ncl.ac.uk/articles2/leigh2.html>, 12 June 2003, 5.
ccclvi See *Duncan v Cammell, Laird & Co* [1942] AC 264, discussed in M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 598.
ccclvii M Aronson and J Hunter, *Litigation Evidence and Procedure* (6th ed, 1998) Butterworths, 598.
ccclviii *Conway v Rimmer* [1968] AC 910.
ccclix *Sankey v Whitlam* (1978) 142 CLR 1, 38–39 (Gibbs ACJ). See also *Alister v R* (1983) 50 ALR 41, 64 (Wilson and Dawson JJ), as cited in A Ligertwood, *Australian Evidence* (3rd ed, 1998) Butterworths, 352.
ccclx A Ligertwood, *Australian Evidence* (3rd ed, 1998) Butterworths, 354.

Chapter 9

ccclxi For example, prosecutors have challenged a court order allowing Moussaoui access to an al-Qaeda prisoner believed to have information important to the defence

on the basis that such access could harm a sensitive key interrogation: *Moussaoui Can Be Tried in Civilian Court*,<www.courttv.com/trials/moussaoui/041503_ap.html>, 15 April 2003. In June 2003, the US Circuit Court of Appeals for the 4th Circuit dismissed the prosecution's appeal in this regard, albeit on a technicality, ruling that the court order could not be appealed 'unless and until the government refuses to comply and the District Court imposes a sanction': *Moussaoui May Question Witness, Appeal Court Says*, The Associated Press, <www.nytimes.com/aponline/national/AP-Moussaoui-Witness.html>,26 June 2003.

cccclxii*Moussaoui Crafts a Defense as Judge Appears to Listen*, <www.courttv.com/trials/moussaoui/042303_defense_ap.html>, 23 April 2003.

cccclxiii *Moussaoui Can Be Tried in Civilian Court*, <www.courttv.com/trials/moussaoui/041503_ap.html>, 15 April 2003.

cccclxiv A recent example of a case involving an intelligence official is that of former FBI agent James Smith, who has been charged with gross negligence in allowing a prominent Chinese businesswoman access to classified documents: G Krikorian, D Rosenzweig and C Kang, 'Ex-FBI Agent is Arrested in China Espionage Case', *Los Angeles Times*, 10 April 2003, <www.latimes.com/news/local/la-me-spy10apr10,1,6136128.story?=coll=la%2Dhome%2Dleftrail>.

cccclxvL Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994) Clarendon Press, Oxford, 292.

cccclxvi Ibid, 292.

cccclxvii E Magner, 'Is a Terrorist Entitled to the Protection of the Law of Evidence?' (1988) 11(3) *Sydney Law Review* 537, 537.

cccclxviii Ibid, 546, 548.

cccclxix Public interest immunity is discussed in Ch 8.

cccclxxE Magner, 'Is a Terrorist Entitled to the Protection of the Law of Evidence?' (1988) 11(3) *Sydney Law Review* 537, 550.

cccclxxi Australian Federal Police Commissioner Mick Keelty has called for the creation of an international court of terrorism with special powers for terrorism suspects, possibly modelled on drug courts which specifically deal with addicts. D Goodsir, 'Police Call for World Court on Terrorism', *The Sydney Morning Herald*, 29 April 2003, 3.

cccclxxii G Bush, 'Military Order of November 13, 2001: Detention, Treatment, and Trial of Certain Non-Citizens in the War against Terrorism' (2001) 66(222) *Federal Register* 57833.

cccclxxiii See also Ch 5 and the observations at para 5.30–5.31 in relation to closing Australian courts.

cccclxxiv The text of the First Amendment is set out in Ch 2, fn xlviii.

cccclxxv *Globe Newspaper Co v Superior Court* 457 US 596 (Supreme Court of USA, 1982); *United States v Cojab* 996 F2d 1404 (2d Cir, 1993).

cccclxxvi *Press-Enterprise Co v Superior Court (Press-Enterprise I)* 464 US 501 (1984); *Press-Enterprise v Superior Court (Press-Enterprise II)* 478 US 1 (1986) as cited in The Reporters Committee for Freedom of the Press, *Secret Justice: Access to*

Terrorism Proceedings, The Reporters Committee for Freedom of the Press, <www.rcfp.org/secretjustice/terrorism/index.html>, Winter 2002.

ccclxxvii *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 12(a). Note that such guidelines are to be transmitted to the appropriate committees of Congress.

ccclxxviii Department of Justice (USA), *Attorney General's Guidelines for Prosecutions Involving Classified Information*, 1981, as cited in S Pilchin and B Klubes, 'Using the Classified Information Procedures Act in Criminal Cases: A Primer for Defense Counsel' (1994) 31 *American Criminal Law Review* 191, 195–196.

ccclxxix Department of Justice (USA), *Attorney General's Guidelines for Prosecutions Involving Classified Information*, 1981, 2, 4–6, cited in S Pilchin and B Klubes, 'Using the Classified Information Procedures Act in Criminal Cases: A Primer for Defense Counsel' (1994) 31 *American Criminal Law Review* 191, 196.

ccclxxx S Pilchin and B Klubes, 'Using the Classified Information Procedures Act in Criminal Cases: A Primer for Defense Counsel' (1994) 31 *American Criminal Law Review* 191, 196.

ccclxxxi *Classified Information Procedures Act 18 USC App 1–16 1982* (USA), s 12(b).

ccclxxxii Ibid, s 12(b).

ccclxxxiii Commonwealth Director of Public Prosecutions, *Prosecution Policy of the Commonwealth*, <www.cdpp.gov.au/cdpp/prospol.html>.

ccclxxxiv An 'investigating agency' is the Australian Federal Police, the National Crime Authority or other Commonwealth department or agency which conducts investigations into offences against Commonwealth law: Commonwealth Director of Public Prosecutions, *Statement on Prosecution Disclosure*,<www.cdpp.gov.au/cdpp/StatementOnProsecutionDisclosure.pdf>, A2.

ccclxxxv Ibid, F7.

ccclxxxvi Ibid, F7.

ccclxxxvii Ibid, F11.

ccclxxxviii Ibid, F12.

ccclxxxix Ibid, Section D.

cccxc In the prosecution of John Walker Lindh in the USA, the government had requested permission to have witnesses, particularly military personnel, testify without revealing their real identity: L Dalgish, G Leslie and P Taylor (eds), *RCFP White Paper Homefront Confidential Second Edition: How the War on Terrorism Affects Access to Information and the Public's Right to Know*, The Reporters Committee For Freedom of the Press, <www.rcfp.org/homefrontconfidential/index.html>, 1 September 2002. Lindh later entered into a plea agreement.

Chapter 10

cccxci G Nettheim, 'Open Justice and State Secrets' (1986) 10 *Adelaide Law Review* 281, 293. See also the discussion of discovery of documents in Ch 6.

cccxcii *Church of Scientology v Woodward* (1982) 154 CLR 25.

cccxciii Ibid, 59.

cccxciv Ibid, 59.
cccxcv Ibid, 76.
cccxcvi *Alister v R* (1983) 50 ALR 41, 46 (Gibbs CJ) citing *Air Canada v Secretary of State for Trade* [1983] 2 WLR 529 (Lord Wilberforce). See also the discussion of public interest immunity in Ch 8.
cccxcvii A Ligertwood, *Australian Evidence* (3rd ed, 1998) Butterworths, 366.
cccxcviii *Burmah Oil Co Ltd v Bank of England* [1980] AC 1090, cited in D Byrne and J Heydon, *Cross on Evidence: Australian Edition* (1996) Butterworths, Sydney, 27057.
cccxcix A Ligertwood, *Australian Evidence* (3rd ed, 1998) Butterworths, 337.
cd L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994) Clarendon Press, Oxford, 337.
cdi Ibid, 331.
cdii Ibid, 332.
cdiii *Church of Scientology v Woodward* (1982) 154 CLR 25, 61 cited in G Nettheim, 'Open Justice and State Secrets' (1986) 10 *Adelaide Law Review* 281, 291.

Chapter 11

cdiv See the discussion of definitional issues in Ch 1.
cdv The *Convention Relating to the Status of Refugees* 1951 as amended by the *Protocol Relating to the Status of Refugees* 1967, known collectively as the 'Refugee Convention'.
cdvi S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 404–405.
cdvii D Cole, 'Secrecy, Guilt by Association and the Terrorist Profile' (2001) 15 *Journal of Law and Religion* 267, 277 as cited in S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 405.
cdviii S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 405.
cdix Ibid, 406.
cdx Refugee Convention, Art 33(1).
cdxi Ibid, Art 33(2).
cdxii *Administrative Appeals Tribunal Act 1975* (Cth), s 39A(11) provides that if 'the Director-General of Security so requests, the Tribunal must do all things necessary to ensure that the identity of a person giving evidence on behalf of the Director-General of Security is not revealed'.
cdxiii L Morris, *Case against Muslim Youth*, The Sydney Morning Herald, <www.smh.com.au/articles/2003/03/10/1047144923803.html>, 11 March 2003.
cdxiv *Administrative Appeals Tribunal Act 1975* (Cth), s 35(1).
cdxv Ibid, s 39A(5).
cdxvi M Sassella, 'Reviewing Particular Decisions Made by ASIO: The Security Appeals Division of the Administrative Appeals Tribunal' (Paper presented at Security

in Government Conference, Canberra, 1 April 2002), 6. See also *Administrative Appeals Tribunal Act 1975* (Cth), s 39A(8) and (9).

cdxvii Including persons who have arrived in Australia on valid temporary visas and then invoke Australia's protection obligations.

cdxviii *Migration Regulations 1994* (Cth) Sch 4, Pt 1, 4002.

cdxix See *Director General, Security v Sultan* (1998) 90 FCR 334 and S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 411–412.

cdxx *Director General, Security v Sultan* (1998) 90 FCR 334, 335.

cdxxi Inspector-General of Intelligence and Security, *Annual Report 1999–2000*, 159, as cited in S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 412.

cdxxii S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 410–411, citing Department of Immigration and Multicultural and Indigenous Affairs, *Procedures Advice Manual 3:SCH4/4002* [11.1.4]; Commonwealth, *Parliamentary Debates*, House of Representatives, 6 February 2001, 24015 (Philip Ruddock, Minister for Immigration and Multicultural Affairs).

cdxxiii See *Freedom of Information Act 1982* (Cth), s 7(2A), Sch 2, Pt 1, which provides that ASIO is exempt from the operation of the Act, and other Commonwealth agencies are exempt from the operation of the Act 'in relation to a document that has originated with, or has been received from' ASIO.

cdxxiv ASIO security assessments of Australian citizens or Australian permanent residents must be accompanied by a statement of the grounds for assessment, containing all information relied upon by ASIO in making the assessment, except for information which the Director-General considers to be contrary to the requirements of security: *Australian Security Intelligence Organisation Act 1979* (Cth), s 37(2). However, a statement of grounds may be withheld from an Australian citizen or permanent resident if the Attorney-General has certified in writing that the disclosure would be prejudicial to the interests of security: *Australian Security Intelligence Organisation Act 1979* (Cth), s 38(2)(b). If the Attorney-General has made such a certification, the AAT in conducting a review of the security assessment is precluded from making disclosure of the document to the applicant: *Administrative Appeals Tribunal Act 1975* (Cth), s 39B. The Federal Court is also precluded from disclosing the document in considering an appeal of the AAT decision: *Administrative Appeals Tribunal Act 1975* (Cth), s 46.

cdxxv S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 411.

cdxxvi Ibid, 411, citing Department of Immigration and Multicultural and Indigenous Affairs, *Procedure Advice Manual 3:SCH4/4002* [10.1.3].

cdxxvii The RRT usually has jurisdiction to conduct merits review of a primary stage protection visa refusal. However, the RRT cannot review a decision to refuse a protection visa on the basis of the Refugee Convention, Art 33(2). Only the AAT constituted by a presidential member sitting alone has jurisdiction to review such exclusion decisions: *Migration Act 1958* (Cth), s 500(5) and (1).

cdxxviii Merits review of ASIO security assessments is available to Australian citizens and permanent residents from the Security Appeals Division of the AAT: see *Australian Security Intelligence Organisation Act 1979* (Cth), s 54 and *Administrative Appeals Tribunal Act 1975* (Cth), s 19(6)(a) and 27AA(1). Note the restrictions on review of security assessments contained in *Australian Security Intelligence Organisation Act 1979* (Cth), s 35 and 36.

cdxxix S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 416. Taylor also endorses the suggestion made by the United Nations High Commissioner for Refugees after 11 September 2001 that states establish specialised exclusion units to process the claims of on-shore asylum-seekers suspected of terrorism or serious crimes. Taylor argues that if Australia were to implement this proposal, staff of the exclusion unit should have the same level of security clearance as ASIO officers, and there could be no objection to allowing the protection visa decision maker access to all of the information upon which the security assessment was based: S Taylor, 'Guarding the Enemy from Oppression: Asylum-Seeker Rights Post-September 11' (2002) 26 *Melbourne University Law Review* 396, 415.

cdxxx *Migration Act 1958* (Cth), s 501(4).

cdxxxi M Kenny, 'Terrorism and Exclusion under the Refugee Convention' (2003) (82) *Reform* 37.

cdxxxii *Nationality, Immigration and Asylum Act 2002* (UK).

cdxxxiii Ibid, s 4 amending *British Nationality Act 1981* (UK), s 40A(1) and (2). Note, however, that a person may still appeal against such a decision to the Special Immigration Appeals Commission: see *Nationality, Immigration and Asylum Act 2002* (UK), s 4, amending *Special Immigration Appeals Commission Act 1997* (UK), s 3.

cdxxxiv S O'Hanlon, *Radical Cleric Hamza Faces Dual Threat*, <http://uk.news.yahoo.com/030406/80/dx3oa.html>, 6 April 2003.

cdxxxv Ibid.

cdxxxvi J Hopps, *Blunkett targets 'Un-British' Immigrants*, <http://uk.news.yahoo.com/030401/80/dwqd1.html>, 1 April 2003.

cdxxxvii *Chalal v The United Kingdom* (1996) European Court of Human Rights No 70/1995/576/662.

cdxxxviii See L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994) Clarendon Press, Oxford, ch 7 and I Leigh, 'The Gulf War Deportations and the Courts' (1991) (Aut 1991) *Public Law* 331 for a review of cases before this panel, including the cases of Gulf War deportees. Leigh notes that prior to the Gulf War deportee hearings,' the panel had … received written reports from the Security Service … and dealt with matters arising from the reports in oral questions to officers of the Service. The deportees were excluded from this part of the process and were not informed that it had occurred': I Leigh, 'The Gulf War Deportations and the Courts' (1991) (Aut 1991) *Public Law* 331, 336.

cdxxxix L Lustgarten and I Leigh, *In From the Cold: National Security and Parliamentary Democracy* (1994) Clarendon Press, Oxford, 190–192. In this regard Lustgarten and Leigh note with approval the safeguards present in the Canadian immigration hearings. While confidentiality of security information is maintained by

requiring evidence to be given in the absence of the applicant or his or her representative, security-cleared counsel are used in closed sessions to cross-examine as though representing the applicant, and a summary (subject to redactions) of the evidence given in this way is released to the applicant.

cdxl *Special Immigration Appeals Commission Act 1997* (UK), s 5(3)(b).

cdxli Ibid, s 6(1).

cdxlii Ibid, s 6(4).

cdxliii See the United Kingdom Parliament website at <www.parliament.the-stationery-office.co.uk/pa/cm200102/cmselect/cmhaff/351/351ap20.htm>.

cdxliv *Anti-Terrorism Crime and Security Act 2001* (UK), Part 4, s 21–32.

cdxlv Ibid, Explanatory Notes, ch 24, para 13.

cdxlvi K Snyder, 'A Clash of Values: Classified Information in Immigration Proceedings' (2002) 88(2) *Virginia Law Review* 447, 454–455.

cdxlvii 8 USC § 1225(c).

cdxlviii This scenario arises where an alien has been found to be removable and is seeking to prove that he or she meets the statutory requirements for discretionary relief: see 8 CFR § 240.8(d).

cdxlix In July 2002, in response to a Congressional request for information, the US Department of Justice stated that as at 29 May 2002, 611 persons had been subject to secret hearings, and 419 of them had more than one secret hearing: Human Rights Watch, *Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees* (2002), Human Rights Watch, New York, see<www.hrw.org/reports/2002/us911/USA0802.pdf>, 25.

cdl Immigration judges do not form part of the judicial branch under Article 3 of the US Constitution. They are employees of the Department of Justice.

cdli M Creppy, *Memorandum from M Creppy, Chief Immigration Judge to All Immigration Judges and Court Administrators attaching Instructions for Cases Requiring Additional Security*, 21 September 2001.

cdlii Human Rights Watch, *Presumption of Guilt: Human Rights Abuses of Post-September 11 Detainees* (2002), Human Rights Watch, New York, see <www.hrw.org/reports/2002/us911/USA0802.pdf>, 7.

cdliii *Detroit Free Press v Ashcroft* (US Court of Appeals for the 6th Circuit, Keith and Daughtrey (Circuit Judges) Carr (District Judge), 26 August 2002), 19. The First Amendment to the US Constitution reads: 'Congress shall make no law respecting an establishment of religion, or prohibiting the free exercise thereof; or abridging the freedom of speech, or of the press; or the right of the people peaceably to assemble, and to petition the government for a redress of grievances.'

cdliv Ibid, 15.

cdlv Ibid, 19.

cdlvi Ibid, 19.

cdlvii The Court stated that the government offered no persuasive reason as to why its concerns could not be addressed on a case-by-case basis: Ibid, 21.

cdlviii Ibid, 19.

cdlix Ibid, 2.

cdlx Ibid, 18–19.

cdlxi *Richmond Newspapers, Inc v Virginia* 448 US 555 (1980), 571.
cdlxii *North Jersey Media Group Inc v John Ashcroft, Attorney General of the United States, and Michael Creppy, Chief Immigration Judge of the United States* (US Court of Appeals for the 3rd Circuit, Becker CJ; Scirica and Greenburg JJ, 8 October 2002).
cdlxiii Ibid, 35.
cdlxiv Center for Constitutional Rights, *Supreme Court Declines to Rule on Legality of Closed Immigration Hearings: North Jersey Media Group v Creppy and Ashcroft*, <www.ccr-ny.org/v2/print_page.asp?ObjID=HKR8ebImq1&Content=246>.
cdlxv *Detroit Free Press v Ashcroft* (US Court of Appeals for the 6th Circuit, Keith and Daughtrey (Circuit Judges) Carr (District Judge), 26 August 2002), 12.

Chapter 12

cdlxvi H Evans, 'Public Interest Immunity Claims in the Senate' (2002) 13(1) *Public Law Review* 3, 3. See also S Brown, *Howard Government Can Keep a Secret*, The Brisbane Institute,<www.brisinst.org.au/resources/brown_susan_secret.html>, 13 February 2003.
cdlxvii H Evans (ed), *Odger's Australian Senate Practice Tenth Edition*, Commonwealth of Australia,<www.aph.gov.au/senate/pubs/html/httoc.htm> 399.
cdlxviii Ibid, 420.
cdlxix Ibid, 438.
cdlxx Ibid, 438.
cdlxxi Ibid, (16 July 1975, J831).
cdlxxii H Evans, 'Public Interest Immunity Claims in the Senate' (2002) 13(1) *Public Law Review* 3, 4. Refer to the attitude of the courts to public interest immunity in Ch 8.
cdlxxiii H Evans (ed), *Odger's Australian Senate Practice Tenth Edition*, Commonwealth of Australia, <www.aph.gov.au/senate/pubs/html/httoc.htm>, 482.
cdlxxiv H Evans, 'Public Interest Immunity Claims in the Senate' (2002) 13(1) *Public Law Review* 3, 5.
cdlxxv Ibid, 5.
cdlxxvi Ibid, 6.
cdlxxvii Ibid, 6.
cdlxxviii H Evans (ed), *Odger's Australian Senate Practice Tenth Edition*, Commonwealth of Australia, <www.aph.gov.au/senate/pubs/html/httoc.htm>, 482.
cdlxxix Ibid, 482.
cdlxxx Commonwealth of Australia, *Government Guidelines for Official Witnesses before Parliamentary Committees and Related Matters*.
cdlxxxi Ibid, 10, citing Senate Parliamentary Privilege Resolutions (1988), rules 1.7, 1.8 and 2.7.
cdlxxxii Ibid, 10.
cdlxxxiii H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney, 116.
cdlxxxiv Ibid, 117.

cdlxxxv *Ombudsman Act 1976* (Cth), s 12(3), see H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney, 117.

cdlxxxvi Freedom of information is discussed in Ch 2.

cdlxxxvii *Ombudsman Act 1976* (Cth), s 9(3)(a).

cdlxxxviii Ibid, s 9(3). See H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney, 118.

cdlxxxix H Lee, P Hanks and V Morabito, *In the Name of National Security: The Legal Dimensions* (1995) LBC Information Services, Sydney, 118.

cdxc T Carmody, 'Royal Commissions, Parliamentary Privilege and Cabinet Secrecy' (1995) 11 *Queensland University of Technology Law Journal* 48, 61.

cdxci *Royal Commissions Act 1902* (Cth), s 2, 3 and 6.

cdxcii T Carmody, 'Royal Commissions, Parliamentary Privilege and Cabinet Secrecy' (1995) 11 *Queensland University of Technology Law Journal* 48, 62.

cdxciii Ibid, 62.

cdxcivM Sassella, 'Reviewing Particular Decisions Made by ASIO: The Security Appeals Division of the Administrative Appeals Tribunal' (Paper presented at Security in Government Conference, Canberra, 1 April 2002), 2.

cdxcv The ASIO Annual Report notes that 12,355 security assessments related to employment or personnel security were conducted in 2001–02, with two adverse and six qualified assessments made. In relation to the issue of visas, five adverse findings were made out of over 39,000 assessments: Australian Security Intelligence Organisation, *Annual Report* (2002), ASIO, Canberra.

cdxcviM Sassella, 'Reviewing Particular Decisions Made by ASIO: The Security Appeals Division of the Administrative Appeals Tribunal' (Paper presented at Security in Government Conference, Canberra, 1 April 2002), 3.

cdxcvii Administrative Appeals Tribunal, *Annual Report* (2002), AAT, Canberra, 103.

cdxcviii Administrative Appeals Tribunal, *Security Appeals*, <www.aat.gov.au/leaflet8.htm>, 21 May 2003. See also the *Administrative Appeals Tribunal Act 1975* (Cth), s 39A(5).

cdxcixM Sassella, 'Reviewing Particular Decisions Made by ASIO: The Security Appeals Division of the Administrative Appeals Tribunal' (Paper presented at Security in Government Conference, Canberra, 1 April 2002), 4. See *Australian Security Intelligence Organisation Act 1979* (Cth), s 38(2)(b).

d *Australian Security Intelligence Organisation Act 1979* (Cth), s 38(2)(a).

di M Sassella, 'Reviewing Particular Decisions Made by ASIO: The Security Appeals Division of the Administrative Appeals Tribunal' (Paper presented at Security in Government Conference, Canberra, 1 April 2002), 5.

dii *Administrative Appeals Tribunal Act 1975* (Cth), s 39A(8)–(9).

diii *Australian Security Intelligence Organisation Act 1979* (Cth), s 38(2)(b).

div The role of the Inspector-General of Intelligence and Security is briefly described in Ch 1.

dv *Inspector-General of Intelligence and Security Act 1986* (Cth), s 18–19.

dvi The section provides that the Commonwealth may make laws with respect to the naval and military defence of the Commonwealth and of the several States and the control of the forces to execute and maintain the laws of the Commonwealth: see A Kirkham, 'The Future of the Defence Force Discipline Act' (2001) 119 *Victorian Bar News* , 53. The Constitutional validity of military tribunals has been considered on a number of occasions by the High Court and upheld, but not without some controversy: see W Walsh-Buckley, 'Military Courts-Martial in Australia' (1999) 23(6) *Criminal Law Journal* 335, 336.

dvii A summary authority may be an officer of the armed forces who is not a legal practitioner: *Defence Forces Discipline Act 1982* (Cth), s 105. Summary authorities hear only less serious offences committed by lower ranking officers, and are not authorised to impose more serious penalties such as dismissal or imprisonment, s 106–113.

dviii A Defence Force Magistrate is a legal practitioner appointed under Ibid, s 127, with the same jurisdiction and powers as a restricted court martial (s 129). Defence Force Magistrates may impose only a limited range of punishments; for example, they are able to sentence a period of imprisonment or detention for a maximum of six months only: *Defence Forces Discipline Act 1982* (Cth), Sch 2: see also W Walsh-Buckley, 'Military Courts-Martial in Australia' (1999) 23(6) *Criminal Law Journal* 335, 338.

dix *Defence Forces Discipline Act 1982* (Cth), Pt VII, Div 3.

dx M Groves, 'The Use of Criminal Law Principles in Military Discipline: Chief of General Staff v Stuart (1995) 133 ALR 513' (1997) 23 *Monash University Law Review* 456, 459.

dxi *Defence Forces Discipline Act 1982* (Cth), s 114.

dxii Ibid, s 116.

dxiii Ibid, s 134.

dxiv Ibid, s 133, see W Walsh-Buckley, 'Military Courts-Martial in Australia' (1999) 23(6) *Criminal Law Journal* 335, 338.

dxv *Defence Forces Discipline Act 1982* (Cth), s 140(2).

dxvi Ibid, s 150.

dxvii Ibid, Part IX.

dxviii W Walsh-Buckley, 'Military Courts-Martial in Australia' (1999) 23(6) *Criminal Law Journal* 335, 338.

dxix M Groves, 'The Use of Criminal Law Principles in Military Discipline: Chief of General Staff v Stuart (1995) 133 ALR 513' (1997) 23 *Monash University Law Review* 456, 464.

dxx *Defence Forces Discipline Act 1982* (Cth), s 101E and 137.

dxxi *Foreign Intelligence Surveillance Act 1978* (USA), 36 USC, s 1802–1804 (1978).

dxxii See the Electronic Frontier Foundation:<www.eff.org/Privacy/Surveillance/Terrorism_militias/fisa_faq.html>.

dxxiii This court was established as part of the original Act in 1978 but had never sat until 2002.

dxxiv F Murray, *High Court Rejects Challenge to Spy Laws*, The Washington Times, <www.washtimes.com/national/20030325-284477.htm>, 25 March 2003.

dxxv The Fourth Amendment to the US Constitution reads: 'The right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no warrants shall issue, but upon probable cause, supported by oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized.'

dxxvi A Ramasastry, *The Foreign Intelligence Surveillance Court of Review Creates a Potential End Run Around Traditional Fourth Amendment Protections for Certain Criminal Law Enforcement Wiretaps*, Findlaw's Writ, <http://writ.news.findlaw.com/ramasastry/20021126.html>, 12 May 2003.

dxxvii F Murray, *High Court Rejects Challenge to Spy Laws*, The Washington Times, <www.washtimes.com/national/20030325-284477.htm>, 25 March 2003.

dxxviii *Antiterrorism and Effective Death Penalty Act*, 12 USC, s 1532 (1996).

dxxix The non-citizens (or aliens) may be deported even if they are legally residing in the US.

dxxx B Wittes, *Does the US Really Need its New Secret Tribunal?*, Slate, <http://slate.msn.com/id/2129/>, 12 May 2003.

dxxxi Ibid.

dxxxii *Antiterrorism and Effective Death Penalty Act*, 12 USC, s 1534 (1996).

dxxxiii S Valentine, *Flaws Undermine Use of Alien Terrorist Removal Court*, Washington Legal Foundation, <www.prestongates.com/publications/article.asp?pubID=259>, 12 May 2003.

dxxxiv Ibid.

dxxxv Detention, Treatment and Trial of Certain Non-Citizens in the War Against Terrorism, s 3(a), 4(b), 66 Fed Reg 57,833 (13 November 2001); see N Katyal and L Tribe, 'Waging War, Deciding Guilt: Trying the Military Tribunals' (2002) 111 *Yale Law Journal* 1259, 1260.

dxxxvi Detention, Treatment and Trial of Certain Non-Citizens in the War Against Terrorism, note 3, s 4(c)(2)–(3), (6)–(7) 66 Fed Reg 57,833 (13 November 2001).

dxxxvii Ibid, s 4(c)(4), as noted in N Katyal and L Tribe, 'Waging War, Deciding Guilt: Trying the Military Tribunals' (2002) 111 *Yale Law Journal* 1259, 1262. Permission is also granted to impose the death penalty without a unanimous vote on either guilt or sentence.

dxxxviii See J Porth, *DOD Legal Officials Ready Rules for Future Military Commissions*, 2 May 2003.

dxxxix Department of Defense (USA), *Military Commission Instruction No 5*, 30 April 2003. The Instruction also sets out appeal rights to have a security clearance decision reviewed.

dxl Department of Defense (USA), *Military Commission Instruction No 7*.

dxli See *Ex Parte Quirin* 317 US (1942) discussed in H Koh, 'The Case Against Military Commissions' (2002) 96 *American Journal of International Law* 337, 338–339. Koh notes there are substantial differences in facts between *Quirin*, where Congress had formally declared war and authorised the commission as part of the

Articles of War, and the case following 11 September 2001, where the President acted without the approval of Congress.

dxlii Ibid, 338–339.

dxliii Ibid, 339.

Chapter 13

dxliv Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, D 21, para 5.1.

dxlv Ibid, D 24, para 5.16.

dxlvi Ibid, D 8, para 1.7.

dxlvii Ibid, D 8, para 1.7. There are two clearance review procedures: revalidation and re-evaluation. Re-evaluation, unlike revalidation, involves a new police check and referee check. Revalidation involves seeking information from the subject and his or her supervisor. Agencies are to determine their own policies and procedures for periodic revalidation and re-evaluation of clearances to the Confidential level. Secret and Top Secret clearances must be re-evaluated at intervals not exceeding five years, and will lapse if not re-evaluated within six years. The minimum requirement for revalidation of Top Secret clearances is every 30 months: see generally Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, D 55, para 8.3–D 56, para 8.11. Note that the US Commission on Protecting and Reducing Government Secrecy stated that most resources are directed to the initial clearance process and relatively less attention is placed on developing more effective procedures for assessing those who already have held security clearances for a number of years: see Commission on Protecting and Reducing Government Secrecy, *Report of the Commission on Protecting and Reducing Government Secrecy* (1997), US Government Printing Office, Washington, see<www.access.gpo.gov/congress/commissions/secrecy/index.html>, XXVII–XXVIII.

dxlviii Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, D 9, para 2.3.

dxlix Ibid, D 9, para 2.4.

dl Ibid, D 9, para 2.5.

dli Ibid, D 29, para 6.4.

dlii An adverse assessment contains a recommendation that the person not be given a clearance. A qualified assessment contains no such recommendation but has opinion, advice or information that is, or may be, prejudicial to the person: Ibid, D 52, para 7.10. In 2002 nine adverse or qualified personnel security assessments were recorded: D Goodsir, 'ASIO to Give Terror Secrets to Business', *The Sydney Morning Herald*, 26–27 April 2003, 3. The Security Appeals Division of the Administrative Appeals Tribunal is discussed in Ch 12.

dliii See the discussion of the Security Appeals Division of the AAT in Ch 12.

dliv F Wilkins, 'National Security and the Legal Aid Rules', *Lawyers Weekly*, 7 February 2003, 10, 10.

dlv Ibid, 10.

dlvi Ibid, 10.
dlvii See discussion below under the heading 'Wider changes'.
dlviii F Wilkins, 'National Security and the Legal Aid Rules', *Lawyers Weekly*, 7 February 2003, 10, 10.
dlix Ibid, 10.
dlx Opposition to Security Clearance Requirement for Legal Representatives' (2003) 41(2) *Law Society Journal* 6.
dlxi C Banham, 'If National Security's In Peril, So Is Legal Aid', *The Sydney Morning Herald*, 25 January 2001, 3.
dlxii C Banham, 'Lawyers Condemn "Secret" Legal Aid Rule Changes', *The Sydney Morning Herald*, 11 March 2003, 6.
dlxiii I Munro, 'Fight Looms on Security Checks', *The Age* (Melbourne), 5. In April 2003 the Standing Committee of Attorneys-General passed a motion asking the Commonwealth not to proceed with the legal aid guidelines: A Crosweller and A Wilson, 'Law Chiefs Test Double Jeopardy', *The Australian*, 12–13 April 2003, 19.
dlxiv The Victorian Bar, *Submission CSSI 1*, 8 April 2002.
dlxv Ibid.
dlxvi New South Wales Bar Association, *Submission CSSI 2*, 11 April 2003.
dlxvii Note that is has been reported that '[a]lthough ASIO experienced enormous backlogs in approving public servants for access to classified documents, it was able to process 98.7 per cent of [applications made in 2002] within 12 weeks': D Goodsir, 'ASIO to Give Terror Secrets to Business', *The Sydney Morning Herald*, 26–27 April 2003, 3.
dlxviii New South Wales Bar Association, *Submission CSSI 2*, 11 April 2003.
dlxix The Hon Daryl Williams AM QC MP, *News Release: Protecting Classified Information in Court Proceedings*, 3 April 2003.
dlxx Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill [No 2] 2002 (Cth), cl 34AA.
dlxxi The Bill allowed for a warrant where there were reasonable grounds for believing, among other things, that it would 'substantially assist the collection of intelligence that is important in relation to a terrorism offence': Ibid, cl 34C(3)(a).
dlxxii Ibid, cl 34C(3B) and (3C).
dlxxiii Office of the Attorney-General, *Australian Security Intelligence Organisation Legislation Amendment (Terrorism) Bill 2002—Government Proposals*, 11 June 2003.
dlxxiv Ibid.
dlxxv The Hon Daryl Williams AM QC MP, *Stronger Tools for ASIO to Combat Terrorism*, News Release, 26 June 2003.
dlxxvi See *Australian Security Intelligence Organisation Act 1979* (Cth), s 37. Section 37(1) provides that one of ASIO's functions is to furnish Commonwealth agencies with security assessments relevant to their functions and responsibilities.
dlxxvii For example, in NSW the person must have practised law for not less than five years and demonstrated a substantial involvement in the area of speciality chosen. After demonstrating eligibility the candidate must be successful in the assessment process. Methods of assessment generally include an open book written exam, a take home mock file and either an interview or a simulation. All applicants must submit the

names of referees who are contacted in writing to vouch for the applicant's competence. All accredited specialists must renew accreditation annually and undergo ongoing specialist legal education to retain their accreditation.

dlxxviii See *Corporations Act 2001* (Cth), s 911A. Section 916A of the Act deals with the authorisation of representatives to provide financial services or specified financial services on behalf of a licensee.

dlxxix See J Wasiliev, 'Accountants Lose Super Battle', *The Australian Financial Review* (Sydney), 12 May 2003, 3, which reports the gazettal of regulation 7.1.29 under the *Financial Services Reform Act 2001* (Cth), which specifies advisory activities that accountants can undertake without being licensed under the Act. Giving specific advice on superannuation is not one of the activities listed.

dlxxx The *Legal Profession Regulation 2002* (NSW), cl 7(1)(g) requires an application by a legal practitioner to disclose if the applicant has been found guilty of any offence (other than an excluded offence) and the nature of the offence. More information about offences is contained at cl 7(2) and 'excluded offences' are defined at cl 3(1) and (2) of the Regulation. In cl 7, 'offence' includes a tax offence. Clause 7(1)(h) requires the applicant to disclose whether he or she has committed an act of bankruptcy within the meaning of the *Legal Profession Act 1987* (NSW), whether or not the act occurred before or after the commencement of the Regulation.

dlxxxi *Legal Practice (Admission) Rules 1999* (Vic), r 4.01(1)(c).

dlxxxii Ibid, r 4.13.

dlxxxiii *Legal Practice (Admission) (Amendment) Rules 2003* (Vic), r 1.

dlxxxiv See Ibid, r 6. This rule amends *Legal Practice (Admission) Rules 1999* (Vic), r 4.03(1)(b)(iv) and 4.06(2)(b)(iv). 'Acceptable deponent' in relation to an applicant for admission 'means a person other than a person with whom the applicant has served under articles or served as a clerk who a) is described in section 107A of the Evidence Act 1958 and who has known the applicant for not less than 12 months; or b) is or was employed at a recognised secondary or tertiary teaching institution and by whom the applicant has been taught for not less than the equivalent of one year of tertiary studies or one of the two final years of secondary studies': *Legal Practice (Admission) (Amendment) Rules 2003* (Vic), r 5. The affidavit as to character in Schedule 9 requires the deponent to state the number of years that he or she has known the applicant, the circumstances in which he or she has known the applicant and to swear his or her belief that the applicant is of 'good reputation and character.'

dlxxxv Parliamentary Counsel's Committee, *Legal Profession—Model Laws Project—Consultation Draft*, 6 May 2003, cl 301(1).

dlxxxvi The admission rules may make provision for the convictions that must be disclosed by an applicant and the convictions that need not be disclosed: Ibid, Notes to cl 309.

dlxxxvii The name of the proposed Act is the *Legal Practitioners Act 2003:* Ibid, cl 101.

dlxxxviii Ibid, cl 309(2) provides that a 'person may be considered suitable for admission as a legal practitioner even though the person is within any of the categories mentioned in subsection (1), if the Supreme Court or certifying body considers that the circumstances warrant the determination.' 'Certifying body' is defined in cl 303.

dlxxxix See discussion in Ch 5.
dxc *Twenty-First Session (1984) General Comment No 13 ICCPR Article 14*, <www.hshr.org/General%20Comment%20files/ICCPR_GC13.htm> para 10.
dxci The Attorney-General's Department, *Commonwealth Protective Security Manual* (2000) Commonwealth of Australia, Canberra, D 27, para 5.29–5.31 sets out the circumstances under which emergency access to security classified information may occur; for example, emergency access to Top Secret information is only available to a person who has a current security clearance at Confidential level or higher. It is not clear whether these circumstances are intended to apply to the government's rules concerning security clearances for legal aid lawyers. In this regard, the Victorian Bar submitted that 'Even the proposed exception for urgent matters applies only where "access to information relating to national security is not required for the proper conduct of the applicant's case."': The Victorian Bar, *Submission CSSI 1*, 8 April 2002.
dxcii *Dietrich v The Queen* (1992) 177 CLR 292, para 40.
dxciii Ibid, para 40.
dxciv See *R v Gudgeon* (1995) 133 ALR 379, which applied and distinguished *Dietrich*, holding that a legally-aided appellant is not entitled to an adjournment on the basis that he is entitled to insist on being represented by a particular senior counsel, especially when junior counsel is still available to conduct the defence. See also *Attorney-General v Milat* (1995) 36 NSWLR 370, where it was held that the principles in *Dietrich* do not require or authorise the setting of a reasonable rate of remuneration for the accused's legal representation by the judiciary. The accused in that matter was unable to show that he was unable to obtain proper legal representation and that his trial would therefore be unfair. The courts have also said that *Dietrich* does not apply to committal proceedings: *Clarke v DPP (Commonwealth)* [1998] Supreme Court ACT 107 (24 September 1998) and that it may not apply to appeals: *Sinanovic v The Queen* [1998] HCA 40 (2 June 1998).
dxcv C Maher, 'The Right to a Fair Trial in Criminal Cases Involving the Introduction of Classified Information' (1988) 120 *Military Law Review* 83.
dxcvi See Ibid, 87–92 for a discussion of US cases dealing with the issue of selection of defence counsel who present a security risk and how that relates to an accused's right to counsel. For example, in *United States v Jolliff*, 548 F. Supp, 227, 233 (D.Md) 1981, the court stated although 'the Sixth Amendment grants an accused an absolute right to have assistance of counsel, it does not follow that his right to particular counsel is absolute.' In *United States v Nichols* 23 CMR 343 (Court of Military Appeals, 1957), the Court of Military Appeal held that 'the accused's right to a civilian attorney of his own choice cannot be limited by a service-imposed obligation to obtain clearance for access to service classified matter'. The Court of Military Appeals left the government with the options of granting access and allowing the defence to represent the accused, deferring proceedings against the accused, or disbarring defence counsel from practice before courts martial.
dxcvii J Porth, *DOD Legal Officials Ready Rules for Future Military Commissions*, 2 May 2003.

dxcviii Department of Defense (USA), *Military Commission Instruction No 5*, 30 April 2003, 2(d).
dxcix Department of Justice (USA), *Criminal Resource Manual*, <www.usdoj.gov/usao/eousa/foia_reading_room/usam>, 2054.
dc Ibid, 2054.
dci W Burger, *Security Procedures Established Pursuant to PL 96–456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information*, 12 February 1981, point 5.
dcii A copy of the draft legislation can be found at <www.dailyrotten.com/source-docs/patriot2draft.html>.
dciii The Foreign Intelligence Surveillance Court is discussed in Ch 12.
dciv There are basically three types of SIRC hearings: complaints about the alleged actions of the Canadian Security Intelligence Service; review of refusal of security clearances brought by government employees; and review of certain findings in immigration cases. See *Canadian Security Intelligence Service Act 1985* (Canada), s 38; and I Leigh, 'Secret Proceedings in Canada' (1996) 34 *Osgoode Hall Law Journal* 113.
dcv I Leigh, 'Secret Proceedings in Canada' (1996) 34 *Osgoode Hall Law Journal* 113, 163.
dcvi *Classified Information Procedures Act 18 USC App 1–16 1982* (USA).
dcvii W Burger, *Security Procedures Established Pursuant to PL 96–456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information*, 12 February 1981, point 4.
dcviii In the recent trial for espionage of Brian Regan in the United States, jurors were asked to fill out a detailed questionnaire revealing their thoughts about crime, espionage, the September 11 terrorist attacks and the death penalty: 'Spy Trial May End in Death', *The Canberra Times*, 15 January 2003, 11.
dcix For example, under the *Classified Information Procedures Act 18 USC App 1–16 1982* (USA) in criminal proceedings involving classified information, the court designates a court security officer who has been certified to the court in writing by a Department of Justice Security Officer as cleared for the level and category of classified information that will be involved. The security procedures established under the CIPA provide that no person appointed by the court or designated for service therein shall be given access to any classified information in the custody of the court, unless such person has received a security clearance as provided herein and unless access to such information is necessary for the performance of an official function': W Burger, *Security Procedures Established Pursuant to PL 96–456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information*, 12 February 1981, point 4. This requirement extends to court reporters: W Burger, *Security Procedures Established Pursuant to PL 96–456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information*, 12 February 1981, point 5.
dcx Department of Justice (USA), *United States Attorneys' Manual*, <www.usdoj.gov/usao/eousa/foia_reading_room/usam/> 9–90.200.
dcxi The Victorian Bar, *Submission CSSI 1*, 8 April 2002.

dcxii See, for example, the *Australian Constitution*, s 80, which reads: 'The trial on indictment of any offence against the law of the Commonwealth shall be by jury …'

dcxiii W Burger, *Security Procedures Established Pursuant to PL 96–456, 94 Stat. 2025, by the Chief Justice of the United States for the Protection of Classified Information*, 12 February 1981, point 6.

dcxiv Ibid, point 6.

dcxv See the proposed *Domestic Security Enhancement Act 2003* (PATRIOT ACT II), s 206.

dcxvi See The Hon Daryl Williams AM QC MP, 'Launch of the Trusted Information Sharing Network' (Paper presented at National Summit on Critical Infrastructure Protection, Melbourne, 2 April 2003).

dcxvii The Hon Daryl Williams AM QC MP, *News Release 35/03: Protecting Our Critical Infrastructure*, 2 April 2003.

dcxviii D Goodsir, 'ASIO to Give Terror Secrets to Business', *The Sydney Morning Herald*, 26–27 April 2003, 3.

dcxix *Australian Law Reform Commission Act 1996* (Cth), s 24(3) requires the ALRC to have regard to any effect that its recommendations might have on the costs of getting access to, and dispensing, justice.